Av. Mehmet Bedii KAYA

TEKNİK VE HUKUKİ BOYUTLARIYLA

İNTERNETE ERİŞİMİN ENGELLENMESİ

5651 Sayılı Kanun ve Dünya Uygulamaları

XII LEVHA

İÇİNDEKİLER

SUNUŞ v

ÖNSÖZ vii

İÇİNDEKİLER xi

KISALTMALAR xvii

KAYNAKÇA xxi

§ 1. GİRİŞ 1

§ 2. İNTERNET 5

I. Gelişim süreci 5
II. Çalışma prensipleri 7
III. İnternetin yönetimi 9
A. Yetkili kurumlar 10
1. ICANN 10
2. IANA 11
3. Kök sunucu operatörleri 11
4. Diğer kurumlar 11
B. Uluslararası yönetim sorunu 11

IV. Kullanım alanları 15
V. Yeni nesil İnternet: Web 2.0 18

§ 3. ERİŞİM ENGELLEME YÖNTEMLERİ 21

I. Engellemenin kapsamına göre 22
A. İSS temelli engelleme 22
B. İnternet omurgası temelli engelleme 23
II. Engelleme sürecine göre 23
A. Doğrudan engelleme 23
B. Uyar-kaldır yöntemiyle engelleme 24
III. Engelleme süresine göre 24
A. Geçici engelleme 24
B. Kalıcı engelleme 25
IV. Engelleme sistemine göre 26
A. Otomatik engelleme 26
B. Bireysel engelleme 27
V. Kullanılan tekniğe göre 27
A. IP engellemesi 28
B. DNS engellemesi 29
C. URL engellemesi 31
D. Proxy engellemesi 32
E. İçerik engellemesi 32
F. DDOS atakları 34
G. Alan adı terkin yöntemi 35
H. Fiziksel sunucu müdahalesi 36
I. Ağ hataları 36
J. Sosyal teknikler 36

§ 4. ENGELLEME AŞMA YÖNTEMLERİ 41

I. Yaygın teknikler 41
A. IP değişikliği 41

B. DNS değişikliği....42
C. URL gizleme....42
D. Proxy kullanımı....42
E. İçerik aldatması....43
F. Uzak masaüstü kullanımı....44
G. Kopya içerik kullanımı....44
H. Önbellek kullanımı....44
I. Online çeviri sistemleri....45
J. Trafik aktarımı....45
II. Değerlendirme....45
§ 5. MUKAYESELİ HUKUKTA ERİŞİMİN ENGELLENMESİ....47
I. ABD....47
II. Avrupa Birliği....54
III. Çin....61
IV. Güney Kore....65
V. Singapur....68
VI. Suudi Arabistan....72
§ 6. TÜRK HUKUKUNDA ERİŞİMİN ENGELLENMESİ....75
I. İnternet ile ilgili yetkili kurumlar....75
A. Bilgi Teknolojileri ve İletişim Kurumu....75
B. Telekomünikasyon İletişim Başkanlığı....76
C. İnternet Kurulu....77
D. Radyo Televizyon Üst Kurulu....78
II. 5651 sayılı Kanunu öncesi erişim engellemeleri....78
III. 5651 sayılı Kanunun hazırlık süreci....79
A. Bilişim Ağı Hizmetlerinin Düzenlenmesi ve Bilişim Suçları Hakkında Kanun Tasarısı....79
B. Bilişim Sistemi Üzerinden Suç Teşkil Eden Zararlı Yayınlarla Mücadele Hakkında Kanun Teklifi....80

C. Elektronik Ortamda İşlenen Suçların Önlenmesi ile 2559 ve 2937 sayılı Kanunlarda Değişiklik Yapılmasına Dair Kanun Tasarısı 81
1. Genel gerekçe 81
2. Adalet Komisyonu raporu 82
3. TBMM müzakereleri 84
IV. 5651 sayılı Kanuna göre İnternet erişiminin engellenmesi 85
A. Engelleme kararlarının hukuki niteliği 86
B. Engelleme sebepleri 86
1. İntihara yönlendirme 87
2. Çocukların cinsel istismarı 92
3. Uyuşturucu veya uyarıcı madde kullanılmasını kolaylaştırma 98
4. Sağlık için tehlikeli madde temini 101
5. Müstehcenlik 104
6. Fuhuş 110
7. Kumar oynanması için yer ve imkân sağlama 112
8. Sabit ihtimalli veya müşterek bahis oynatılması 114
9. Atatürk aleyhine işlenen suçlar 116
10. Fikri mülkiyet ihlalleri 119
C. Erişim engelleme yöntemi 120
1. Yetkili makamlar 120
a. Adli makamlar 120
b. TİB 121
2. Engelleme usulü 123
3. Engelleme kararının kaldırılması 124
4. Engellemenin sona erme halleri 125
5. Tazminat 125
D. Sorumluluk rejimi 127
1. İçerik sağlayıcılar 127
2. Yer sağlayıcılar 130

3. Erişim sağlayıcılar 132
4. İnternet toplu kullanım sağlayıcıları 134
5. Ortak hükümler 135
E. Yayından çıkarma ve cevap hakkı 135
V. 5651 sayılı Kanunun değerlendirilmesi 138
A. Sınırlama rejimi açısından değerlendirme 138
1. Kanunla sınırlama 139
2. Anayasanın sözüne ve ruhuna uygunluk 139
3. Ölçülülük ilkesi 140
4. Hakkın özü 143
5. Demokratik toplum düzeninin gereklilikleri 145
B. İfade hürriyeti açısından değerlendirme 149
§ 7. SONUÇ 153

KISALTMALAR

AB	:	Avrupa Birliği
ABD	:	Amerika Birleşik Devletleri
a.g.e.	:	adı geçen eser/eserler
aşa.	:	aşağıda
AİHM	:	Avrupa İnsan Hakları Mahkemesi
AMKD	:	Anayasa Mahkemesi Kararları Dergisi
ARPANET	:	Advanced Research Project Authrotiy Net
b.	:	bent
Bkz./bkz.	:	bakınız
BMJ	:	British Medical Journal
BTK	:	Bilgi Teknolojileri ve İletişim Kurumu
c.	:	cümle
CC	:	Creative Commons
CD	:	Ceza Dairesi
CDA	:	Communications Decency Act
CGK	:	Ceza Genel Kurulu
CIPA	:	Children's Internet Protection Act
CLN	:	Class Licence Notification
CMK	:	5271 sayılı Ceza Muhakemeleri Kanunu
COPA	:	Child Online Protection Act
DDOS	:	Distributed Denial of Service
dn.	:	dipnot

DNS	:	Domain Name System
DRM	:	Digital Rights Management
E.	:	Esas
E-Ticaret Yönergesi	:	Avrupa Birliği İç Pazarda Bilgi Toplumu Hizmetlerinin Bazı Hukuksal Yönlerine, Özelliklere Elektronik Ticaret İlişkin Avrupa Birliği Yönergesi
f.	:	fıkra
Faaliyet Yönetmeliği	:	Telekomünikasyon Kurumu Tarafından Erişim Sağlayıcılara ve Yer Sağlayıcılara Faaliyet Belgesi Verilmesine İlişkin Usul ve Esaslar Hakkında Yönetmelik
FSEK	:	5846 sayılı Fikir ve Sanat Eseleri Kanunu
http	:	Hypertext Transfer Protocol
IANA	:	Internet Assigned Numbers Authority
ICANN	:	Internet Corporation for Assigned Names and Numbers
ICP	:	Internet Code of Practice
INCB	:	Uluslararası Narkotik Kontrol Kurulu
Inhope	:	The International Association of Internet Hotlines
Interpol	:	Uluslararası Polis Teşkilatı
IP	:	Internet Protocol
IWF	:	Internet Watch Foundation
İSS	:	İnternet Servis Sağlayıcısı
İYUK	:	2577 sayılı İdari Yargılama Usulü Kanunu
K.	:	karar
K.T.	:	Karar tarihi
KACST	:	King Abdulaziz City for Science and Technology
KISCOM	:	The Korean Internet Safety Comission

LICRA	:	International League against Racism and Anti-Semitism
m.	:	madde
MDA	:	Media Development Authority
MÜYAP	:	Türkiye Bağlantılı Hak Sahibi Fonogram Yapımcıları Meslek Birliği
no	:	numara
ODTÜ	:	Ortadoğu Teknik Üniversitesi
par.	:	paragraf
Protokol	:	Çocuk Haklarına Dair Sözleşmeye Ek Çocuk Satışı, Çocuk Fahişeliği ve Çocuk Pornografisi İle İlgili İhtiyari Protokol
RG	:	Resmi Gazete
RSS	:	Rich Site Summary
RTÜK	:	Radyo Televizyon Üst Kurulu
s.	:	sayfa
STMP	:	Simple Mail Transfer Protocol
t.	:	tarih
Tasarı	:	Elektronik Ortamda İşlenen Suçların Önlenmesi ile 2559 ve 2937 sayılı Kanunlarda Değişiklik Yapılmasına Dair Kanun Tasarısı
TBA	:	Telecommunications Business Act
TBMM	:	Türkiye Büyük Millet Meclisi
TCK	:	Türk Ceza Kanunu
TCP	:	Transmission Control Protocol
TDK	:	Türk Dil Kurumu
Teklif	:	Bilişim Sistemi Üzerinden Suç Teşkil Eden Zararlı Yayınlarla Mücadele Hakkında Kanun Teklifi
TİB	:	Telekomünikasyon İletişim Başkanlığı
TL	:	Türk Lirası

Toplu Kullanım Yönetmeliği	:	İnternet Toplu Kullanım Sağlayıcıları Hakkında Yönetmelik
UN	:	United Nations
URL	:	Uniform Resource Locator
Uygulama Yönetmeliği	:	İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik
vb.	:	ve benzeri
vd.	:	ve devamı
Vol.	:	Volume
www	:	World Wide Web
XML	:	Extensible Markup Language
YHGK	:	Yargıtay Hukuk Genel Kurulu
yuk.	:	yukarıda
.tr UKK	:	İnternet Alan Adları Ulusal Koordinasyon Kurulu
1996 Tebliği	:	Avrupa Komisyonu İnternetteki Hukuka Aykırı ve Zararlı İçerik Tebliği

KAYNAKÇA

Akal	:	Cemal Bâli Akal, İktidarın Üç Yüzü, 2. Baskı, Ankara 2003
Akdeniz	:	Yaman Akdeniz, Beyaz Kitap - İnternet'in Çok Taraflı Yönetimi, İstanbul 2003
Akdeniz/Altıparmak	:	Yaman Akdeniz/Kerem Altıparmak, İnternet: Girilmesi Tehlikeli ve Yasaktır, Ankara 2008
Alexander	:	Gerd Alexander, The U.S. On Tilt: Why The Unlawful Internet Gambling Enforcement Act Is A Bad Bet, Duke Law & Technology Review, Rev. 6, 30 June 2008
Alptürk	:	Ercan Alptürk, Hukuksal, Teknik ve Vergisel Boyutlarıyla İnternette Kumar Oyunları, Lebib Yalkın Mevzuat Dergisi, Yıl: 2005, Sayı: 2 (Şubat)
ANCOILR	:	Andrews Computer & Online Industry Litigation Reporter, Rep. 24416, 1 July 1997
Arifoğlu/Körnes/ Yazıcı/Akgül/Ayvalı	:	Ali Arifoğlu/Abdullah Körnes/Ali Yazıcı/ Kemal Akgül/Ahmet Ayvalı, Türkiye Bilişim Derneği, E-Devlet Yolunda Türkiye, Ankara 2002
Article-19	:	Article 19: Global Campaign for Free Expression, Freedom of Expression and the Media in Singapore, London 2005
Bayamlıoğlu	:	İbrahim Emre Bayamlıoğlu, Fikir ve Sanat Eserleri Hukukunda Teknolojik Koruma, İstanbul 2008

Bick	:	Jonathan Bick, 101 Things You Need To Know About Internet Law, New York 2000
BMJ (2002/325)	:	Keith Hawton/Kathryn Williams, Influences of the media on suicide, BMJ Vol. 325, 11 December 2002
BMJ (2004/329)	:	Sundararajan Rajogopal, Sucide pacts and the Internet, BMJ Vol. 336, 4 December 2004
BMJ (2008/336)	:	Lucy Biddle/Jenny Danovan/Keith Hawton/ Navneet Kapur/David Gunnell, Suicide and the Internet, BMJ Vol. 336, 12 April 2008
Campbell/Machet	:	Penny Campbell/Emmanuelle Machet, European Policy on Regulation of Content on the Internet, Liberating Cyberspace: Civil liberties, human rights, and the Internet (Edited by Liberty), s. 140-158, London 1999
Canbay	:	Cafer Canbay, Alan Adları Yönetimi, Dünya Uygulamaları ve Türkiye İçin Çözümsel Yaklaşımlar, Ankara 2005
Chadwick	:	Andrew Chadwick, Internet Politics: States, Citizens and New Communication Technologies, New York 2006
Cisneros	:	Dannielle Cisneros, "Virtual Child" Pornography on the Net: A "Virtual" Victim?, Duke Law & Technology Review, Rev. 19, 23 September 2002
Civisec	:	Civisec - The Citizen Lab, Everyone's Guide to By-passing Internet Censorship: For Citizens Worldwide, Toronto 2007
Deibert/Palfrey/ Rohozinski/Zittrain	:	Ronald Deibert/John Palfrey/Rafal Ronozinski/Jonathan Zittrain, Access Denied: The Practice and Policy of Global Internet Filtering, Massachusetts 2008
Demirbaş	:	Timur Demirbaş, Ceza Hukuku Genel Hükümler, 3. Baskı, Ankara 2005

Dülger	:	Murat Volkan Dülger, İnternet Erişiminin Engellenmesinin Hukuksal Açıdan Değerlendirilmesi ve 5651 Sayılı Yasayla Getirilen Düzenleme, İstanbul Barosu Dergisi, Cilt: 81, Yıl: 2007, Sayı: 4, s. 1477–1547.
Erdoğan	:	Mustafa Erdoğan, Demokratik Toplumda İfade Özgürlüğü: Özgürlükçü Bir Perspektif, Teorik ve Pratik Boyutlarıyla İfade Hürriyeti (Editör: Bekir Berat Özipek), s. 37-47, Ankara 2003
Erem	:	Faruk Erem, Türk Ceza Kanunu şerhi: Özel Hükümler, Cilt III, Ankara 1993
Erman/Özek	:	Sahir Erman/Çetin Özek, Ceza Hukuku Özel Bölüm Kişilere Karşı İşlenen Suçlar (TCK 448-490), İstanbul 1994
Falcıoğlu	:	Mete Özgür Falcıoğlu, Karşılaştırmalı Hukuk (Amerikan Hukuku ve Viyana Antlaşması) ve Türk Hukukunda Elektronik Satım Sözleşmesi ve Kurulması, Ankara 2004
Farrell	:	Kristen Farrell, Corporate Complicity in the Chinese Cencoprship Regime: When Freedom of Expression and Profitability Collide, Journal of Internet Law, January 2008
Fuller	:	Kathleen E. Fuller, ICANN: The Debate Over Governing the Internet, Duke Law & Technology Review, Rev. 2, 14 February 2001
Goldsmith/Wu	:	Jack L. Goldsmith/Tim Wu, Who Controls the Internet? Illusions of a Borderless World, North Carolina 2006
Hall	:	Eric A. Hall, Internet core protocols: The definitive guide, Massachusetts 2000
Hick/Halpin/ Hoskins	:	Stewen Hick/Edward F. Halpin/Eric Hoskins, Human Rights and the Internet, New York 2000
Hofstetter	:	Fred T. Hofstetter, Internet Literacy, Boston 2006

Ivezaj	:	George Ivezaj, Child Pornography On the Internet: An Examination of the International Communities Proposed Solutions For a Global Problem, Michigan State University - DCL Journal of International Law, Fall, 1999
Kunter/Yenisey/ Nuhoğlu	:	Nurullah Kunter/Feridun Yenisey/Ayşe Nuhoğlu, Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku, 14. Bası, İstanbul 2006
Kuru/Arslan/Yılmaz	:	Baki Kuru/Ramazan Arslan/Ejder Yılmaz, Medeni Usul Hukuku, 16. Baskı, Ankara 2005
Kurt	:	Şahin Kurt, Uygulamada Uyuşturucu Madde Suçları ve İlgili Mevzuat, İstanbul 1992
Küçük	:	Adnan Küçük, İfade Hürriyetinin Unsurları, Ankara 2003
Meran	:	Necati Meran, Yeni Türk Ceza Kanununda Kişilere Karşı Suçlar, Ankara 2005
Otacı	:	Cengiz Otacı, Genel Adap ve Aile Düzenine Karşı İşlenen Suçlar, Ankara 2000
Öngören	:	Gürsel Öngören, İnternet Hukuku, İstanbul 2006
Özbudun	:	Ergun Özbudun, Türk Anayasa Hukuku, 8. Baskı, Ankara 2005
Özmen	:	Remzi Özmen, Notlu-Gerekçeli-Karşılaştırmalı 5237 sayılı Türk Ceza Kanunu, Ankara 2004
Parlar/Demirel	:	Ali Parlar/Güleç Demirel, Açıklamalı-İçtihatlı Kişilerin Hayatına ve Beden Bütünlüğüne Karşı Suçlar, Ankara 2002
Preston	:	Cheryl B. Preston, Internet Porn, ICANN and Families: A Call To Action, Journal of Internet Law, October 2008
Rao/Klopfenstein	:	Sandhya Rao/Bruce C. Klopfenstein, Cyber Path to Development in Asia: Issues and Challenges, Connecticut 2001

Sarıakçalı : Turgay Sarıakçalı, İnternet Üzerinden Akdedilen Sözleşmeler, Ankara 2008

Schauer : Frederick Schauer, İfade Özgürlüğü: Felsefi Bir İnceleme (çeviren: M. Bahattin Seçilmişoğlu), Ankara 2002

Shurville : Simon Shurville, Readings in Technology in Education: Selected Papers from the International Conference on Information and Communications Technology in Education 2006, Bradford 2007

Sınar : Hasan Sınar, İnternet ve Ceza Hukuku, İstanbul 2001

Steed : Charles Steed, The User Friendly Guide to Internet & Computer Terms, Nevada 2001

Stuckey : Kent D. Stuckey, Chapter 4: Obscenity and Indenecy, Internet and Online Law – Law Journal Press, 2008

Toluner : Sevin Toluner, Milletlerarası Hukuk Dersleri: Devletin Yetkisi, 5. Bası, İstanbul 1996

Yürüşen : Melih Yürüşen, Pornografiyi İfade Özgürlüğü Bağlamında Düşünmek, Teorik ve Pratik Boyutlarıyla İfade Hürriyeti (Editör: Bekir Berat Özipek), s. 209-244, Ankara 2003

Von Arx : Kim g. Von Arx, ICANN – Now and Then: ICANN's Reform and Its Problems, Duke Law & Technology Review, Rev. 7, 11 April 2003

Zittrain : Jonathan Zittrain, ICANN: Between the Public and the Private Comments Before Congress, Berkeley Technology Law Journal, Fall 1999

ELEKTRONİK AĞ ADRESLERİ*

Action Plan on Promoting Safer Use of the Internet, Decision No 276/1999/EC of the European Parliament and of the Council of 25 January 1999, http://ec.europa.eu/archives/ISPO/legal/fr/internet/actplan.html

Adalet Komisyonu raporu, Esas No: 1/305, 2/958 (12.04.2007), Karar No: 122, http://www.tbmm.gov.tr/sirasayi/donem22/yil01/ss1397m.htm

Alkollü İçkilerde Reklam ve Satış Geliştirmede Uyulacak İlke ve Kriterler, http://www.tapdk.gov.tr/alkol_duyuru9.htm

Anayasa Mahkemesi, K.T.: 08.04.1963, E: 1963/25, K: 1963/87, http://www.anayasa.gov.tr/eskisite/kararlar/iptalitiraz/K1963/K1963-087.htm

Anayasa Mahkemesi, K.T.: 22.05.1987, E: 1986/17, K: 1987/11, http://www.anayasa.gov.tr/eskisite/kararlar/iptalitiraz/K1987/K1987-11.htm

Anayasa Mahkemesi, K.T.: 22.05.1987, E: 1986/17, K: 1987/11, http://www.anayasa.gov.tr/eskisite/kararlar/iptalitiraz/K1987/K1987-11.htm

Anayasa Mahkemesi, K.T.: 28.01.1964, E: 1963/128, K: 1964/8, RG 17.04.1964/11685, http://www.anayasa.gov.tr/eskisite/kararlar/iptalitiraz/K1964/K1964-08.htm

Ankara Ticaret Odası, Sanal Tuzak: İnternet Kumarhaneleri, http://www.atonet.org.tr/turkce/index9.html

Arab Media: Saudi Internet rules, http://www.al-bab.com/media/docs/saudi.htm

Bilişim Ağı Hizmetlerinin Düzenlenmesi ve Bilişim Suçları Kanun Tasarısı, Kişisel Verilerin Korunması Hakkında Kanun Tasarısı, http://bt-stk.org.tr/bilisim-hizmetler-suclari.html

Bilişim Sistemi Üzerinden Suç Teşkil Eden Zararlı Yayınlarla Mücadele Hakkında Kanun Teklifi, http://www2.tbmm.gov.tr/d22/2/2-0958.pdf

Blogger.com, http://tr.wikipedia.org/wiki/Blogger.com

* Bu bölümde yer alan elektronik ağ adreslerinin tamamının güncelliği 1 Kasım 2009 tarihinde tekrar erişilmek suretiyle teyit edilmiştir.

Bush administration annexes internet, http://www.theregister.co.uk/2005/07/01/bush_net_policy/
CAN-SPAM Act of 2003, http://www.ftc.gov/bcp/edu/pubs/business/ecommerce/bus61.shtm
Censored: List of Countries that Banned YouTube, http://mashable.com/2007/05/30/youtube-bans/
Child Online Protection Act, http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=105_cong_bills&docid=f:h3783eh.txt.pdf
China Surpasses U.S. In Internet Use, http://www.forbes.com/2006/03/31/china-internet-usage-cx_nwp_0403china.html
Class Licence Notification (1996), http://www.mda.gov.sg/wms.file/mobj/mobj.487.ClassLicence.pdf
Commercial Sexual Exploitation of Children and Child Trafficking, http://www.yapi.org/csec/
Communications Decency Act, http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=104_cong_public_laws&docid=f:publ104.104.pdf
Convention against the Illicit Traffic in Narcotic Drugs and Psychotropic Substances, 1988, http://www.unodc.org/pdf/convention_1988_en.pdf
Convention on Psychotropic Substances, 1971, http://www.unodc.org/pdf/convention_1971_en.pdf
Convention on the Rights of the Child, http://www.unhchr.ch/html/menu3/b/k2crc.htm
COPA Litigation, http://www.cdt.org/speech/copa/litigation.php
Council of Europe - Convention on Cybercrime, http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm
Crimes against children, http://www.interpol.int/Public/Children/Default.asp
Crimes and Criminal Procedure - 18 USC Section 2256, http://law.onecle.com/uscode/18/2256.html
Devletin Kısayolu, https://www.turkiye.gov.tr

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:EN:NOT

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:178:0001:0016:EN:PDF

Directive of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, http://register.consilium.eu.int/pdf/en/05/st03/st03677.en05.pdf

Domain Registries in Turkey, http://www.webhosting.info/registries/country_stats/TR

Domain Registries, http://www.webhosting.info/registries/global_stats/

DPT - Bilgi Toplumu Dairesi Başkanlığı, http://www.bilgitoplumu.gov.tr/edtr.asp

Elektronik Ortamda İşlenen Suçların Önlenmesi ile 2559 ve 2937 sayılı Kanunlarda Değişiklik Yapılmasına Dair Kanun Tasarısı, http://www2.tbmm.gov.tr/d22/1/1-1305.pdf

Türkiye'de Site Erişime Kapatmalarının Tarihçesi, http://turk.internet.com/haber/yazigoster.php3?yaziid=20909

Erişim Sağlayıcı Yetkisine Sahip İşletmeler, http://www.tib.gov.tr/ES_listesi.html

European Commission Communication on Illegal and Harmful Content on the Internet (1996), http://aei.pitt.edu/5895/01/001527_1.pdf

Europe's Information Society Portal, http://ec.europa.eu/information_society/index_en.htm

Faaliyet Belgesine Sahip Yer Sağlayıcılar, http://www.tib.gov.tr/YS_listesi.html

Facebook, http://www.facebook.com/press/info.php?statistics

GEMA obtains injunctions against data exchange services, http://www.heise.de/english/newsticker/news/83948

German Politician Blocks Local Wikipedia, http://www.techcrunch.com/2008/11/16/german-politician-blocks-local-wikipedia/
Gesetz über die Nutzung von Telediensten (Teledienstegesetz -TDG), http://net-law.de/gesetze/tdg.htm
Girişimlerde Bilişim Teknolojileri Kullanımı Araştırması 2008, http://www.tuik.gov.tr/PreHaberBultenleri.do?id=2068
Google Cached Pages: What Are Cached Pages?, http://www.google-guide.com/cached_pages.html
Green Paper on the protection of minors and human dignity in audiovisual and information services (1996), http://aei.pitt.edu/1163/01/minors_info_soc_gp_COM_96_483.pdf
Guidelines for Governments on Preventing the Illegal Sale of Internationally Controlled Substances through the Internet, http://www.incb.org/pdf/Internet_Guidelines/Internet_guidelines_English.pdf
Hanehalkı Bilişim Teknolojileri Kullanımı Araştırması, http://www.tuik.gov.tr/PreIstatistikTablo.do?istab_id=46
How Obama's Internet Campaign Changed Politics, http://bits.blogs.nytimes.com/2008/11/07/how-obamas-internet-campaign-changed-politics/
ICANN Factsheet, http://www.icann.org/en/factsheets/fact-sheet.html
Information Operations Roadmap, http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB177/info_ops_roadmap.pdf
International Criminal Police Organization, http://www.interpol.int
Internet Archive: Wayback Machine, http://www.archive.org/web/web.php
Internet Censorship in the Gulf Countries, Part III, http://www.arabpressnetwork.org/articlesv2.php?id=2051
Internet Censorship: Law & policy around the world, http://www.efa.org.au/Issues/Censor/cens3.html
Internet Code of Practice, http://www.mda.gov.sg/wms.file/mobj/mobj.981.internet_code_of_practice.pdf
İnternet Daire Başkanlığı, 23 Kasım 2007 - 23 Kasım 2008 Faaliyet Raporu, http://www.tib.gov.tr/dokuman/faaliyet_raporu.pdf

Internet Servis Sağlayıcıların, Wi-Fi'lerin Logları Polis İçin Saklamalarını Öngören Kanun Tasarısı, http://www.leylakeser.org/2009/02/internet-servis-saglaycларn-wi-filerin.html
Internet Usage and Population in North America, http://www.internetworldstats.com/stats14.htm
Internet Usage in Asia, http://www.internetworldstats.com/stats3.htm
Internet Usage in European Union, http://www.internetworldstats.com/stats9.htm
Internet Watch Foundation and Wikipedia, http://en.wikipedia.org/wiki/Internet_Watch_Foundation_and_Wikipedia
IWF statement regarding Wikipedia webpage, http://www.iwf.org.uk/media/news.archive-2008.251.htm
İlker Atamer, 5651 Sayılı Kanun Çerçevesinde Erişim Engelleme Kararları, http://turk.İnternet.com/haber/yazigoster.php3?yaziid=20078
İnternet Alan Adları Yönetmeliği Taslağı, http://www.tk.gov.tr/Basin_Duyurular/Duyurular/kamuoyu/2009/Internet_Alan_Adlari_Yonetmelik_Taslagi.doc.
İnternet Daire Başkanlığı, 23 Kasım 2007 – 23 Kasım 2008 Faaliyet Raporu, http://www.tib.gov.tr/dokuman/faaliyet_raporu.pdf
İnternet Kurulu Üyeler Listesi, http://kurul.ubak.gov.tr/netkrl/ik_kurul_uyeleri
İnternet Üzerinde Çocuk Pornografisi, http://turk.internet.com/haber/yazigoster.php3?yaziid=13179
İntihar ve Şiddet, http://www.psikolog.org.tr/articles_detail.asp?cat=4&id=9
İntihar yöntemleri, http://tr.wikipedia.org/wiki/İntihar_yöntemleri
Jugendschutz, http://www.jugendschutz.net
Kişisel Verilerin Korunması Kanun Tasarısı, http://www.kgm.adalet.gov.tr/tbmmkom/kisiselveriler.pdf
Laws relating to the work of IWF, http://www.iwf.org.uk/police/page.22.htm
Localized Google search result exclusions, http://cyber.law.harvard.edu/filtering/google/
Middle East Internet Usage and Population Statistics, http://www.internetworldstats.com/stats5.htm

Miller v. California, http://laws.findlaw.com/us/413/15.html; http://www.oyez.org/cases/1970-1979/1971/1971_70_73/
Nepal: Internet Down, Total Censorship Imposed, http://www.nartv.org/2005/02/03/nepal-internet-down/
Netiquette Guidelines, http://www.ietf.org/rfc/rfc1855.txt
NSF and the Birth of the Internet, http://www.nsf.gov/news/special_reports/nsf-net/textonly/index.jsp
Nüdizm, http://tr.wikipedia.org/wiki/Nudizm
Obama Yönetimi Siber Güvenlik Stratejisinin Ana Çizgilerini Açıkladı!, http://www.leylakeser.org/2009/01/obama-yonetimi-siber-guvenlik.html
Online Sales to Climb Despite Struggling Economy, http://www.shop.org/c/journal_articles/view_article_content?groupId=1&articleId=702
Open architecture, http://en.wikipedia.org/wiki/Open_architecture
Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography, http://www.unhchr.ch/html/menu2/6/crc/treaties/opsc.htm
Pakistan lifts the ban on YouTube, http://news.bbc.co.uk/2/hi/technology/7262071.stm
Port Numbers, http://www.iana.org/assignments/port-numbers
Provisions on the Administration of Internet News Information Services (Chinese and English Text), http://www.cecc.gov/pages/virtualAcad/index.phpd?showsingle=24396
Psychotropics Desk, http://www.interpol.int/public/Drugs/synthetic/default.asp
Public Official Election Act, http://www.nec.go.kr/english/res/Public_Official_Election.pdf
Quarterly Retail E-Commerce Sales, http://www.census.gov/mrts/www/ecomm.html
Recovery Act, http://www.recovery.gov
Reno v. American Civil Liberties Union, http://www.law.cornell.edu/supct/html/96-511.ZS.html
Report of the Tunis phase of the World Summit on the Information Society, http://www.itu.int/wsis/docs2/tunis/off/9rev1.pdf
Root Server Technical Operations Assn, http://www.root-servers.org

Safer Internet Programme: Safer Internet Centres, http://ec.europa.eu/information_society/activities/sip/projects/centres/index_en.htm
Saudi Arabia: New Act on Cyber-Crimes will Boost e-Governance, https://www.zawya.com/story.cfm/sidZAWYA20070410055304
Sexual Offences Laws - Countries, http://www.interpol.int/Public/Children/SexualAbuse/NationalLaws/Default.asp
Sibersuç Sözleşmesi, http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/ConventionOtherLg_en.asp
Single Convention on Narcotic Drugs, 1961, as amended by the Protocol amending the Single Convention on Narcotic Drugs, http://www.unodc.org/pdf/convention_1961_en.pdf
South Korea's National Security Law, http://www.hartford-hwp.com/archives/55a/205.html
Stock Focus: Adult Entertainment Companies, http://www.forbes.com/2001/05/23/0523sf.html
Suicide Promotion (Internet), http://www.iwf.org.uk/government/page.101.351.htm
Suicide rates per 100,000 by country, year and sex, http://www.who.int/mental_health/prevention/suicide_rates/en/index.html
Sunshine Book Co. v. Summerfield, Postmaster General, 355 U.S. 372, http://altlaw.org/v1/cases/799128
Swedish ISPs vow to erase users' traffic data, http://news.cnet.com/8301-1023_3-10229618-93.html
TBMM Dönem: 22, Yasama Yılı: 3, Yalova Milletvekili Şükrü Önder'in; Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun Teklifi ve İçişleri Komisyonu Raporu (2/546), http://www.tbmm.gov.tr/sirasayi/donem22/yil01/ss962m.htm
Teenager commits suicide live on internet as 1,500 watch, http://www.telegraph.co.uk/news/worldnews/northamerica/usa/3497263/Teenager-commits-suicide-live-on-internet-as-1500-watch.html
Terör Örgütlerinin İnternet Ortamında Yürüttüğü Faaliyetler, http://www.caginpolisi.com.tr/20/41-43.htm
The Battle for the Communications Decency Act 1996 is over, http://www.cyber-rights.org/battle.htm

The Communist Cyber-Block, http://www.ifex.org/en/content/view/full/68881/
The Hotline and the law, http://www.iwf.org.uk/public/page.31.htm
The International Association of Internet Hotlines, https://www.inhope.org
The Korean Internet Safety Comission, http://www.icec.or.kr
The Telecommunications Business Act, http://www.itu.int/ITU-D/treg/Legislation/Korea/BusinessAct.htm
The top countries for cybercrime, http://www.msnbc.msn.com/id/19789995/
TİB İnternet Dairesi Başkanı Osman N. Şen İnternet Alanında Türkiye ve Dünya'da Yaşanan Gelişmeleri değerlendirdi, http://www.tib.gov.tr/etkinlikler_detay12.html
Top-Level Domains ("gTLDs"), http://www.icann.org/en/tlds/
Turkey 2008 Progress Report, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SEC:2008:2699:FIN:EN:PDF
Türk İnterpolü, http://www.egm.gov.tr/interpol/turkce/turkint.htm
Türkiye'de Uyuşturucu Suçu, http://www.cte.adalet.gov.tr/kaynaklar/yayinlar/uyusturucu.pdf
U.N. control of Internet? An idea for the "delete" file, http://www.usatoday.com/news/opinion/editorials/2005-11-14-our-view_x.htm
UN control of internet? Try again, http://www.csmonitor.com/2005/0916/p08s02-comv.html
URL Forwarding and URL Masking Services, http://www.washington.edu/computing/web/publishing/url-forwarding.html
US Court of Appeals for the 3rd Circuit, No. 99-1234, http://vls.law.vill.edu/locator/3d/Jun2000/991324.txt
VHO - Index of Censorship, http://www.vho.org/censor/Censor.html#Web
Web 2.0 Nedir?, http://turk.internet.com/haber/yazigoster.php3?yazi_id=14394
What Is Web 2.0, http://www.oreillynet.com/lpt/a/6228
World Internet Usage Statistics News and World Population Stats, http://www.internetworldstats.com/stats.htm

Yahoo Inc. v. L.I.C.R.A. and U.E.J.F., 169 F. Supp. 2d 1181 (N.D. Cal. 2001) (No. 00-21275), http://w2.eff.org/legal/Jurisdiction_and_sovereignty/LICRA_v_Yahoo/20040823_yahoo_v_licra-9th.pdf.

Youtube denetimi istemedi, http://www.tk.gov.tr/Basin_Duyurular/basintk/2008/02.08.2008/1d17f8.pdf

Yurdum Internet'i 10 Yaşında, http://www.internetarsivi.metu.edu.tr/10yil.php

11.05.2009 Tarihli İhbar İstatistikleri ("İhbar İstatistikleri"), http://www.guvenliweb.org.tr/content/11052009-tarihli-ihbar-istatistikleri-yayınlanmıştır

2007 Siber Suçluların ve DDOS Saldırıların Arttığı Yıl Oldu, http://turk.internet.com/haber/yazigoster.php3?yaziid=20166

2008 Yılı Hanehalkı Bilişim Teknolojileri Kullanım Araştırması Sonuçları, http://www.tuik.gov.tr/PreHaberBultenleri.do?id=2055

22. Dönem 5.Yasama Yılı 99. Birleşim Genel Kurul Tutanağı, http://www.tbmm.gov.tr/develop/owa/tutanak_g_sd.birlesim_baslangic?PAGE1=1&PAGE2=1&p4=19906&p5=B

5 Mayıs 2008 İtibariyle Son YouTube Erişime Kapatılma Olayı ve 5651 ile İlgili Gelişmeler, http://turk.internet.com/dosya/0809/yazilar/

5651 sayılı İnternet ortamında yapılan yayınların düzenlenmesi ve bu yayınlarlar yoluyla işlenen suçlarla mücadele edilmesi hakkında kanun hakkında düşünceler, http://www.turkhukuksitesi.com/makale_626.htm

5651 Sayılı Kanun Çerçevesinde Erişim Engelleme Kararları, http://turk.internet.com/haber/yazigoster.php3?yaziid=20078

§ 1. GİRİŞ

İnternet, dünyanın farklı noktalarında bulunan milyonlarca bilgisayarın birbirine bağlı olduğu ve kamusal kullanıma açık küresel bir ağdır[1]. İnternet kelimesi, İngilizce "uluslararası ağ" anlamına gelen "international network" sözcüklerinin birleştirilmesinden meydana gelmiştir[2]. İnternet hem bireysel ve kitlesel bir iletişim aracı hem de bir bilgiye erişim aracıdır. Bilginin çok hızlı ve ucuz bir şekilde yayılmasına olanak sağlayan İnternet sosyal hayatın her alanını etkilemekte ve yeni hukuki sorunlar ortaya çıkarmaktadır[3].

İnternet, her türlü ifadenin kendisine yer bulabildiği özgür bir ortam olarak düşülmektedir. Ayrıca, İnternetin devletlerin egemenlik alanlarının dışında kaldığı ve kendine özgü bir sistem olduğu şeklinde bir anlayış vardır. İnternetin kendine özgü bir sistemi olmakla birlikte sanıldığı gibi devlet müdahalesinden uzak ve tamamen özgür bir ortam değildir[4]. Dev-

[1] Fred T. Hofstetter, Internet Literacy, Boston 2006 ("*Hofstetter*"), s. 4.

[2] İnternet kelimesi baş harfi büyük yazıldığı zaman küresel ağı, küçük yazıldığı zaman bilgisayarlar arası herhangi bir ağı ifade etmektedir. Bkz. Charles Steed, The User Friendly Guide to Internet & Computer Terms, Nevada 2001 ("*Steed*"), s. 67.

[3] İnternetin yaygınlaşmasıyla birlikte modern toplum "bilgi toplumu" olarak adlandırılmaya başlanmıştır. Modern toplum "bilgi toplumu" olarak adlandırılsa da bu kavram modern toplumun önceki dönemleriyle farkını yeterince ifade etmemektedir. Nihayetinde, avcı toplayıcı hayattan tarım ekonomisine, oradan da üretim ekonomisine geçişte zaten temel belirleyici unsur bilgi olmuştur. Bilgi-işlem teknolojilerinin hayatın her alanında kullanılması sebebiyle bu dönemde modern toplumun değerlerini en iyi "ağ toplumu" kavramının yansıttığı düşünülmektedir. Daha fazla bilgi için bkz. İbrahim Emre Bayamlıoğlu, Fikir ve Sanat Eserleri Hukukunda Teknolojik Koruma, İstanbul 2008 ("*Bayamlıoğlu*"), s. 21.

[4] Ronald Deibert/John Palfrey/Rafal Ronozinski/Jonathan Zittrain, Access Denied: The Practice and Policy of Global Internet Filtering, Massachusetts 2008 ("*Deibert/Palfrey/Rohozinski/Zittrain*"), s. vii.

letler çeşitli sosyal, kültürel, siyasal veya ekonomik sebeplerle İnternet içeriğine müdahale etmekte ve vatandaşlarının İnternet üzerindeki aktivitelerini yoğun bir şekilde takip etmektedir.

Bir devletin kendi egemenlik alanında kendi koyduğu kuralları uygulaması uluslararası hukukun en temel ilkelerinden biridir[5]. Dolayısıyla, devletlerin İnternete müdahale etmeleri egemenliklerinin klasik bir icra şeklidir. Devletlerin İnternete müdahale etmelerinde iki temel sorun ortaya çıkmaktadır. Birinci sorun yapılan müdahalenin demokrasi ve insan hakları ilkelerine uygunluğu sorunudur. İkinci sorun ise, yapılan müdahalenin İnternetin kendine özgü yapısıyla ne kadar bağdaştığı sorunudur.

İnternet içeriğine devletlerin müdahale etmesi lehinde ve aleyhinde farklı görüşler ileri sürülmektedir. Devletlerin İnternete müdahalesini yerinde görenler, devletin öncelikli görevinin vatandaşlarının maddi ve manevi varlığını geliştirebileceği ortamı hazırlamak olduğunu; bu sebeple devletin İnterneti her türlü hukuka aykırı ve zararlı içerikten arındırması gerektiğini ileri sürmektedir. Ayrıca, devletin vatandaşlarını İnternetten gelen her türlü haksız müdahaleye karşı koruması için aktif rol oynaması gerektiği savunulmaktadır. Tüm bu iddialar devletin genel ahlakı ve aileyi koruma gibi yükümlülükleriyle desteklenmektedir.

Devlet müdahalesini yerinde görmeyenler ise müdahalelerin demokrasi ve insan hakları ilkeleriyle bağdaşmadığını ileri sürmektedir. Ayrıca, müdahalelerin İnternetin hızlı ve ucuz bilgiye erişim niteliğine darbe vuracağı ve İnternetin kalitesini düşüreceği iddia edilmektedir. Tüm bunların yanı sıra, her devletin İnterneti kendi önceliklerine göre düzenlemesi sonucunda düzenleme yapan ülke sayısı kadar farklı İnternet ortaya çıkacağı ve İnternetin kürsel ağ olma niteliğini kaybedeceği belirtilmektedir[6].

---

[5] Sevin Toluner, Milletlerarası Hukuk Dersleri: Devletin Yetkisi, 5. Bası, İstanbul 1996 (*"Toluner"*), s. 1.

[6] Farklı devletlerin müdahalesi farklı hukuk kurallarının uygulanmasını gündeme getirecektir. Bu kuralların birbiriyle çatışması kaçınılmaz olması bireyleri hareketsizliğe itecektir. Bkz. *Deibert/Palfrey/Rohozinski/Zittrain*, a.g.e., s. 31; Jack L. Goldsmith/Tim Wu, Who Controls the Internet? Illusions of a Borderless World, North Carolina 2006 (*"Goldsmith/Wu"*), s. 9.

İnterneti tamamını kontrol eden tek bir otorite olmadığı için kötüye kullanmaya açık bir sistemdir[7]. Devletler ilk zamanlar İnternetin kötüye kullanımlarını önlemek ve İnternet üzerinden işlenen suçlarla mücadele etmek için kurallar koymuşlarsa da, düzenlemelerin nitelik ve nicelikleri zamanla değişmiş ve devletler sosyal, politik, ekonomik birçok sebeple İnternet içeriğine müdahale etmeye başlamışlardır.

Her devletin İnternete yaklaşımı farklı olmuştur ve her devlet farklı bir sebep ve yöntemle İnternet içeriğine müdahale etmektedir. Ayrıca, her devlet farklı sorumluluk esaslarına göre İnternet kullanıcılarının ve diğer aktörlerin hukuki ve cezai sorumluluklarını düzenlemektedir. Bazı devletler İnternet içeriğine müdahale etmeksizin vatandaşlarının hukuki veya cezai sorumluluğuna giderken, bazıları içeriğe müdahale etmekle yetinmektedir.

İnterneti düzenleme sorunu sadece az gelişmiş veya gelişmekte olan devletlerin bir sorunu değildir. Hangi İnternet içeriğinin hangi sebeple ve yöntemle engelleneceğine ilişkin belirsizlik komünist düzene sahip Çin'in olduğu kadar, birer Avrupa Birliği ülkeleri olan Almanya, Fransa ve İngiltere'nin de sorunudur[8]. Çin, yoğun bir şekilde komünizme tehdit oluşturan içerikle mücadele ederken, ABD ve İngiltere çocuk pornografisiyle, Almanya ve Fransa aşırı sağcı içerikle, Suudi Arabistan İslam aleyhtarı içerikle, Güney Kore Kuzey Kore propagandasıyla mücadele etmektedir. Singapur ise seçim dönemlerinde İnternet içeriğine karşı katı bir tavır almaktadır.

Bu çalışma kapsamında İnternet erişiminin engellenmesi teknik ve hukuki boyutları ile mukayeseli bir şekilde ele alınmıştır. Çalışmada öncelikle engelleme yöntem ve teknikleri sınıflandırılmıştır. Bu sınıflandırmadan sonra İnternet içeriğine müdahale konusunda her biri bir ucu temsil eden ABD, Avrupa Birliği, Çin, Güney Kore, Singapur ve Suudi Arabistan devletlerinin erişim engelleme politikaları incelenmiştir. Son bölümde ise Türkiye uygulaması 5651 sayılı Kanun kapsamında ele alınmış ve kanunun uygulaması temel hak ve hürriyetleri sınırlandırma rejimi açısından değerlendirilmiştir.

---

[7] *Goldsmith/Wu*, a.g.e., s. 21.

[8] *Deibert/Palfrey/Rohozinski/Zittrain*, a.g.e., s. 33.

§ 2. İNTERNET

I. Gelişim süreci

İnternetin temeli ABD'nin askeri amaçlı veri iletişimi için çalıştığı Advanced Research Project Authrotiy Net ("ARPANET") projesine dayanmaktadır[9]. Bilginin bilgisayarlar tarafından kullanılabilmesi için sayısal birimlere dönüştürülmesi gerekmektedir. Bilginin bilgisayarlar tarafından kullanılabilecek ve işlenebilecek şekilde sayısal birimlerde gösterilmiş haline veri denilmektedir[10]. 1960'lı yılların başlarında, devletler ve şirketler bilgisayarlar arasında veri iletişimi için farklı teknolojiler kullanmaktaydı. Her bir bilgisayar kendine özgü ağ protokolü üzerinden başkaca bir bilgisayarla veri iletişimi yapmaktaydı. Bu sebeple, bilgisayarlar arasında bir ağ kurabilmek için tüm bilgisayarların sistem ayarlarının değiştirilmesi ve donanımlarının uyumlulaştırılması gerekmekteydi. Ağ kurmanın ekonomik olarak külfetli olması ve pratik olmaması sebebiyle, ağlar büyüyememekte, bu da verinin bilgisayarlar arasında iletimini ve dolayısıyla bilgi paylaşımını zorlaştırmaktaydı.

Yazılım ve donanım uyumsuzluğu sorunu dışında o dönemdeki ağların diğer bir sorunu ise her bir ağın çalışmak için bir ana bilgisayara ihtiyaç duymasıydı. Ana bilgisayar saldırı veya teknik bir sorun sebebiyle

---

[9] İnternetin tarihçesi için bkz. Mete Özgür Falcıoğlu, Karşılaştırmalı Hukuk (Amerikan Hukuku ve Viyana Antlaşması) ve Türk Hukukunda Elektronik Satım Sözleşmesi ve Kurulması, Ankara 2004 ("*Falcıoğlu*"), s. 44; Eric A. Hall, Internet core protocols: The definitive guide, Massachusetts 2000 ("*Hall*"), s. 1.

[10] *Falcıoğlu*, a.g.e., s. 43.

kapandığı takdirde tüm ağ çökmekteydi. Veriler de belirli güzergâhlar üzerinden iletildikleri için bir bağlantı hattının kesilmesi durumunda o güzergâh ile iletişim tamamen kesilmekteydi. Tüm bu sebeplerle, ABD Savunma Bakanlığı, Advanced Research Project Agency birimi bünyesinde nükleer saldırı dâhil herhangi bir saldırı sırasında veya sonrasında askeri kuvvetler, devlet kurumları ve araştırma merkezleri arasında kesintisiz iletişim sağlanması amacıyla 1969 yılında ARPANET projesi üzerinde çalışmaya başlamıştır.

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 Transmission Control Protocol ("TCP") ve Internet Protocol ("IP") protokolleri geliştirilmiştir[11]. 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 halinde ve aktif herhangi bir ağ üzerinden iletimi olanaklı hale gelmiştir. Ayrıca protokolün bir standart olarak kabul edilmesiyle donanım ve yazılım uyumsuzluğu sorunu gidermiş ve bilgisayarlar arasında kesintisiz veri iletişimi sağlanmıştır.

ARPANET askeri 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. 1983 yılında askeri amaçlı kullanılan ağ MILNET olarak ayrılmış ve geliştirilen ağ kamusal kullanıma tamamen açılmıştır.

1992 yılında Centre Europeén Recherces Nucléares tarafından World Wide Web ("www") standardı ve temel dosya transfer protokolü Hypertext Transfer Protocol ("http") geliştirilmiştir. Bu teknoloji sayesinde, İnternet üzerinden yazı, resim, ses, video gibi farklı nitelikteki verilere veri bütünlüğü bozulmadan iletmek mümkün olmuştur. İnternet ağına her geçen gün yeni bilgisayarlar eklenerek İnternet bugünkü hali-

[11] *Hall*, a.g.e., s. 4.

ni almıştır. İnternet ve TCP/IP protokolü sayesinde, bilgi bilgisayarlar aracılığıyla belirli bir merkeze ihtiyaç duymaksızın ve kesintisiz olarak dünyanın her noktasına iletilmektedir.

Türkiye'de ilk İnternet bağlantısı 1993 yılında Ortadoğu Teknik Üniversitesi'nden ("ODTÜ") gerçekleştirilmiştir. 12 Nisan 1993'de ODTÜ Bilgi İşlem Daire Başkanlığı'ndan, 64 Kbps kapasiteli hat ile ABD'de bulunan National Science Foundation Network ağına ilk bağlantı gerçekleştirilmiştir[12].

Görülmektedir ki, İnternetin ilk mimarları İnterneti şu an olduğu gibi kamuya açık bir ağ olarak tasarlamamışlardır. Tam aksine, İnternet askeri bir proje olarak geliştirilmiştir ve belirli noktalarda hâlâ onu geliştiren ABD'nin güvenlik stratejisinin bir parçası olmaya devam etmektedir[13]. Bu durum İnterneti tüm devletlerin ortak aklının ürünü ve kayıtsız bir özgürlük alanı olarak görmeyi engellemektedir[14].

II. Çalışma prensipleri

İnternet, dünyanın herhangi bir noktasındaki herhangi bir işletim sistemini veya bilgisayar donanımını kullanan herhangi bir kişinin dâhil olabileceği açık ağ mimari prensibine göre tasarlanmıştır. Açık mimari yayımlanmış standartlara sahip tasarım demektir[15]. İnternet için bu standart TCP/IP protokolüdür ve protokolünün çalışma esasları uluslararası bir standart olarak kabul edilmiştir. Bu sayede İnternet küresel bir ağ halini almıştır.

TCP/IP protokolü sayesinde, kişi veya kurumların mevcut ağ yapılarında köklü değişiklik yapmak zorunda kalmadan ve ek donanıma ihtiyaç duymadan İnternete bağlanmaları mümkün olmaktadır. İnterne-

[12] Yurdum Internet'i 10 Yaşında, http://www.internetarsivi.metu.edu.tr/10yil.php.

[13] Kim g. Von Arx, ICANN – Now and Then: ICANN's Reform and Its Problems, Duke Law & Technology Review, Rev. 7, 11 April 2003 ("*Von Arx*"), s. 3.

[14] Jonathan Zittrain, ICANN: Between the Public and the Private Comments Before Congress, Berkeley Technology Law Journal, Fall 1999 ("*Zittrain*"), s. 3.

[15] Açık mimari hakkında daha fazla bilgi için bkz. Open architecture, http://en.wikipedia.org/wiki/Open_architecture.

te bağlanan kimsenin hangi işletim sistemini veya donanımı kullanarak İnternete bağlandığı veri iletimi sırasında oluşturulacak paketin niteliğini etkilememektedir.

İnternet üzerindeki uygulamalar ağ üzerinde değil, web sitelerinin barındırıldığı sunucu olarak adlandırılan bilgisayarlarda uygulanmakta ve TCP/IP protokolü çalışan programlar arasında ayrım yapmamaktadır[16]. Bu durum ağ tarafsızlığı olarak ifade edilmektedir. Diğer bir deyişle, İnternet protokolü her türlü yazılıma ve donanıma karşı tarafsızdır[17].

TCP/IP teknolojisine göre iletilecek veri önce paketlere ayrılır ve her bir parça içerik ve etiket katmanı olmak üzere temelde iki katmanda paketlenerek ağ içerisinde iletilir[18]. İçerik katmanında verinin bir parçası, etiket katmanında ise verinin nihai iletim adresi yer almaktadır. İnternet kullanıcısı tarafından oluşturulan veri paketleri İnternet Servis Sağlayıcıları ("İSS") tarafından İnternet ağına aktarılmaktadır. Diğer bir deyişle İSS'ler verilerin kullanıcılardan ana İnternet ağına taşınmasında sadece aracılık etmektedirler. İSS'ler tarafından aktarılan paketler fiberoptik veya normal kablolar, kısa-mesafeli kablosuz bağlantılar veya uydu hatları gibi değişik noktalardan İnternet ağına bağlı router olarak adlandırılan ağ donanımları tarafından nihai iletim adreslerine taşınır.

İnternete bağlı her bilgisayarın Internet Protocol ("IP") denilen eşsiz bir nümerik adresi vardır. IP adresi İnternet üzerindeki herhangi bir bilgisayarı, cihazı, noktayı tanımlayan, bunlar arasında iletişim sağlayan, veri akışını sağlamak ve yönlendirmek amacıyla kullanılan biricik sayısal adres olarak tanımlanmaktadır[19]. Bir sunucu üzerinde sadece bir web sitesi barınabileceği gibi sunucunun teknik kapasitesine göre binlerce web sitesi de barınabilir. Routerlar web sitelerini IP adreslerine göre tanımlar ve paketleri üzerlerindeki etiket katmanına göre nihai iletim adreslerine

[16] *Bayamlıoğlu*, a.g.e., s. 342.

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

[18] *Hall*, a.g.e., s. 33.

[19] Cafer Canbay, Alan Adları Yönetimi, Dünya Uygulamaları ve Türkiye İçin Çözümsel Yaklaşımlar, Ankara 2005 ("*Canbay*"), s. 9.

iletir. Diğer bir deyişle, routerlar paketin içeriğiyle ilgilenmeksizin sadece etiket katmanına göre paketleri işlerler.

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

İnternet üzerindeki bilgi alışverişi bu şekilde veri paketlerinin farklı noktalar üzerinden taşınarak gerçekleştirildiği için dünya üzerindeki bir bilgisayarın diğer bir bilgisayardan daha fazla önemi olmadığı gibi tüm veri iletiminin gerçekleştirilmesi için sadece bir bilgisayar da sorumlu değildir[20]. Bu şekilde, İnternet ağına bağlı herhangi bir kullanıcı herhangi bir ülkedeki başkaca bir kullanıcıya veriyi göndermekte ve veri saniyeler içerisinde farklı devletleri ve dolayısıyla farklı hukuk rejimlerini herhangi bir merkeze uğramadan aşmaktadır.

III. İnternetin yönetimi

İnternet ağının tamamını kontrol eden tek bir otorite yoktur. İnternetin yönetimi ve işlerliği çeşitli ulusal ve uluslararası kurumlar tarafından işbirliği içerisinde sağlanmaktadır. İnterneti çekici kılan ve İnternetin çok kısa bir sürede yaygınlaşmasını sağlayan faktörlerin başında İnterneti yöneten tek bir otoritenin olmaması gösterilmektedir[21]. İnternet ağının tamamını yöneten tek bir otoritenin olmaması, İnternetin hukuksuz bir ortam olduğu manasına gelmemektedir. İnternet ağının kontrolüne ilişkin ulusal ve uluslararası düzeyde birçok düzenleme bulunmaktadır. İnternette ayrıca "netiquette" olarak adlandırılan ve İnternet kullanıcılarının oluşturduğu bazı etik kurallar da bulunmaktadır[22].

---

[20] *Hofstetter*, a.g.e., s. 20.

[21] Turgay Sarıakçalı, İnternet Üzerinden Akdedilen Sözleşmeler, Ankara 2008 ("Sarıakçalı"), s. 32.

[22] Bu tür kurallara uymak gönüllülük esasına bağlıdır. Spam olarak da adlandırılan istenmeyen epostalar göndermeme en yaygın ilkedir. Öte yandan, bazı devletler bu tür ku-

İnternetin küresel ağ niteliğinin korunması için bazı politikaların merkezi bir şekilde belirlenme gerekliliği vardır. Ana İnternet mekanizmalarının yönetimi ve politikaların belirlenmesi görevi çeşitli kurumlar tarafından gerçekleştirilmektedir. Bu kurumların en önemlileri şunlardır:

A. Yetkili kurumlar

1. ICANN

ABD İnternet ağının yaygınlaşmasıyla birlikte alan adı sisteminin özelleştirmesi için özerk olarak faaliyet göstermek üzere 1998 yılında Internet Corporation for Assigned Names and Numbers ("ICANN") kurumunu yetkilendirmiştir[23]. ICANN alan adları sisteminin teknik yönetimi, protokol parametrelerinin belirlenmesi ve kök sunucu sistemi yönetimi işlevlerini koordine etmekte ile görevlendirilmiştir. Bu yetkileri sebebiyle İnternetin tamamını ICANN'ın yönettiği şeklinde bir yanılgı vardır. Bu sebeple, ICANN ilk oluşturulduğun günden beri her zaman eleştirilere ve menfaat çekişmelerine maruz kalmıştır[24]. İnternet kullanımının yaygınlaşması ve alan adlarının ekonomik değerlerinin artması sebebiyle eleştiriler artarak ICANN'ın tüm yetkilerinin bağımsız bir uluslararası örgüt tarafından gerçekleştirilmesi talep edilmektedir.

---

rallara uymayı zorunlu hale getirebilmektedir. Örneğin, ABD 2003 yılında istenmeyen epostalar göndermeyi suç kabul etmiştir. Düzenleme için bkz. CAN-SPAM Act of 2003, http://www.ftc.gov/bcp/edu/pubs/business/ecommerce/bus61.shtm; Fikir ve sanat eserlerinin İnternette paylaşımı konusunda Creative Commons ("CC") adlı sivil toplum örgütü çeşitli netiquette kuralları oluşturmaktadır. Bkz. CC, http://www.creativecommons.org;Yaygın netiquette ilkeleri için bkz. Netiquette Guidelines, http://www.ietf.org/rfc/rfc1855.txt.

[23] Kurumun oluşturulma süreci için bkz. *Canbay*, s. 26; ICANN Factsheet, http://www.icann.org/en/factsheets/fact-sheet.html.

[24] Kathleen E. Fuller, ICANN: The Debate Over Governing the Internet, Duke Law & Technology Review, Rev. 2, 14 February 2001 ("*Fuller*"), s. 1.

2. IANA

Internet Assigned Numbers Authority ("IANA") ICANN ile koordinasyon içerisinde IP adreslerinin yönetimini gerçekleştirmek amacıyla ve ICANN gibi bağımsız olarak faaliyet göstermek üzere ABD Ticaret Bakanlığı tarafından yetkilendirilmiş kurumdur[25]. IANA'nın yetkisi, IP yönetimi için politikalar belirlemekten ziyade önceden belirlenmiş politikaları tarafsız bir şekilde uygulamaktan ibarettir. ICANN için yöneltilen uluslararası katılım sorunu IANA için de geçerlidir.

3. Kök sunucu operatörleri

İnternet trafiğini düzenleyen toplam 13 kök sunucu bulunmaktadır ve her bir sunucu ICANN tarafından akredite edilmiş farklı kurumlar tarafından yönetilmektedir[26]. Yönetimdeki ABD etkisi sebebiyle, ICANN ve IANA için yöneltilen uluslararası katılım eleştirileri kök sunucu yönetimi için de ileri sürülmektedir.

4. Diğer kurumlar

Tüm bu kurumlar dışında, Internet Engineering Task Force, Internet Research Task Force, Internet Society, World Wide Web Consortium gibi kurumlar İnternet ile ilgili temel politikaların belirlenmesine yardımcı olmakta ve bu alanda çeşitli araştırma-geliştirme çalışmaları sürdürmektedir.

B. Uluslararası yönetim sorunu

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 onları kim kontrol edeceği sorunu bazıları tarafından telefon numaralarının veya trafik plakalarının tahsis edilmesi gibi basit bir teknik bir sorun olarak

---

[25] About the Internet Assigned Numbers Authority, http://www.iana.org/about/.

[26] Türk İnternet trafiği I isimli ana İnternet sunucusu üzerinden akmaktadır. Daha fazla bilgi için bkz. Root Server Technical Operations Assn, http://www.root-servers.org.

görülmektedir[27]. Ancak, İnternetin kullanım alanlarının artması, İnternetin milyarlarca dolarlık elektronik ticarete ev sahipliği yapması, alan adlarının değerlenmesi ve çeşitli fikri mülkiyet sorunlarına yol açması ve İnternet üzerinden veri iletişimin ulusal güvenliğin bir parçası olarak görülmesi gibi sebeplerle alan adları ve IP adreslerinin yönetimi büyük bir menfaat çatışması doğurmaktadır[28].

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 çekişmelerinden nitelik olarak farklı devletlerarası bir menfaat ve ideoloji sorundur[29]. Devletler, İnternetin yaygınlaşmasıyla, İnternetin sosyal, siyasal ve ekonomik hayatı yönlendiren etkili bir araç olduğunun farkına varmışlardır[30]. Bu sebeple, her devlet farklı bir iç dinamikten dolayı İnternet üzerindeki etkisini artırmak istemektedir.

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

İnternetin tamamını yöneten tek bir otoritenin yokluğunun getirdiği en önemli avantaj olarak İnternetin işlerliğim ekonomik olarak tek bir kuru-

---

[27] *Goldsmith/Wu*, a.g.e., s. 31.

[28] Bu konudaki tüm eleştiriler için bkz. *Canbay*, a.g.e., s. 20; *Zittrain*, a.g.e., s. 6.

[29] Devletlerin İnternet üzerindeki hâkimiyetleri uzay ile ilgili egemenlik tartışmalarına benzetilmektedir. Bkz. *Goldsmith/Wu*, a.g.e., s. 171; Uzay ve gök cisimlerinin hukuki statüsü konusunda egemenlik ilkesinden hareket edilmemektedir. Devletlerin iktisadi ve bilimsel gelişme derecesi ne olursa olsun, bu kaynaklardan yararlanma tüm devletlere açık olması kabul edilmektedir. Diğer bir deyişle egemenlik hakkından ziyade yararlanma hakkı ön plana çıkmaktadır. Daha fazla bilgi için bkz. *Toluner*, a.g.e., s. 49.

[30] U.N. control of Internet? An idea for the 'delete' file, http://www.usatoday.com/news/opinion/editorials/2005-11-14-our-view_x.htm.

ma bağlı olmaması gösterilmektedir[31]. En önemli dezavantaj olarak ise, İnternetin kötüye kullanılmasını yaptırıma bağlayacak merkezi bir otoritenin bulunmaması gösterilmektedir. İnternetin kötüye kullanılmasını önlemek amacıyla her bir devletin kendi egemenlik alanında üzerine düşeni yapması gerekmektedir. Aynı doğrultuda, her bir devlet İnternet aracılığıyla veya İnternet üzerinden işlenen suçlarla mücadele etmeli ve ağının suçlular tarafından mesken edinilmesini önlemelidir. Bu amaçların sağlanmasında her bir devletin menfaati bulunmaktadır. Aksi durumda, bazı devletler İnternet suçları için odak haline gelmekte ve bu da İnternet üzerindeki işlem güvenliğini tehdit etmekte ve İnternete olan güveni zedelemektedir[32].

Devletlerin katılımı İnternetin yönetiminde önemli bir yer tutsa da ICANN ve IANA'nın mevcut yapılanma şekilleri İnternet politikalarının taraflı olmasına yol açmaktadır[33]. ICANN ve IANA devlet müdahalesi olmaksızın İnterneti düzenleyecek ve İnternetin tüm aktörleri arasında etkileşimi sağlayacak bağımsız kurumlar olarak düşünülmüşlerdir[34]. Ancak ne ICANN ne de IANA düşünüldükleri gibi bağımsız olamamıştır. Aynı şekilde, tüm kök sunucular üzerinde ve özellikle verileri tüm kök sunucular tarafından temel değer olarak alınan A Kök sunucusu üzerindeki ABD'nin mutlak hâkimiyeti, devletlerin kendi üst düzey ülke alan adları üzerinde bile egemen olmalarına veya bu alan adları üzerinde hak iddia etmelerine imkân vermemektedir[35].

ABD, özellikle ICANN'ı özelleştirme ve uluslararası katılıma açma konularında çeşitli denemelerde bulunsa da, sahip olduğu yetkilerini devretme konusunda hiçbir zaman istekli davranmamıştır. ABD tam aksine İnternet üzerindeki yetkilerini daha fazla artırmak için çeşitli girişimlerde bulunmaktadır. Yukarıda açıklandığı üzere, İnternet, ABD'nin askeri iletişim stratejisinin bir parçası olarak ortaya çıkmıştır. ABD İnterneti aynı

[31] Hasan Sınar, İnternet ve Ceza Hukuku, İstanbul 2001 ("*Sınar*"), s. 30.

[32] Örneğin Çin siber suçlar için kullanılan çeşitli yazılımların en çok barındırıldığı ülke olarak bir siber suç cenneti olarak kabul edilmektedir. Bkz. The top countries for cybercrime, http://www.msnbc.msn.com/id/19789995/.

[33] Cheryl B. Preston, Internet Porn, ICANN and Families: A Call To Action, Journal of Internet Law, October 2008 ("*Preston*"), s. 2.

[34] *Goldsmith/Wu*, a.g.e., s. 169.

[35] *Von Arx*, a.g.e., s. 1.

amaç için kullanmaya devam etmekte ve elektronik ticaret ABD ekonomisinin önemli dinamiklerinden birisini oluşturmaktadır[36]. Bu sebeple, ABD İnternet üzerindeki egemen konumunu korumayı ekonomik ve ulusal güvenlik menfaatleri gereğince sürdürmektedir[37].

İnternetin yoğun ticari işlemler ve kritik iletişim alanlarında kullanılması, devletlerin gizlilik politikalarının farkı olması, ulusal güvenlik tehditleri ve İnternet altyapı yatırımları sebepleriyle, başta Avrupa Birliği olmak üzere uluslararası toplum, İnternet üzerindeki ABD etkisinin kırılması için çeşitli girişimlerde bulunmuştur. Ayrıca ICANN'ın kök sunucularının güvenliğini sağlayamaması ve devletlerin bu yöndeki taleplerini geri çevirmesi de bu yöndeki girişimleri hızlandırmıştır[38]. Bu girişimlerden en önemlisi 2005 yılında Tunus'ta gerçekleştirilen Dünya Bilgi Toplumu Zirvesi'nde gerçekleştirilmiştir. Zirvede, Avrupa Birliği radikal bir teklifte bulunarak, alan adı yönetiminin ICANN ve Amerikan Ticaret Bakanlığı'ndan alınarak Birleşmiş Milletler nezdinde faaliyet gösterecek bir ihtisas kurumuna aktarılmasını önermiştir[39]. ABD bu teklifi kabul etmemiş ve mevcut tepkileri dindirmek için devletlerin İnternetle ilgili görüşlerini doğrudan beyan edebilecekleri Internet Governance Forum isimli uluslararası platformu faaliyete sokacağını belirtmekle yetinmiştir[40].

Öte yandan, İnternet yönetiminin Birleşmiş Milletler'e bırakılmasına da çeşitli eleştiriler getirilmektedir. Eleştirilerin başında, yönetimin

---

[36] Sadece Amerika genelinde 2008 yılında 204 Milyar Dolarlık elektronik ticaret hacminin gerçekleştiği tahmin edilmektedir. Bkz. Online Sales to Climb Despite Struggling Economy, http://www.shop.org/c/journal_articles/view_article_content?groupId=1&articleId=702; Diğer e-ticaret istatistikleri için bkz. Quarterly Retail E-Commerce Sales, http://www.census.gov/mrts/www/ecomm.html.

[37] İnternetle ilgili politikaların ABD'nin etkisinde ancak görünürde bağımsız ICANN tarafından belirlenmesi ve icra edilmesi sayesinde ABD'nin siyasal sorumluluktan kaçtığı iddia edilmektedir. Bkz. *Fuller*, a.g.e., s. 2.

[38] Kök sunucuların sorumluluğunun ICANN'da bulunmasına karşın hayati önem taşıyan bu sunucular farklı şirketler tarafından kontrol edilmektedir. Devletlerin katılım taleplerine olumsuz bakan ICANN, kök sunucuların düzenli çalışması ve güvenliği konusunda devletlere güvence de vermemektedir. Daha fazla bilgi için bkz. *Canbay*, a.g.e., s. 31.

[39] *Goldsmith/Wu*, a.g.e., s. 171.

[40] Report of the Tunis phase of the World Summit on the Information Society, http://www.itu.int/wsis/docs2/tunis/off/9rev1.pdf, s. 17.

Birleşmiş Milletlere bırakılmasının bürokrasiyi artıracağı ve bunun da İnternet gibi dinamik bir yönetimi gerektiren bir alanın işlerliğinin tehlikeye gireceği korkusu gelmektedir[41]. Ayrıca, İnternet yönetiminin Birleşmiş Milletler'e ek mali külfet getireceği ve Birleşmiş Milletlerin bu külfeti tüm devletlere eşit olarak yansıtmakta zorlanacağı iddia edilmektedir. Tüm bunların yanı sıra, Birleşmiş Milletlerin mevcut yapılanmasının karar alma süreçlerinde Güvenlik Konseyi'nin beş daimi üyesi lehine dengesizlik yaratması sebebiyle, aynı dengesizliğin İnternet politikalarına da yansıyacağı korkusu olası bir Birleşmiş Milletler yönetiminin önünde engel oluşturmaktadır.

Hem mevcut ABD yönetimine hem de olası bir Birleşmiş Milletler yönetimine çeşitli eleştiriler getirilmektedir. Aslında önemli olan İnterneti kimin yönettiği değil, nasıl yönettiğidir. Hangi kurum tarafından yönetilirse yönetilsin, İnternet yönetim politikalarının ulusal değerlerden arındırılması ve yönetimin tarafsızlığının sağlanması gerekmektedir[42]. Tüm bunlar yapılırken, İnternetin teknik işlerliğine öncelik verilmesi ve yönetimin teknik, politik ve yapısal olarak pratik olması İnternetin dinamizmine uygun düşecektir[43].

IV. Kullanım alanları

İnternetin kullanıldığı alanlar ve İnternete bağlı insan sayısı günbegün hızla artmaktadır. 2009 yılı itibariyle birbuçuk milyarı aşkın kişinin İnterneti kullandığı tahmin edilmektedir[44]. Ayrıca aynı yıl itibariyle 107.251.409[45] kayıtlı alan adı bulunmaktadır. Özellikle, mobil aygıtlar üzerinden hızlı İnternet bağlantısına imkân veren 3G ve yüksek hızda

[41] *Von Arx*, a.g.e., s. 7; UN control of Internet? Try again, http://www.csmonitor.com/2005/0916/p08s02-comv.html.

[42] Yaman Akdeniz, Beyaz Kitap - İnternet'in Çok Taraflı Yönetimi, İstanbul 2003 ("*Akdeniz*"), s. 35.

[43] *Akdeniz*, a.g.e., s. 44; *Von Arx*, a.g.e., s. 9.

[44] World Internet Usage Statistics News and World Population Stats, http://www.internetworldstats.com/stats.htm.

[45] Domain Registries, http://www.webhosting.info/registries/global_stats/. Bu alan adlarının 810.765 tanesi Türk kullanıcılara aittir. Bkz. Domain Registries in Turkey, http://www.webhosting.info/registries/country_stats/TR.

kablosuz İnternet bağlantısına olanak veren WiMAX teknolojilerinin yaygınlaşmasıyla, İnternet kullanıcısı sayısının daha hızlı artacağı tahmin edilmektedir.

İnternetin sosyal, ekonomik veya kültürel amaçlarla kullanım alanlarının artması sebebiyle devletler tarafından olası bir müdahale durumunda etkilenecek hak ve hürriyetlerin sayısı da aynı oranda artırmaktadır. Diğer bir deyişle, bir engelleme kararı sadece iletişim hakkı ve bilgiye erişim hakkını etkilememekte, aynı zamanda din ve vicdan hürriyeti, mülkiyet hakkı, maddi ve manevi varlığı geliştirme hakkı gibi birçok hakkı da etkilemektedir. İnternetin hayatın hangi alanlarda kullanıldığının tespit edilmesiyle engelleme kararlarından etkilenen hakların tespit edilmesi kolaylaşacaktır.

İnternetin en öne çıkan özelliklerinden birisi küresel bir kitle iletişim aracı olmasıdır. Televizyon veya radyo gibi klasik kitle iletişim araçları geniş kitlelere ulaşmakla birlikte belirli bir coğrafyaya hitap ettikleri için sınırlıdırlar[46]. Oysa İnternet coğrafi sınırlara veya belirli bir merkeze bağlı olmadan ortak bir standart dil üzerinden çalışma esasına göre tasarlanmıştır. Bu özelliği sayesinde, İnternet herkese hitap etmektedir. Ayrıca, İnternet diğer kitle iletişim araçlarının aksine muhatap kitleyle karşılıklı etkileşimi mümkün kılmaktadır. Diğer bir deyişle İnternet, kullanıcılarını klasik kitle iletişim araçlarının aksine edilgen olmaktan çıkarıp etken bir hale getirmektedir[47].

İnternet bağlantı ücretlerinin ucuzlaması ve devletlerin İnterneti yaygınlaştırmak için yaptıkları özendirme ve destekleme faaliyetlerinin bir sonucu olarak İnternet kullanmak bir lüks olmaktan çıkmış ve artık temel bir yetenek halini almıştır[48]. Bu sebeple, İnterneti kim kullanıyor sorusuna tüketici bir yanıt vermek zorlaşmaktadır. Aynı şekilde, İnter-

---

[46] *Falcıoğlu*, a.g.e., s. 49.

[47] *Falcıoğlu*, a.g.e., s. 49.

[48] Türkiye'de, İnternet üzerinden alınan özel iletişim vergisinin %15'ten %5'e düşürülmesi İnternetin yaygınlaştırılması yönünde atılmış olumlu bir adımdır. Bkz. 5838 sayılı Bazı Kanunlarda Değişiklik Yapılması Hakkında Kanun, Kabul T.: 18.02.2009, RG 28.02.2009/27155 (Mükerrer).

netin etkileşimli özelliği, İnternetin kullanım alanları için tüketici bir listeleme yapmayı imkânsız kılmaktadır.

İnternet ilk zamanlarda her ne kadar bir iletişim aracı olarak düşünülmüşse de, artık ticaretin en önemli araçlarından birisi haline gelmiştir[49]. Özellikle, Amazon, Ebay, Yahoo gibi şirketlerin İnternet üzerinden yoğun hacimli ticari işlemler yapması, elektronik ticarete ivme kazandırmış ve İnternetin özellikle ticari amaçlı olarak kullanımı ön plana çıkarmıştır[50].

İnternet suçta aracı olarak kullanılabileceği gibi, İnternet üzerinden suç işlenilmesi de mümkündür. Özellikle, terör örgütleri İnterneti yoğun bir şekilde propaganda, militanların eğitimi, haberleşme, bilgi toplama gerçekleştirmek amacıyla kullanmaktadır[51]. Başkasının ağına saldırı yapma ve veriler müdahale etme gibi İnternete özgü suçlar da işlenmesi mümkündür. Bazen bu tür suçlar büyük maddi zararlara da sebep olabilmektedir. Örneğin, Filipinlerden yayılan "I love you" isimli bir virüs dünya genelinde 15 milyar dolar zarara sebep olduğu tahmin edilmektedir[52].

İnternet devletler tarafından da çeşitli amaçlarla kullanılmaktadır. İnternetin devletler tarafından vatandaşlarına hem hizmet sunmak hem de vatandaşlarını kontrol etmek amacıyla kullanılabilmektedir. Devletlerin sunmakla yükümlü olduğu görev ve hizmetler ile vatandaşların buna karşılık devlete karşı olan görev ve hizmetlerinin karşılıklı olarak İnternet gibi elektronik ortamlarda yürütülmesi e-devlet olarak ifade edilmektedir[53]. E-devlet sistemi vatandaşların devlet tarafından sunulan hizmetlere tek noktadan giriş, kolay işlem ve arama yapmalarına olanak sağlamakta-

---

[49] *Sarıakçalı*, a.g.e., s. 25.

[50] ABD e-ticaret istatistikleri için bkz. dn. 36.

[51] Terör Örgütlerinin İnternet Ortamında Yürüttüğü Faaliyetler, http://www.caginpolisi.com.tr/20/41-43.htm.

[52] *Goldsmith/Wu*, a.g.e., s. 165.

[53] Ali Arifoğlu/Abdullah Körnes/Ali Yazıcı/Kemal Akgül/Ahmet Ayvalı, Türkiye Bilişim Derneği, E-Devlet Yolunda Türkiye, Ankara 2002 ("*Arifoğlu/Körnes/Yazıcı/Akgül/Ayvalı*"), s. 12; ABD, kamu kurumlarının web sitelerini etkileşimli hale getirmek için 2004 yılında 50 milyon dolardan fazla harcama yapmıştır. Bu girişim başarılı olmuş ve ABD'deki birçok kamu kurumunun web sitesi ülke genelinde en çok ziyaret edilen web siteleri arasında yer almıştır. Bkz. Andrew Chadwick, Internet Politics: States, Citizens and New Communication Technologies, New York 2006 ("*Chadwick*"), s. 177 vd.

dır. Türkiye'de e-devlet sisteminin kurulması, işletilmesi ve yönetilmesi görev ve sorumluluğu Başbakanlık adına Ulaştırma Bakanlığı'nca gerçekleştirilmektedir[54].

İnternet aynı zamanda insan hakları aktivizminin en etkin araçlarından birisidir[55]. İnsan hakları örgütleri, dünyanın farklı noktalarından yayın yapan web siteleri sayesinde devletlerin insan hakları ihlalleri takip ederek ve ihlallere karşı eyleme geçilmesi için kamuoyu oluşturarak dünyanın farklı noktalarındaki bireyler arasında işbirliği oluşturmaktadır.

Türkiye İstatistik Kurumu'nun yayınlamış olduğu Hanehalkı Bilişim Teknolojileri Kullanımı Araştırmasına göre Türkiye'de İnternet, en çok "iletişim, bilgi arama ve çevrimiçi hizmetler, mal ve hizmet siparişi vermek ve satmak, bankacılık, kamu kurumlarıyla iletişim, eğitim ve sağlık" gibi amaçlarla kullanılmaktadır[56].

V. Yeni nesil İnternet: Web 2.0

İnternetin kullanım alanlarının artmasıyla birlikte web siteleri etkileşimli uygulamalarını artırmıştır. Kullanıcı etkileşimini artırarak İnternetin etkinliğini en üst düzeye çıkarmak için çeşitli teknolojiler geliş-

[54] Bu yetki 20.04.2006 t. ve 26145 sayılı RG'de yayımlanarak yürürlüğe giren, 24.03.2006 t. ve 2006/10316 sayılı Bakanlar Kurulu Kararıyla Ulaştırma Bakanlığı'na verilmiştir. Bu hizmetler anılan Bakanlar Kurulu kararı ve 10.08.2006 t. ve 26255 sayılı RG'de yayımlanan, 2006/22 sayılı Başbakanlık Genelgesi gereği Türksat Uydu Haberleşme Kablo TV ve İşletme A.Ş. tarafından yürütülmektedir. Bkz. Devletin Kısayolu, https://www.turkiye.gov.tr; 58. Hükümet tarafından hazırlanan Acil Eylem Planı'nda e-Dönüşüm Türkiye Projesi'ne yer verilmiş, söz konusu projenin koordinasyonu, izlenmesi, değerlendirilmesi ve yönlendirilmesi ile ilgili olarak DPT Müsteşarlığı görevlendirilmiştir. Bu görevin yerine getirilmesi amacıyla DPT bünyesinde Bilgi Toplumu Dairesi Başkanlığı kurulmuştur. Ayrıca, 27 Şubat 2003 tarihinde yayımlanan 2003/12 sayılı Başbakanlık Genelgesi ile e-Dönüşüm Türkiye Projesi'nin amaçları, kurumsal yapısı ve uygulama esasları belirlenmiştir. Bkz. DPT - Bilgi Toplumu Dairesi Başkanlığı, http://www.bilgitoplumu.gov.tr/edtr.asp.

[55] İnternetin insan hakları mücadelesinde nasıl etkin bir şekilde kullanıldığına ilişkin örnekler için bkz. Stewen Hick/Edward F. Halpin/Eric Hoskins, Human Rights and the Internet, New York 2000 ("*Hick/Halpin/Hoskins*"), s. 41 vd.

[56] Hanehalkı Bilişim Teknolojileri Kullanımı Araştırması, http://www.tuik.gov.tr/PreIstatistikTablo.do?istab_id=46.

tirilmiştir. Web 2.0 yüksek etkileşimli yeni nesil İnternet teknolojilerinin genel adıdır[57]. Kavram temel olarak web sitelerinin sağladıkları kullanıcı katılımını ifade etmektedir. Web 2.0 teknolojileri kullanıldığında kullanıcılar yorum yazarak, resim göndererek veya bizzat içerik oluşturarak içeriğin bir parçası olmaktadır. Diğer bir deyişle, Web 2.0 teknolojileri verinin akış yönünü değiştirmekte ve her bir kullanıcı edilgen olmaktan çıkarak birer içerik sağlayıcı haline gelmektedir.

Web 2.0 teknolojinin temel taşları Extensible Markup Language ("XML") ve Rich Site Summary ("RSS") gibi etiket programlama dilleridir. Bu diller web siteleri arasında otomatik içerik değişimi yapılmasını mümkün kılmaktadır. Örneğin, bir içerik sağlayıcısı kendi web sitesini güncellediğinde, güncellemiş olduğu içerik anında o web sitesinin XML veya RSS servisine abone olmuş tüm web sitelerinde görünmektedir. Bu şekilde, içerik otomatik olarak milyonlarca web sitesinde anında yayınlanabilmektedir. Web 2.0 teknolojilerinin hızlı ve çoğu zamanda ücretsiz kullanılması bilgi kirliliğini beraberinde getirmektedir. Ayrıca bir bilgi sahibi tarafından düşünülmediği bir biçimde İnternet üzerinden dolaşıma girebilmektedir[58]. Bu durum baş edilemez fikri mülkiyet ihlalleri de ortaya çıkarmaktadır.

---

[57] What Is Web 2.0, http://www.oreillynet.com/lpt/a/6228, Makalenin çevirisi için bkz. Web 2.0 Nedir?, http://turk.internet.com/haber/yazigoster.php3?yaziid=14394.

[58] Simon Shurville, Readings in Technology in Education: Selected Papers from the International Conference on Information and Communications Technology in Education 2006, Bradford 2007 ("*Shurville*"), s.155.

§ 3. ERİŞİM ENGELLEME YÖNTEMLERİ

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

Web sitelerine erişimin engellenmesi için kullanılan tek bir yöntem yoktur. Engellemenin kapsamı, kullanılan teknik, engelleme süresi, engelleme öncesi ve sonrası takip edilen süreç devletten devlete değişmektedir. Her şeyden önce, devletlerin kullandıkları yöntemler teknolojik gelişmişlikleriyle doğrudan bağlantılıdır. Nihayetinde, erişim engelleme tekniklerinin uygulanmasının külfetli altyapı yatırımları gerektirdiği için devletlerin ekonomik gelişmişlikleri de diğer bir faktör olarak ortaya çıkmaktadır. Ayrıca kullanılacak yöntem, erişim engellemenin hangi düzeylerde gerçekleştirilmesi istendiğine, diğer bir deyişle, engellemenin dozajına göre de değişmektedir. Bazı devletler tek yöntem kullanırken, bazı devletler birden çok yöntemi kombine şekilde 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.

I. Engellemenin kapsamına göre

Web sitelerine erişim İSS'ler nezdinde ayrı ayrı engellenebileceği gibi ana İnternet omurgası üzerinden tüm 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.

A. İSS temelli engelleme

İSS temelli engelleme yönteminde, web sitelerinin ülke genelinde faaliyet gösteren her bir İSS nezdinde ayrı ayrı engellenmesi sağlanmaktadır[59]. Engelleme kararları karar mercileri tarafından icra edilmek üzere İSS'lere gönderilmekte ve kararlar İSS'ler tarafından kontrolleri altındaki ağ üzerinde uygulanmaktadır.

Erişim engellemesinin etkili olabilmesi için, erişim engelleme kararının tüm İSS'ler tarafından aynı anda ve aynı tekniği kullanarak uygulanması gerekmektedir. Bu sebeple bu yöntem ülke genelinde az sayıda İSS'nin faaliyette bulunduğu veya tüm sektörün devlet tekelinde olduğu ülkelerde etkin bir şekilde kullanılabilmektedir.

Engelleme her bir İSS nezdinde ayrı ayrı uygulanması bürokratik bir süreç gerektirdiği için engelleme kararlarının İSS'ler tarafından geç veya hiç uygulanmaması riskini ortaya çıkarmaktadır[60]. Bu da farklı İSS'ler kullanan İnternet kullanıcıları nezdinde eşitsizlik doğurabilmektedir. Örneğin, bir İSS'ye bağlı kullanıcılar birçok web sitesine erişim engelleme sebebiyle ulaşamazken, kararları icra etmede geciken İSS'ye bağlı kullanıcılar erişimleri engellenme kararı alınmış web sitelerini ziyaret edebilmektedir.

Benzer bir şekilde, İSS'ler tarafından erişim engellemesi için farklı teknikler kullanması engellemenin etkinliğinin ülke genelinde farklılaşmasına sebep olacaktır. Erişim engelleme teknolojileri ne kadar hızlı gelişiyorsa, engellemeleri aşacak teknolojiler de aynı hızda gelişmektedir.

[59] *Deibert/Palfrey/Rohozinski/Zittrain*, a.g.e., s. 12.

[60] *Deibert/Palfrey/Rohozinski/Zittrain*, a.g.e., s. 34.

Bu sebeple, İSS'lerin erişimi etkin bir şekilde engelleyecek ve kolay aşılamayacak teknolojileri kullanması gerekmektedir. Ülke genelinde her İSS'nin farklı gelişmişlikte teknolojiler kullanması, kararların geç uygulanmasında olduğu gibi kullanıcılar arasında eşitsizlik doğuracaktır.

B. İnternet omurgası temelli engelleme

Web sitesi engelleme için kullanılan diğer bir yöntem ise web sitesinin ana İnternet omurgası üzerinden engellenmesidir[61]. Erişim engellemesi doğrudan ülke genelindeki ana İnternet ağına işlenmekte ve bu şekilde ISS'lerden bağımsız bir şekilde web sitesine tüm ülke genelinde erişim engellenmektedir. Bu yöntem sayesinde, tüm ülke genelinde aynı anda ve seviyede web sitelerinin erişimi engellenmektedir.

İnternet omurgası üzerinde koyulan engellemeler bazen beklenmedik sorunlara da yol açabilmektedir. Pakistan devleti her türlü erişim hem İSS hem de ana İnternet omurgasında engellemektedir. 26 Şubat 2008 tarihinde Pakistan Hükümeti, İslam aleyhtarı videolar sebebiyle Youtube sitesinin erişimini engellemiştir[62]. Ancak engelleme sırasında yapılan bir hata sebebiyle dünya genelindeki ana İnternet omurgasında teknik bir problem ortaya çıkmış ve dünya genelindeki ağların üçte ikisi etkilenerek Youtube sitesine dünya genelinde belirli bir süreyle erişilememiştir.

II. Engelleme sürecine göre

A. Doğrudan engelleme

Doğrudan engelleme durumunda, web siteleri herhangi bir ihtar olmadan doğrudan engellenmektedir. Bu yöntem, özellikle içeriğin suç teşkil ettiği ve içeriğin yayında kalmasının zararı artırdığı durumlarda başvurulmaktadır. Ayrıca hem içerik hem de erişim sağlayıcının yurtdışında bulunması durumunda özellikle tercih edilmektedir. Diğer bir deyişle,

---

[61] *Deibert/Palfrey/Rohozinski/Zittrain*, a.g.e., s. 12.

[62] Pakistan lifts the ban on YouTube, http://news.bbc.co.uk/2/hi/technology/7262071.stm.

web sitesiyle ilgili ülkede herhangi bir muhatabın olmadığı durumlarda bu engelleme yöntemine başvurulmaktadır.

B. Uyar-kaldır yöntemiyle engelleme

Uyar-kaldır yönteminde adli veya idari bildirimler hukuka aykırı veya zararlı içeriğin kaldırılması için içerik sağlayıcıya veya somut olayın özelliklerine göre servis sağlayıcıya ihtarda bulunmaktadır. İçeriğin, içerik sağlayıcı veya erişim sağlayıcı tarafından belirli süre içerisinde kaldırmaması durumunda erişim engelleme kararı gündeme gelmektedir. Tüm bu süreç içerisinde, içerik veya erişim sağlayıcılar erişim engelleme kararı uygulanmadan kamu görevlileri ile müzakere etme fırsatı bulabildikleri için, kendilerini savunabilmekte ve olası bir erişim engelleme kararının olumsuz etkilerini bertaraf edilebilmektedir[63]. Öte yandan, bu yöntem ancak içerik veya erişim sağlayıcıdan en az birinin yurt içinde bulunması durumunda etkili olarak kullanılabilmektedir.

III. Engelleme süresine göre

A. Geçici engelleme

Bir web sitesinin erişimi, tedbir amaçlı geçici olarak engellenmesi mümkündür. Bu yola, hukuki bir ihtilafın varlığında ihtiyati tedbir olarak veya bir suçun varlığı durumunda 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[64]. Koruma tedbirleri, suç şüphesinin ortaya çıkmasıyla yargılama yapılarak kesin hükme varıncaya kadar yargılamanın sağlıklı işlemesini temin edecek tedbirlerdir[65]. Koruma tedbir-

[63] Yaman Akdeniz/Kerem Altıparmak, İnternet: Girilmesi Tehlikeli ve Yasaktır, Ankara 2008 (*"Akdeniz/Altıparmak"*), s. 35.

[64] Baki Kuru/Ramazan Arslan/Ejder Yılmaz, Medeni Usul Hukuku, 16. Baskı, Ankara 2005 (*"Kuru/Arslan/Yılmaz"*), s. 694.

[65] Nurullah Kunter/Feridun Yenisey/Ayşe Nuhoğlu, Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku, 14. Bası, İstanbul 2006 (*"Kunter/Yenisey/Nuhoğlu"*), s. 753.

lerine başvurularak, haklı görünüşe öncelik verilerek, henüz ortada kesin bir hüküm olmadan temel hak ve hürriyetlere müdahale edilmektedir[66].

Web sitelerinin erişimi bazen ihtiyati bir tedbir veya koruma tedbiri olmaksızın politik sebeplerle ülke genelinde geçici olarak kapatılabilmektedir. Örneğin, 2005 yılında Nepal kralı Parlamentoyu feshettikten sonra telefon hatlarını iptal ederek ve cep telefonu operatörlerini kapatarak İnternet erişimini ülke genelinde engellemiştir[67]. Diğer yandan, web sitelerinin erişimi web sitesi yöneticileri üzerinde baskı kurmak için de kapatılabilmektedir. İran, New York Times gazetesinin web sitesinin erişimini gazetenin yayınlarından memnuniyetsizliğini vurgulamak için sadece bir günlüğüne engellemiştir[68].

B. Kalıcı engelleme

Bir web sitesinin içeriğinin hukuka aykırılığı bir mahkeme kararıyla tespit edilmesi üzerine web sitesinin erişimi kalıcı olarak engellenebilmektedir. Ancak bazı durumlarda, geçici bir tedbir olarak başvurulan koruma tedbirleri kalıcı engellemeye sebep verebilmektedir[69]. İhtiyati tedbir kararları alındıktan sonra zamanında dava açılmaması sebebiyle kararlar kendiliğinden hükümsüz hale geleceği için karar gereğince erişimi engellenmiş web sitelerinin erişiminin tekrar açılması gerekmektedir. Aynı şekilde, ceza yargılamasının ortadan kalkmasıyla koruma tedbirleri olarak alınmış erişim engellemenin de kaldırılması gerekmektedir. Çoğu zaman bürokratik sebeplerle web siteleri üzerindeki engellemeler kaldırılmamaktadır.

Başka bir ülkede erişimleri engellenen web siteleri ise, erişim kaldırılması için o ülkedeki itiraz mekanizmalarını işletmenin ekonomik külfeti sebebiyle engellemeleri kaldıramamaktadır. Özellikle web sitelerinin farklı ülkeler tarafından engellendiği durumlarda bu külfet daha da artmaktadır. Dolayısıyla, web sitelerinin erişimleri belirsiz bir süreye

[66] *Kunter/Yenisey/Nuhoğlu*, a.g.e., s. 753

[67] Nepal: Internet Down, Total Censorship Imposed, http://www.nartv.org/2005/02/03/nepal-internet-down/.

[68] *Deibert/Palfrey/Rohozinski/Zittrain*, a.g.e., s. 18

[69] *Akdeniz/Altıparmak*, a.g.e., s. 69.

kadar engellenmiş olmaktadır. Yanlışlıkla web siteleri engellenen site sahipleri ise yaptırıma uğrama korkusu yüzünden itiraz mekanizmalarına işletmekten çekinebilmektedir. Bu da web sitelerinin kalıcı olarak engellenmesine sebep olmaktadır.

IV. Engelleme sistemine göre

A. Otomatik engelleme

Otomatik engelleme yönteminde, sakıncalı görülen içerik ve web siteleri için ulusal bir veritabanı oluşturulmakta ve web sitelerinin bu veritabanı referans alınarak erişim noktalarında otomatik olarak engellenmesi sağlanmaktadır[70]. Veritabanın içeriği doğrudan devlet tarafından oluşturulabileceği gibi özel sektörden de temin edilmesi mümkündür. Devletler, özellikle kaynak ve zaman tasarrufu yapmak için filtreleme yazılımı yapan şirketlerin hazırladıkları veritabanlarını referans alabilmektedir.

Veritabanları kamu görevlileri tarafından düzenli aralıklarla kamu kurumları, okullar, kütüphaneler veya İnternet kafeler gibi İnternet toplu kullanım sağlayıcılarına gönderilmekte ve veritabanındaki sitelerin bu sağlayıcılar nezdinde engellenmesi sağlanmaktadır. Ayrıca, bazı devletler bu listelerde belirtilen sakıncalı web sitelerinin İSS'ler tarafından otomatik olarak engellenmesini de zorunlu tutabilmektedir. Kamu görevlileri yaptıkları denetimlerle veritabanlarının aktif olarak kullanılıp kullanılmadığını ve güncelliklerini ayrıca kontrol etmektedir.

Bu yöntemin kullanılmasının çeşitli sakıncaları bulunmaktadır. Erişim, ana İnternet omurgası veya İSS temelli engellenmedikleri durumlarda, web siteleri sadece kamu kurumları veya İnternet kafeler gibi sınırlı alanlarda engellendikler için web sitesi sahipleri bu tür engellemelerden haberdar dahi olamamaktadır[71]. Öte yandan, özellikler listelerin özel şirketler tarafından hazırlanarak kullanıldığı durumlarda veritabanın

[70] *Deibert/Palfrey/Rohozinski/Zittrain*, a.g.e., s. 38.

[71] *Akdeniz/Altıparmak*, a.g.e., s. 49.

denetimi mümkün olmadığı için engellemeler keyfiliğe yol açmaktadır. Bu tür durumlarda, engellenecek web siteleri için son kararı devlet yerine özel şirketler tarafından vermiş olmaktadır.

B. Bireysel engelleme

Bireysel engelleme yönteminde her bir web sitesi için ayrı ayrı engelleme kararı alınmaktadır. Alınan kararlar mahkemeler veya kamu yetkililerince icra edilmek üzere ülke genelinde faaliyet gösteren her bir İSS'ye gönderilmektedir.

V. 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, bazı devletler farklı katmanlardan oluşan kombine teknikler kullanmaktadır. Engelleme tekniklerinin etkin olması için engellemenin ülke genelindeki İnternet trafiğinin tüm çıkış noktalarında uygulanması gerekmektedir.

Erişim engellemede yüzde yüz başarılı bir teknik bulunmamaktadır[72]. Erişim engelleme amacıyla kullanılabilecek her bir tekniğin kendine özgü güçlü ve zayıf tarafları vardır. Dünyanın en gelişmiş erişim engelleme sistemlerine sahip olan Çin ve Suudi Arabistan devletleri bile birçok içeriği engellemede çaresiz kalmaktadır. Bu sebeple devletler kullandıkları teknolojinin mükemmel olmasından öte etkili olmasına önem vermektedir[73].

Her bir teknik engelleme sebebiyle ilgisiz web sitelerini engelleme şeklinde aşırı engelleme riski ile ilgili web sitelerini engelleyeme şeklinde etkisiz engelleme riski taşımaktadır[74]. İnternet içeriğinin hızla değişmesi ve içeriğin değişik web sitelerine yayılması çoğu zaman engellemeyi imkânsız kılmaktadır. Bu sebeple, kullanılacak tekniğin etkinliği engel-

[72] *Deibert/Palfrey/Rohozinski/Zittrain*, a.g.e., s. 34.

[73] *Goldsmith/Wu*, a.g.e., s. 103.

[74] *Deibert/Palfrey/Rohozinski/Zittrain*, a.g.e., s. 66.

lenecek somut web sitesinin özelliklerine göre değişmektedir. Aşağıda, yaygın olarak kullanılan erişim engelleme teknikleri yer almaktadır.

A. IP engellemesi

Web siteleri temel olarak IP adresi üzerinden İnternet üzerindeki yerleri konumlandırılır[75]. En temel erişim engelleme yöntemi web sitelerinin barındığı sunucuların IP adreslerini engellemektir. Kapsam bakımından tercih edilecek yönteme göre ya her bir İSS nezdinde ya da ana İnternet omurgasında web sitesinin IP adresinin engellenmesi sağlanmaktadır. IP engelleme sistemi için ek bir donanım yatırımına gerek yoktur. Çoğu zaman, erişim engelleme için devlet tarafından İSS'lere bir teknik zorunlu kılınmamaktadır. Bu sebeple, İSS'ler ek bir donanım yatırımına gerek olmadığı için en ucuz engelleme yöntemi olan IP engellemesi tekniğini tercih edebilmektedir[76].

IP engellemesi tekniği başlıca iki nedenden dolayı etkin bir erişim engelleme tekniği olmaktan uzaktır. Yukarıda belirtildiği üzere, bir sunucunun birden fazla web sitesini barındırması mümkündür. Bu sebeple, hukuka aykırı veya zararlı içerikli bir web sitesine erişimin engellenmesi durumunda aynı sunucuda barınan masum diğer tüm sitelerde otomatik olarak engellenmekte ve temel bir ceza hukuku ilkesi olan ceza sorumluluğunun şahsiliği ilkesi ihlal edilmektedir[77]. Zira böyle bir engelleme sebebiyle bir web sitesindeki içerik sebebiyle aynı IP adresini paylaşan tüm web siteleri cezalandırılmaktadır.

Erişimi engellenen web sitesinin barındırıldığı sunucusu değiştirildiğinde web sitesinin IP adresi de değişeceğinden erişim engellemesi de otomatik olarak ortadan kalkmaktadır. Bazı durumlarda, sunucu değiştirmeye bile gerek olmadan IP değişikliğine gitmek teknolojik olarak mümkündür. Tüm bu sebeplerle IP engelleme yöntemi somut engellenecek web sitesinin özellikleri göz önüne alınarak diğer yöntemlerle kombine şekilde kullanıldığı takdirde etkin olacaktır.

---

[75] *Canbay*, a.g.e., s. 16.

[76] *Deibert/Palfrey/Rohozinski/Zittrain*, a.g.e., s. 14.

[77] 5237 sayılı TCK, m. 20.

Öte yandan, IP engellemesi bir web sitesinin tüm servislerini erişime kapatmaktadır. İnternet kullanıcıları siteyi ziyaret edemediği gibi web sitesinin e-posta servisleri de kullanılamaz hale gelir. IP engellemesinin servis temelli olarak yapılması teknolojik olarak mümkündür[78]. Her bir İnternet servisinin kendine özgü "port" olarak adlandırılan bir alt-bağlantı numarası vardır[79]. Web trafiği temel olarak 80 numaralı port üzerinden yayın yaparken, e-posta servisleri Simple Mail Transfer Protocol ("STMP") protokolü üzerinden 25 numaralı portu kullanmaktadır. Sadece 80 portu üzerinde yapılacak bir sınırlama ile web trafiği engellenirken, web sitesinin diğer temel servisleri kullanmaya devam etmesi sağlanabilir. Belki de bu şekilde, erişim engellemenin özellikle iletişim özgürlüğü üzerinde ortaya çıkardığı ağır sonuçlarının kısmen hafifletilmesi mümkün olacaktır.

B. DNS engellemesi

Web sitelerine erişim için kullanılacak IP adreslerinin hatırlanmaları zor olduğu için Domain Name System ("DNS") alan adı sistemi geliştirilerek, IP adresleri yerine geçen alan adı olarak adlandırılan harf dizilerinin kullanılmasını sağlamıştır. Örneğin, bu sistem sayesinde 72.14.235.104 IP numaralı sunucuda barındırılan Google arama motoru içeriğine www.google.com yazmak suretiyle erişmek mümkün olmaktadır.

DNS sistemi hiyerarşik şekilde yapılanmıştır[80]. Alan adı için en üst düzey yönetim A kök sunucusu tarafından gerçekleştirilmekte ve diğer 12 kök sunucu A kök sunucusu değerlerini referans almaktadır. Kök sunucuların altında jenerik ("generic")[81], ülke kodlu ("country code")[82] ve

[78] *Deibert/Palfrey/Rohozinski/Zittrain*, a.g.e., s. 59.

[79] İnternet servislerinin kullandıkları port numarları için bkz. Port Numbers, http://www.iana.org/assignments/port-numbers.

[80] *Von Arx*, a.g.e., s. 2.

[81] Jenerik üst-düzey alan adları herhangi bir ülkeye veya bölgeye bağlı olmaksızın evrensel olarak kullanılmaktadır. En yaygın olarak kullanılan jenerik üst-düzey alan adları uzantıları com ("commercial"), net ("network") ve org ("organisation") uzantılarıdır. Daha fazla bilgi için bkz. *Canbay*, a.g.e., s. 4.

[82] Her bir ülke kodlu üst-düzey alan adı uzantısı bir ülke ile ilişkilendirilmiştir. Örneğin, ABD "us", Çin "cn", Almanya "de", Fransa "fr", Türkiye "tr" uzantısını kullanmaktadır.

altyapı ("infrastructure") göre ayrılmış üst-düzey alan adları ("Top Level Domains") vardır[83]. Alan adları "ilk gelen alır" prensibine göre bireylere veya kurumlara tahsis edilmektedir[84]. Ülke kodlu uzantılar için ise devletlerin bazı sınırlamalar koyması mümkündür.

DNS engelleme tekniğinde alan adı tüm alt içeriği ile birlikte erişime kapatılmaktadır[85]. Kullanıcı web sitesine girmeye çalıştığında alan adlarının IP çözümlemesi yapan DNS sunucusu engellenmesi istenen web sitesinin çözümleme yanıtını yanıtsız bırakır. Bu şekilde siteye erişim engellenmiş olur. Her bir İSS nezdinde uygulanacak DNS engellemesi yöntemi sayesinde, kullanıcı erişim sorgusunun İnternet trafiğine ulaşmadan önce sorgunun engellenmesi ve bu şekilde ağ trafiğinin hafifletilmesi de mümkün olmaktadır. Ayrıca, sisteme müdahale ederek alan adının istenmeyen bir IP adresine de gönderilmesi mümkündür.

DNS engellemenin en büyük dezavantajı IP engellemesinde olduğu gibi alan adını tüm alt içeriği ile birlikte erişime kapatmasıdır. Dünya çapında yayın yapan ve milyonlarca İnternet kullanıcısına ücretsiz blog, e-posta veya benzeri hizmetler veren web sitelerinin engellemesi bazen engellemenin sonuçlarını ağırlaştırabilmektedir. Örneğin, T.C. Diyarbakır 1. Sulh Ceza Mahkemesi 20 Ekim 2008 tarihinde popüler blog servisi www.blogger.com web sitesinin erişimini www.justin.tv adlı web sitesinin yayınladığı

Türkiye'nin "tr" alan adı uzantısı 1990 yılından 2008 yılına kadar ODTÜ bünyesinde bulunan Nic.tr Yönetimi tarafından yönetilmiştir. ODTÜ yönetimi döneminde ülkemizde alan adları ile ilgili yasal düzenleme veya devlet tarafından verilmiş özel bir yetki bulunmamaktaydı. Bu sebeple, ODTÜ'nün yapmış olduğu işlemlerin hukuki dayanağı bulunmadığı iddia edilmekteydi. 10.11.2008 tarihinde yürürlüğe giren 5809 sayılı Elektronik Haberleşme Kanunun 35. maddesi "İnternet alan adlarının tahsisini yapacak kurum veya kurulusun tespiti ile alan adı yönetimine ilişkin usul ve esasları belirleme" görev ve yetkilerini Ulaştırma Bakanlığı'na vermiştir. Ulaştırma Bakanlığı 03.03.2009 tarihli ve 321 sayılı kararı ile "İnternet Alan Adları" tahsisine ilişkin iş ve işlemlerin yürütülmesi hususunda Bilgi Teknolojileri ve İletişim Kurumu'nu ("BTK") yetkilendirmiştir. Bu şekilde Türkiye'de alan adları yönetimi hukuki bir zemine kavuşmuştur. ODTÜ'ye yönelik eleştiriler için bkz. *Canbay*, a.g.e., s. 155; BTK hakkında daha fazla bilgi için bkz. aşa. §6 I A.

[83] Tüm uzantılar için bkz. Top-Level Domains ("gTLDs"), http://www.icann.org/en/tlds/.

[84] *Canbay*, a.g.e., s. 19.

[85] *Deibert/Palfrey/Rohozinski/Zittrain*, a.g.e., s. 60.

LigTV maçlarının bir blog üzerinden sunulmasından dolayı engellemiştir[86]. Site üzerindeki engelleme yasaktan dört gün sonra delil yetersizliğinden dolayı kaldırılmıştır. Blogger.com sitesi kullanıcılarına alt-düzey alan adı ("subdomain") olarak ücretsiz blog kurmalarına izin vermektedir. Sitenin bu şekilde yapılanması sayesinde, kullanıcı blogları içerik olarak birbirinden bağımsız bir şekilde yayınlarını sürdürmekte ve hukuka aykırı içerik ortaya çıktığında sadece o kullanıcıya ait blogun kapatılması mümkün olmaktadır. Buna rağmen Mahkeme ilgili blogları kapamak yerine tüm web sitesinin erişimini engellemiştir. Bunun sonucunda, masum milyonlarca blog da otomatik olarak engellenmiştir. Diğer bir deyişle, birden fazla web sitesini barındıran sunucu üzerinde IP engellemesinde olduğu gibi ceza sorumluluğunun şahsiliği ilkesi ihlal edilmiş olmaktadır.

Öte yandan, bir web sitesinin ülke kodlu üst düzey alan adını engellemesiyle o ülkede barındırılan web sitelerinin engellenmesi birbirinden farklı durumlardır. 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. Ancak ülke kodlu üst düzey alan adlarının o ülkenin vatandaşları tarafından kullanılması gibi zorunluluklar getirilebilmektedir[87].

C. URL engellemesi

Uniform Resource Locator ("URL"), İnternette resim, yazı veya müzik gibi bir kaynağa karşılık gelen standart bir formata uygun bir karakter

[86] T.C. Diyarbakır 1. Sulh Ceza Mahkemesi 20.10.2008 tarih ve 2008/2761 sayılı kararıyla erişim engellenmiştir. Bkz. *Akdeniz/Altıparmak*, a.g.e., s. 43; Süreç hakkında daha fazla bilgi için bkz. Blogger.com, http://tr.wikipedia.org/wiki/Blogger.com.

[87] ABD, "us" uzantısının sadece ABD vatandaşları tarafından kullanılmasını öngörmektedir. Ayrıca, alan adının tescil edilebilmesi için başvuruda bulunanın fiziki adresini doğrulaması talep edilmektedir. ABD bu şekilde kişilerin fiziksel adreslerini sanal adresleriyle birleştirmeyi amaçlamaktadır. Daha fazla bilgi için bkz. *Zittrain*, a.g.e., s. 5.

dizgisidir. URL İnternet üzerindeki bir kaynağın koordinatıdır. Pratik bir anlatımla URL, İnternette gezinirken herhangi bir kaynağa tıklandığında tarayıcının adres çubuğunda görünen adrestir.

URL engellemesi koordinatları bilinen hukuka aykırı veya zararlı belirli bir içeriğin engellenmesi amacıyla kullanılan bir tekniktir[88]. Bu yöntemin en önemli avantajı, hukuka aykırı veya zararlı bir içerik için tüm web sitesinin içeriğinin engellenmesini önlemesidir.

D. Proxy engellemesi

Proxy İnternette içeriğine erişim için kullanılan bir ara sunucudur. Proxy sunucuya daha çok İnternetteki bir içeriğe doğrudan bağlanmak istenilmediği durumlarda başvurulmaktadır[89]. Proxy kullanmanın çeşitli avantajları bulunmaktadır. Proxy sunucu erişilmek istenen veriyi önbelleğine aldığı için kullanıcılar web sitelerine daha hızlı şekilde erişir ve gereksiz ağ trafiğinin kullanılmasının önüne geçer. Proxy sunucusu içerik ve kullanıcı arasında filtreleme görevi üstlendiği için kullanıcının istenmeyen içerikle veya virüs gibi zararlı programlarla karşılaşma riski ortadan kalkmaktadır. Ayrıca, proxy sunucular içerik ve kullanıcı arasında yer aldığından, asıl kullanıcının kimliğinin gizlenmesine olanak vermektedir. Sağladığı bu avantajlar sebebiyle, proxy sunucuları üniversiteler ve kütüphaneler gibi İnternetin ücretsiz ve ortak kullanıma açık olduğu alanlarda yaygın olarak kullanılmaktadır. Devletler proxy sunucularını İnternet bağlantı noktalarına konumlandırılarak web içeriğini filtreleyebilmekte ve bireylerin hangi web sitesine veya hangi tür içeriğe erişeceğini belirlemektedirler[90]. Bu şekilde proxy sunucuları erişim engellemesi amacıyla kullanılmaktadır.

E. İçerik engellemesi

IP ve DNS engellemesi teknikleri kullanılarak TCP/IP protokolü altında belirli bir noktaya gönderilen veya belirli bir noktadan alınan veri

---

88 *Deibert/Palfrey/Rohozinski/Zittrain*, a.g.e., s. 16.

89 Jonathan Bick, 101 Things You Need To Know About Internet Law, New York 2000 ("Bick"), s. 137.

90 *Deibert/Palfrey/Rohozinski/Zittrain*, a.g.e.,s. 61.

parçacıklarının engellenmesi sağlanmakta, veri içeriğine müdahale edilmemektedir. İçeriğe müdahale edebilmek için ağ sisteminin yazılımsal ve donanımsal olarak değiştirilmesi gerekmektedir[91]. Bu şekilde bir web sitesinin hem URL hem alan adı hem de içeriğine ağda otomatik olarak müdahale etmek mümkün olmaktadır.

Ağın belirli kuralları tanıyarak otomatik engelleme yapması fikir ve sanat eserlerinin dijital ortamda korunması için kullanılmakta olan Dijital Hak Yönetimi ("DRM")[92] sistemleriyle aynı prensiplerle çalışmaktadır. DRM sistemleri hem eserler üzerinde hakların dijital ortamda tanımlanmasına hem de bu hakka dayanarak eserin kullanım ve erişimini denetlemeyi sağlamaktadır[93]. DRM sistemleri nihayetinde birer ağ yazılımları oldukları için ağın kendisinin belirtilen sınırlamaları otomatik olarak tanıması ve ancak izin verilen türde verilerin akışına izin vermeleri sağlanmaktadır. Diğer bir deyişle bu sistem hukuk kurallarının fiziki ortamda uygulanmasında olduğu gibi sadece davranışı tespit etmekle yetinmemekte, ağdaki ihlalleri yaptırıma bağlamakta ve ayrıca bireyleri sürekli gözetleyerek oto-sansür uygulamalarını sağlamaktadır[94].

Daha önce açıklandığı üzere, routerlar içerik katmanına müdahale etmeksizin veri paketlerinin üzerlerinde yer alan etiket katmanını esas alarak veri iletimini gerçekleştirmektedir[95]. Veriler parça parça iletildiği için engellenecek içeriğin tespit edilebilmesi için paketlerin bir noktada birleştirilerek denetlenmesi gerekmektedir. Engellenmeyen içerik ise tekrar parçalara ayrılarak nihai iletim adreslerine iletilmesi gerekmektedir. Routerlar 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 olarak inceleme yapılması mümkün olmaktadır.

---

[91] *Deibert/Palfrey/Rohozinski/Zittrain*, a.g.e., s. 59.

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

[93] *Bayamlıoğlu*, a.g.e., s. 303.

[94] *Bayamlıoğlu*, a.g.e., s. 304.

[95] Bkz. yuk. §2 II.

Router programlama sisteminin farklı devletler tarafından kullanılması durumunda bir veri geçtiği her noktada hukuka uygunluk denetiminden geçirilmiş olmaktadır. Diğer bir deyişle, ağ tarafsızlığı ortadan kalkarak devletlerin kurallarını İnternet ağına yaymaları ve eşzamanlı icra etmeleri gibi bir durum ortaya çıkmaktadır[96]. Yapılan bir araştırmaya göre içerik engelleme dünya genelinde en çok ifade hürriyeti, insan hakları, reform, askeri kuvvetler, din, azınlık hakları, etnik köken, kadın hakları, ulusal güvenlik, tarih, sanat, edebiyat, cinsellik, ücretsiz yazılımlar, müstehcenlik, kumar, içki, uyuşturucu gibi konular için gündeme gelebilmektedir[97].

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 olarak muamele göreceklerdir. Benzer bir şekilde, cinsel hastalıklar konusunda bilgi veren bir sağlık sitesi de aynı tür bir engellemeye takılacaktır. Diğer taraftan, web sitelerinin içeriği şifreli olarak sunulduğu durumlarda, içerik engelleme sistemleri çaresiz kalmaktadır[98].

F. DDOS atakları

Bazen devletler, egemenlik alanları dışında kalan yabancı ağlarda barındırılan sitelerin erişimini tamamen engelleme ihtiyacı duyabilirler. Bu durum daha çok ülke genelinde erişim engellemenin gereken faydayı vermediği veya siyasi muhaliflerin veya terör örgütlerinin propagandalarını tamamen engelleme ihtiyacı duyulduğu zamanlarda gündeme gelebilmektedir. Örneğin, devlet siyasi muhaliflerin web sitelerini ülke genelinde erişimini engellemiş ve ülke genelinde web sitelerini etkisiz kılmıştır. Ancak, siteler dünya genelinde erişilir olduğu 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.

96 Ağ tarafsızlığı için bkz. *Bayamlıoğlu*, a.g.e., s. 340; *Preston*, a.g.e., s. 4.

97 *Deibert/Palfrey/Rohozinski/Zittrain*, a.g.e., s. 7.

98 Daha fazla bilgi için bkz. aşa. §4 I D.

DDOS, bilişim sistemlerini işlemez hale getirmek için kullanılan bir ağ saldırı yöntemidir[99]. DDOS atakları hem ağ sistemini çökertmek için 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 saldırı yapması asıl saldırı yapanın kimliğinim gizlenmesine yardımcı olur. Aynı anda binlerce bilgisayarlardan milyonlarca sorgu alan ağ veya sunucu bu sorgulara yanıt vermekle meşgul olur ve saldırı sonucunda ya ağ tamamen çöker ya da bağlantı hızı yavaşladığı için 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 saldırı yapabilirler. Binlerce bilgisayar içinden DDOS saldırılarının asıl faillerini tespit zor olduğu için DDOS saldırıları bazen devletler tarafından hukuka aykırı bir engelleme tekniği olarak kullanılabilmektedir. Örneğin, Kırgızistan'da gerçekleştirilen Şubat 2005 seçimleri sırasında tüm muhalif partilerinin web siteleri DDOS saldırısına uğramış ve erişilmez hale gelmişlerdir[100]. Muhalif partiler, bu saldırılardan dolayı iktidar partisini suçlamışlardır. Ancak belirtildiği üzere, bu tür saldırılarda failleri tespit etmek zor olduğu için bir neticeye varamamışlardır.

G. Alan adı terkin yöntemi

Alan adı terkin yöntemi erişimi engellenmek istenen web sitesinin ülke kodlu üst düzey alan adı kullandığı durumlarda başvurulabilecek bir engelleme tekniğidir. Her devlet kendi ülke kodlu üst düzey alan adını yönetmektedir. Bu doğrultuda iç hukuk kurallarına aykırı içerik taşıyan bir alan adının devlet tarafından terkin edilmesi mümkündür[101].

---

[99] 2007 Siber Suçluların ve DDOS Saldırıların Arttığı Yıl Oldu, http://turk.internet.com/haber/yazigoster.php3?yaziid=20166.

[100] *Deibert/Palfrey/Rohozinski/Zittrain*, a.g.e., s. 41.

[101] *Deibert/Palfrey/Rohozinski/Zittrain*, a.g.e., s. 64.

H. Fiziksel sunucu müdahalesi

İnternete bağlı her bir sunucunun fiziksel olarak bir yerde barındırılması gerekmektedir. Sunucu barındırma hizmetleri devletlerin denetimi altında gerçekleştirilmektedir. Bulunduğu ülkenin hukuk kurallarına aykırı içerik taşıyan bir web sunucusunun İnternet bağlantısı fiziksel olarak kesilerek içeriğe erişimin tamamen engellenmesi mümkündür[102].

I. Ağ hataları

Erişim engellemelerinde sık rastlanan diğer bir durum ise web sitesine erişilmeye çalışıldığında bağlantı hatası oluştuğunu gösteren mesajlarla karşılaşmaktır[103]. Bir siteye erişmeye çalıştıklarında ağ hatası oluştuğu hatasıyla karşılaşan ziyaretçiler, içerik ve hizmet sağlayıcılar siteye teknik bir sorundan dolayı erişilemediği yanılgısına düşmekte ve sitelerinin devlet tarafından engellendiğinin farkına dahi varamamaktadırlar. Özellikle, telekomünikasyon sektörünün devlet tekelinde olduğu ve dolayısıyla tüm İnternet ağının sadece devlet tarafından yönetildiği ülkelerde bu yöntem etkin bir erişim engelleme yöntemi olarak kullanılabilir. Nihayetinde, devlet tekeli yüzünden içerik veya hizmet sağlayıcıların elinde hatanın kesin çözümlenmesini sağlayacak ve ağda ayrıntılı inceleme yapacak yetkiler olmadığı için devlet müdahalesi ispatlanamamaktadır.

J. Sosyal teknikler

Devletler, bazı sebeplerden dolayı doğrudan engelleme kararı almak yerine, başkaca yöntemler kullanmak suretiyle sitelere erişimi fiilen zorlaştırmakta veya kullanıcıların oto-sansür uygulamalarını sağlamaktadır. Bu yöntemlerin etkinliğinin bireysel davranışlara dayanması sebebiyle sosyal teknikler olarak adlandırılmaktadır[104].

İnternetin etkin bir şekilde kullanılabilmesi için devletlerin İnternete bağlantı öncesi ve bağlantı sonrası sınırlamalarının asgari düzeyde

---

[102] *Deibert/Palfrey/Rohozinski/Zittrain*, a.g.e., s. 64.

[103] *Deibert/Palfrey/Rohozinski/Zittrain*, a.g.e., s. 16.

[104] *Deibert/Palfrey/Rohozinski/Zittrain*, a.g.e., s. 65.

olması gerekmektedir. Devletlerin İnternete kimlerin bağlanabileceğini belirlemesi veya İnternete bağlandıktan sonra bireylerin her adımını izlemesi bireyler üzerinde erişim engellemenin oluşturduğu aynı olumsuz sonuçları oluşturmaktadır. Ziyaret edilen her web sitesinin devlet tarafından kontrol edileceği düşüncesi bireyler üzerinde psikolojik baskı oluşturmaktadır.

İnternet kullanıcılarını en yoğun kontrol eden devlet Çin'dir[105]. Çin'de İnternete her bağlanıldığında, İnternette yapılan her şeyin kaydedildiğini ve kuralları ihlal edenlerin ihbar edilmesi gerektiğini belirten bir uyarı kullanıcılara gönderilmektedir. Bu şekilde, hem bireyler üzerinde psikolojik baskı oluşturulmakta hem de kullanıcıların devletin fark etmediği sakıncalı içeriği ihbar etmeleri sağlanmaktadır.

Takip konusunda Çin'den sonra en uç örneği Güney Kore oluşturmaktadır[106]. Güney Kore'de İnternet kablolu veya kablosuz olarak ülke genelinde hemen her noktada sunulmaktadır. Ancak bireylerin İnternete bağlanabilmesi için vatandaşlık bilgilerini sisteme tanıtmaları istenmektedir. Ayrıca, ziyaret edilen web sitelerinin tümümün kaydı İSS'ler nezdinde kaydedilmektedir. Vatandaşlık bilgileri ile İnternete bağlanan kişiler, girecekleri web sitelerine dikkat etmek zorunda kalmaktadırlar.

Öte yandan, İnternette web sitesi oluşturmak için bürokratik bazı aşamaların geçilmesini istemek veya sadece ülke üst düzey alan adı uzantılı sitelerin kullanılmasını zorunlu kılmak da erişim engellemeyle eşdeğer sonuçlar doğurmaktadır.

Devletler, yer sağlayıcıları ve erişim sağlayıcıları da çeşitli usullerde takip ve kontrol etmektedir. Birçok devlette erişim ve yer sağlayıcı olmak izin sistemine tabi tutulmuş ve izin düzenli olarak faaliyetlerini devlete bildirim şartına bağlanmıştır. Aynı doğrultuda, erişim ve yer sağlayıcıların hukuki ve cezai sorumlulukları farklı sorumluluk rejimlerine tabi kılınmıştır. Söz konusu aktörlerin sorumluluğun artırılması, erişim veya yer sağlayıcının müşterileri kabul ederken daha seçici davranmalarına

[105] Çin için bkz. aşa. §5 III.

[106] Güney Kore için bkz. aşa. §5 IV.

sebep olmaktadır[107]. Özellikle, otoriter rejimlerde, erişim ve yer sağlayıcılar kendilerini hukuki sorumluluk altına sokmamak için, ister istemez muhalif web sitelerini barındırmaktan çekinmektedirler. Forum sitelerinin yöneticileri de her türlü sakıncalı içerikleri hukuki sorumluluk altına girmemek için sistemden kendileri kaldırabilmektedir.

Benzer bir şekilde bazı web siteleri kullanıcıların hangi ülkeden İnternete bağlandığını ya IP dağıtım tabloları sayesinde kendileri tespit etmekte veya kullanıcıya siteye girişinde hangi ülkeden İnternete bağlandığını sorarak öğrenmektedir. Web sitesinde tespit edilen ülkeye özel sakıncalı bir içerik varsa, kullanıcının bu içeriğe erişmesi doğrudan site tarafından tamamen engellenmekte veya içeriğin sakıncalı olduğu kullanıcıya ihtar edilmektedir. Bu engelleme yöntemi ilk kez International League against Racism and Anti-Semitism ("LICRA") isimli sivil toplum örgütünün 2000 yılında Yahoo şirketi aleyhine Fransa'da açtığı davada gündeme gelmiştir[108]. LICRA, Yahoo online artırma sitesi üzerinden Nazi ürünlerinin satıldığı ve bu durumun her türlü Nazi eşyasının Fransa'da satışını yasaklayan Fransız hukuk kurallarına aykırı davrandığı gerekçesiyle Yahoo'ya davayı açmıştır. Yahoo şirketi Fransız mahkemesinin yetkisine itiraz etmiştir[109]. Ancak mahkeme, Yahoo şirketinin Fransız ziyaretçilerinin Nazi ürünlerini görüntülemesini engellemekle yükümlü olduğuna hükmetmiştir[110]. Yahoo her ne kadar Fransız mahkemesini yetkisiz kabul etse de Fransa'daki yatırımlarını riske atmamak için kararın gereğini yerine getirmek zorunda kalmıştır. Bu doğrultuda Yahoo, kullanıcılarının IP adreslerine bakarak ve kullanıcılardan da bulundukları

---

[107] *Deibert/Palfrey/Rohozinski/Zittrain*, a.g.e., s. 42.

[108] Yahoo Inc. v. L.I.C.R.A. and U.E.J.F., 169 F. Supp. 2d 1181 (N.D. Cal. 2001) (No. 00-21275) *Goldsmith/Wu*, a.g.e., s. 2; Ayrıca bkz. http://w2.eff.org/legal/Jurisdiction_and_sovereignty/LICRA_v_Yahoo/20040823_yahoo_v_licra-9th.pdf.

[109] Yahoo yetkilileri dava sırasında İnternete devletlerin müdahalesine ile ilgili çok temel bir soruna değinmişlerdir. Eğer Fransız hukuku Amerika'daki bir web sitesine uygulanabiliyorsa, aynı doğrultuda Alman ve Japon hukuku hatta Suudi ve Çin Hukuku da uygulanabilecektir. Bu durumda şirketlerin tüm vakitlerini uygulanacak hukuku tespit etmekle geçireceklerini ve ticaret yapamaz hale geleceklerini belirtmişlerdir. Bkz. *Goldsmith/Wu*, a.g.e., s. 2.

[110] *Goldsmith/Wu*, a.g.e., s. 61.

ülkeyi doğrulamalarını talep ederek Fransız ziyaretçilerin Nazi içeriğine erişimini zorlaştırmıştır.

Görülmektedir ki, sosyal tekniklerin etkinliği bireylerin bu konuda gösterdiği katılım ve dirence göre değişmektedir. Devletlerin engelleme politikaları bireyler üzerinde psikolojik etki yaratmaktadır. Nihayetinde devletler doğrudan engelleme yapmadıkları için ortaya çıkan durumdan dolayı sorumlu olmadıklarını ileri sürmektedir. Bu sebeple, kullanılan bu sosyal teknikler, başta ifade hürriyeti, özel hayatın gizliliği, iletişim özgürlüğü olmak üzere çeşitli temel hak ve hürriyeti ihlal etmektedir.

§ 4. ENGELLEME AŞMA YÖNTEMLERİ

Web sitelerinin erişimleri değişik teknikler kullanılarak engellenebildiği için engellemelerin aşılması uygulanan tekniğe göre değişiklik göstermektedir. Erişim engelleme yöntemleri kombine şekilde kullanıldığı gibi engelleme aşma yöntemleri de kombine şekilde kullanılabilmektedir.

I. Yaygın teknikler

A. IP değişikliği

Web sitesinin IP engelleme yöntemiyle engellendiği durumlarda, web sitesinin barındırıldığı sunucunun IP adresinin sunucu yöneticisi tarafından değiştirilmesi engellemeyi etkisiz kılacaktır. Sunucunun barındırma şirketini değiştirmeksizin salt IP değişikliğinin maliyeti düşük olmakla birlikte, sunucu ayarlarının yeni IP adresine göre yapılandırılması bazı teknik sorunlar oluşturabilmektedir.

Bireysel web sitesi sahipleri, erişimi engellenen web sitesi sahipleri sitelerini farklı bir barındırma şirketine taşımak suretiyle IP engellemesini aşabilecektir. Ancak, bunun için yeni barındırma şirketiyle yeni bir hizmet sözleşmesi yapmak zorunda kalacakları için engellemenin aşılması mali açıdan külfetli olacaktır.

Sosyal teknikler kısmında açıklandığı barındırma şirketlerinin faaliyeti birçok devlet tarafından izin sistemine tabi tutulmakta ve şirketlerin faaliyetleri kontrol edilmektedir. Barındırma şirketleri hem sunmuş oldukları hizmetin işlerliğinin engelleme sebebiyle etkilenmemesi için hem

de hukuki veya cezai sorumluluk altına girmemek için erişimi engellenmiş veya içeriği şüpheli web sitelerini barındırmaktan çekinebilmektedir.

B. DNS değişikliği

Web sitesinin İnternet kullanıcısı tarafından erişilebilmesi için, web sitesinin kullandığı alan adının kullanıcının İSS'nin DNS sunucusu tarafından çözümlenmesi gerekmektedir. DNS engellemesi bu çözümlemenin sonuçsuz kalmasını sağlamaktadır. Bu engellemeyi aşmak için kullanıcı nezdinde DNS ayarları değiştirilerek, kullanıcının ulaşmaya çalıştığı web sitesinin alan adının başka DNS sunucuları tarafından çözümlenmesi sağlanmaktadır[111]. Öte yandan, web sitesi sahipleri alternatif alan adları kaydetmek suretiyle olası bir DNS engellemesini bertaraf edebilmektedir[112]. Ancak, engellemeden sonra hedef kitlenin yeni alan adından bir şekilde haberdar edilmesi gerekmektedir.

C. URL gizleme

Bir içeriğin URL'si içerik sağlayıcı tarafından kolayca değiştirilebileceği için URL engellemesi en kolay aşılan engelleme tekniğidir. URL Masking olarak adlandırılan teknikler gerçek URL'nin gizlenmesini ve içeriğe birden fazla URL'den ulaşmayı olanaklı kılmaktadır[113]. Bu şekilde içerik bir URL'den erişilemezken, URL Masking tekniğiyle oluşturulmuş kopya URL'den erişilmektedir.

D. Proxy kullanımı

Proxy sunucular devletler tarafından erişim engelleme amacıyla kullanılabileceği gibi İnternet kullanıcıları tarafından engellemelerin aşılması amacıyla kullanılabilmektedir. Esasında içeriğe proxy sunucu erişir ve eriştiği içeriği İnternet kullanıcısına aktarır. Proxy sunucu başka bir ülkede yer aldığı için içeriğe engelsiz bir şekilde erişmektedir. Ayrıca,

[111] *Deibert/Palfrey/Rohozinski/Zittrain*, a.g.e., s. 67.

[112] Civisec - The Citizen Lab, Everyone's Guide to By-passing Internet Censorship: For Citizens Worldwide, Toronto 2007 ("*Civisec*"), s. 28.

[113] URL Forwarding and URL Masking Services, http://www.washington.edu/computing/web/publishing/url-forwarding.html.

içeriğe ilk elden proxy sunucusu eriştiği için İnternet kullanıcısı kimliğini gizleyebilmekte ve İnternette anonim olarak gezinebilmektedir[114]. Proxy sunucuların hem engellemeleri aşmak için hem de çeşitli suçlarda aracı olarak kullanılabildikleri için devletlerin sıkı takibine tabidirler.

E. İçerik aldatması

İçerik engellemesi tekniği kullanılarak gerçekleştirilen erişim engellemesini aşmak için çeşitli yöntemler kullanılmaktadır. Bu yöntemlerin başında içerik şifreleme yöntemi gelmektedir.

Şifreleme yöntemi basit bir teknik olmasına rağmen dünyanın en gelişmiş erişim engelleme sisteme sahip Çin devleti tarafından bile engellenememektedir. Bu teknikte web sitesinin ana temasını oluşturan anahtar kelimeler yerine ilgisiz kelimeler kullanılmakta ve bu şekilde web siteleri engellemeden kurtulmaktadır. Örneğin, Çinli bir insan hakları sitesinde demokrasi kelimesi yerine "lahana", çok partili sistem için ise "havuç" kelimesi kullanılmaktadır[115]. Bu yöntem devlet sansüründen kurtulmak için film ve kitapların isimlerini değiştirmek şeklinde kullanılagelen klasik bir yöntemdir. Her ne kadar bu teknik içerik engellemelerini bertaraf etmek için etkin olarak kullanılabilirse de hedef kitlenin bu teknikten bihaber olması düşüncelerin hedef kitleye ulaştırılamaması riskini doğurmaktadır[116].

İçerik aldatması içeriğin URL adresi veya doğrudan web sitesinin alan adı için de kullanılabilmektedir. Alan adları için "ilk gelen alır" ilkesi uygulandığı için, 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 "tag" kodları içinde ilgisiz kelimeler kullanılarak resimlerin de engelleme sistemleri tarafından algılanması engellenmektedir.

Bir diğer içerik aldatması yöntemi ise web sitesi içeriğindeki kelimelerin arasına rastgele gizli karakterler eklemektir. Örneğin, "demokrasi" kelimesi "de-m.okras,i" şeklinde yazılmakta ve kelime arasına eklenen ka-

[114] *Civisec*, a.g.e., s. 25.

[115] *Goldsmith/Wu*, a.g.e., s. 103.

[116] *Goldsmith/Wu*, a.g.e., s. 103.

rakterler 1 punto gibi çok küçük boyutlara küçültülerek gizlenmektedir. İnternet kullanıcısı kelimeyi "demokrasi" olarak okumakta, ancak erişim engelleme programı kelimeyi demokrasi olarak algılayamamaktadır.

F. Uzak masaüstü kullanımı

Mevcut işletim sistemleri, bilgisayarların uzak mesafeden İnternet üzerinden kontrol edilmesini mümkün kılmaktadır. Bu yöntem sayesinde, fiziksel erişimin olmadığı veya zor olduğu bilgisayarların tek bir noktadan kontrol edilmesine olanak vermektedir. Uzak masaüstü kullanıcısı bağlandığı bilgisayarın tüm servislerini sanki o bilgisayarın karşısındaymış gibi kullanabildiği için bu teknik erişimi engellenmiş web sitelerine ulaşmak için de kullanılabilmektedir. Proxy kullanımında olduğu gibi siteye erişine asıl bilgisayar uzaktan bağlanılan bilgisayar olduğu için İnternet kullanıcısı kimliği de gezinme sırasında gizlenmektedir.

G. Kopya içerik kullanımı

Web 2.0 teknolojilerinin yaygınlaşmasıyla, web sitelerinin etkileşimi artarak bir içerik çok kısa süre içerisinde birçok web sitesinde yayınlanabilmektedir. Bir web sitesinin erişimi engellendiğinde, web sitesi içeriği XML ve RSS kanallarından başka web sitelerine yayılarak, erişim engelleme kararının amacına ulaşması önlenebilmektedir. Kopya web sitelerinin sayısının milyonları bulması ve web sitelerinin otomatik olarak içeriklerini güncelleştirebilmeleri sebebiyle, bu tür web siteleriyle mücadele büyük çaba gerektirmektedir. Milyonlarca kopya web sitesi verinin kaynağını, bir suç işlendiği takdirde failini tespitini de imkânsızlaştırmaktadır. Bu tür bir girişimle karşı karşıya kalındığında devletler engellemenin seviyesi artırılarak ve farklı teknikleri kombine şekilde kullanarak söz konusu içerikle mücadele etmektedir.

H. Önbellek kullanımı

Arama motorları ve çeşitli siteler İnternet içeriğini çeşitli amaçlarla işlemek için kendi sunucularında saklamaktadır[117]. Bir web sitesine erişim

[117] Google arama motorunun bu şekilde bir hizmeti vardır. Bkz. Google Cached Pages: What Are Cached Pages?, http://www.googleguide.com/cached_pages.html; Önbel-

engellendiğinde, arama motoru veya ilgili sitenin önbelleğinde bulunan içerik etkilenmemektedir. Eğer ki web sitesi önbelleğe alınmışsa, ek bir yazılım veya başkaca bir yönteme başvurmaksızın erişim engelleme kararına rağmen sitenin içeriğine ulaşmak mümkün olmaktadır[118].

I. Online çeviri sistemleri

İnternette ücretsiz olarak sunulan birçok çeviri sitesi yer almaktadır. Google Translate, Babelfish gibi popüler çeviri siteleri bir web sitesini eşzamanlı olarak istenilen dile çevirebilmektedir. Çeviri içeriğin çeviri sitesinin önbelleğine alarak gerçekleştirilmekte ve içerik kullanıcıya önbellekten sunulmaktadır. Çeviri sitelerinin kullanılmasıyla erişimi engellenmiş bir web sitesinin içeriğine erişmek mümkün olmaktadır[119].

J. Trafik aktarımı

Bir diğer engelleme aşma tekniği ise trafik aktarım tekniğidir[120]. Trafik aktarımı proxy kullanımına benzemektedir. Bu teknik kullanılarak bilgisayarın tüm İnternet trafiğinin İnternet ağına başkaca bir sunucu aracılığıyla taşınması sağlanmaktadır. İnternet kullanıcısı proxy tekniğinde olduğu gibi farklı bir sunucu aracılığıyla İnternet ağına bağlanmış olduğu için engellemeleri de aşmış olmaktadır.

II. Değerlendirme

Erişim engelleme teknolojilerinin gelişmelerine paralel olarak engelleme aşma yöntemleri da aynı hızda gelişmektedir. Devletler, engelleme aşma tekniklerindeki gelişmeleri yakından takip etmektedirler. Diğer bir deyişle, devletler erişim engelleme amacıyla kullandıkları tekniklerin güçlü ve zayıf yönlerinin farkındadırlar. Dolayısıyla, bir web

lek konusunda popüler diğer bir web sitesi ise www.archive .org web sitesidir. Bu web sitesi 85 milyar web sitesini önbelleğinde tutmaktadır. Daha fazla bilgi için bkz. Internet Archive: Wayback Machine, http://www.archive.org/web/web.php.

[118] *Civisec*, a.g.e., s. 28.

[119] *Civisec*, a.g.e., s. 28.

[120] Trafik aktarma tünel tekniği olarak da anılmaktadır. Yaygın kullanılan trafik aktarım yazılımları için Bkz. *Civisec*, a.g.e., s. 19.

sitesine yönelik engellemenin kolay aşılabilir olması, devletlerin bilinçli bir tercihi olabileceği gibi devletin teknolojik yetersizliğinin bir sonucu da olabilmektedir. Bu sebeple, bazı engellemeler çok kolay aşılabilirken, bazı engellemeleri aşmak uzun soluklu bir çabayı gerekli kılabilmektedir.

Öte yandan engelleme aşma teknikleri gizli bilgiler değildir. Her erişim engelleme kararından sonra engellemenin nasıl aşılabileceği hem İnternette hem de basında geniş ayrıntılarıyla yer alabilmektedir[121]. Bu sebeple, erişim engelleme kararları çok kısa bir sürede etkinliklerini yitirebilmektedir. Erişim engelleme teknikleri bazen o kadar etkisiz olabilmektedir ki, erişim engelleme kararına rağmen o web sitesi ülke genelinde en çok ziyaret edilen web siteleri arasında yer alabilmektedir[122].

Erişim engelleme için birden çok tekniğin kombine şekilde kullanılması engellemelerin aşılmasını zorlaştırmaktadır. Bu sebeple, engelleme aşma yöntemleri de kombine şekilde kullanılabilmektedir. Örneğin, bir web sitesinin aynı anda farklı alan adları kullanarak DNS engellemesinden ve farklı ülkelerde yer alan birbirinden bağımsız barındırma hizmetleri 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. Her koşulda, erişim engellemenin kolay veya zor aşılıyor olması, engellemenin hukuka aykırılığını ortadan kaldırmamaktadır. Ayrıca, her zaman İnternet bilgisi orta düzeyin altında olan ve en basit engelleme aşma tekniklerini kullanamayacak bireyler var olmaya devam edecektir. Erişim engellemelerini aşan teknolojilerin yaygınlaşması devletlerin aldıkları erişim engelleme kararlarını manasız kılabilmektedir. Bu sebeple, devletlerin aldıkları bu karar erişim engellemeden ziyade erişimin zorlaştırılmasına hizmet etmektedir[123].

---

[121] *Akdeniz/Altıparmak*, a.g.e., s. 60.

[122] Örneğin www.yotutube.com web sitesinin erişimi engellenmesine rağmen Türkiye'de en çok ziyaret edilen web siteleri arasında yer almaktadır. Bkz. Top Sites in Turkey, http://www.alexa.com/topsites/countries;0/TR.

[123] *Akdeniz/Altıparmak*, a.g.e., s. 78; Murat Volkan Dülger, İnternet Erişiminin Engellenmesinin Hukuksal Açıdan Değerlendirilmesi ve 5651 Sayılı Yasayla Getirilen Düzenleme, İstanbul Barosu Dergisi, Cilt: 81, Yıl: 2007, Sayı: 4 ("*Dülger*"), s. 1480.

§ 5. MUKAYESELİ HUKUKTA ERİŞİMİN ENGELLENMESİ

Her devlet farklı sebep ve yöntemlerle İnternet içeriğine müdahale etmektedir. Daha önce belirtildiği üzere, devletlerin ekonomik ve teknolojik gelişmişliği ve hatta bulunduğu coğrafya gibi faktörler İnternet politikalarını etkilemektedir. Aşağıda, ABD, Çin, Güney Kore, Singapur ve Suudi Arabistan devletleri ile Avrupa Birliği'nin İnternet içeriğine müdahale politikaları ve uygulamaları yer almaktadır.

Bu devletlerin tercih edilmesinin farklı nedenleri bulunmaktadır. ABD İnterneti geliştiren ve doğal olarak en uzun süredir İnterneti kullanan devlet olduğu için tercih edilmiştir. Avrupa Birliği ise kapsadığı ülke sayısının fazla olması sebebiyle tercih edilmiştir. Çin devletinin tercih edilme sebebi ise dünyanın en fazla İnternet kullanıcısına sahip olması ve aynı zamanda İnternet içeriğine en çok müdahale eden devlet olmasıdır. Güney Kore devleti dünya genelinde en gelişmiş İnternet altyapısına sahip devlet olduğu için tercih edilmiştir. Singapur devletinin tercih edilmesinin sebebi ise yoğun İnternet kullanım oranına sahip olmasına rağmen, İnternet içeriğine en az müdahale eden devletlerden biri olmasıdır. Son olarak Suudi Arabistan, İnternet içeriğine ülke genelinde resmi olarak müdahale eden ilk devlet olduğu için tercih edilmiştir.

I. ABD

ABD, 220 milyonu aşkın İnternet kullanıcısıyla dünyanın en büyük İnternet aktörlerinden birisidir[124]. İnternet, ABD'nin ulusal güvenliğinin

[124] Internet Usage and Population in North America, http://www.internetworldstats.com/stats14.htm; ABD, İnterneti geliştiren ülke olmasına rağmen, İnternetin günlük

önemli bir parçası olmaya devam etmektedir. Bu sebeple ABD, İnterneti geliştiren ülke olarak ICANN, IANA gibi kurumların üzerindeki etkisini koruyarak İnternet politikalarının belirlenmesinde söz sahibi olmaya devam etmektedir. Ancak ABD, ağ tarafsızlığının korunması amacıyla ICANN ve IANA tarafından kontrol edilen İnternet trafik ağında herhangi bir içerik kontrol veya başkaca bir denetim mekanizması kullanmamaktadır. Bunun yerine, ABD İnternet içeriğine kendi ülkesinde federal ve federe düzeyde farklı sebep ve yöntemlerle müdahale etmektedir.

ABD'de İnternet içeriğine müdahale konusunda temel odak noktasını müstehcen içerik oluşturmaktadır. Müstehcen içeriğin sınırlanması sorunu görsel ve işitsel araçların yaygınlaşmaya başladığı 1960 yıllardan itibaren ABD'de önemli bir tartışma konusu olmuştur[125]. ABD 1996 yılına kadar müstehcen içeriğe müdahale edilmesine ilişkin yasal bir düzenleme yapmamış, yargı içtihatları ile ihtilafları gidermeye çalışmıştır.

ABD'de müstehcenliğe ilişkin ile ilgili temel içtihat, Amerikan Yüksek Temyiz Mahkemesi'nin 1973 tarihli Miller v. California isimli kararıdır[126]. Miller isimli şahıs, posta yoluyla cinsel içerikli ürünlerin tanıtımını yaptığı için müstehcen içeriğin yayılmasını yasaklayan Kaliforniya kanunlarını ihlal ettiği gerekçesiyle aleyhine ceza davası açılmıştır. Yargılama sırasında, müstehcen içerikli ürünlerin iletiminin ifade hürriyeti kapsamında korunması gerekip gerekmediği tartışılmış ve Mahkeme müstehcen içeriğin ancak belirli şartlar altında korunacağına hükmetmiştir.

Mahkeme, müstehcenliğin tespit edilebilmesi için üç aşamalı bir testin yapılmasını öngörmüştür[127]. İlk aşamada ortalama çağdaş ahlak anlayışına sahip sıradan bir kişinin o içeriği bir bütünsel olarak şehevi ilgi duyup duymadığı tespit edilecektir. İkinci aşamada, içeriğin yürürlükteki

kullanım yoğunluğu bakımından yakın bir zamanda Çin'in gerisinde kalmıştır. Bkz. China Surpasses U.S. In Internet Use, http://www.forbes.com/2006/03/31/china-internet-usage-cx_nwp_0403china.html.

[125] Kent D. Stuckey, Chapter 4: Obscenity and Indenecy, Internet and Online Law – Law Journal Press, 2008 ("*Stuckey*"), §4.0.2, s. 1.

[126] The Supreme Court, Miller v. California, 413 U.S. 15, 24, 93 S.Ct. 2607, 37 L.Ed.2d 419 (1973); Ayrıca bkz. Miller v. California, http://laws.findlaw.com/us/413/15.html; http://www.oyez.org/cases/1970-1979/1971/1971_70_73/.

[127] *Stuckey,* §4.0.2, s. 1

kanunlarda tanımlanan cinsel hareketleri açıkça saldırgan ve/veya iğrenç bir şekilde tanımlayıp tanımlamadığı veya tasvir edip etmediği tespit edilecektir. Son aşamada ise, içerik bütünsel olarak edebi, sanatsal, siyasi veya bilimsel bir değerinin olup olmadığı tespit edilecektir. Bu aşamalardan herhangi birini geçemeyen içerik müstehcen kabul edilerek ifade hürriyeti kapsamında korunmayacaktır.

Amerikan Yüksek Temyiz Mahkemesi'nin bu içtihadına rağmen müstehcen içeriğe ne ölçüde müsaade edileceği, diğer bir deyişle, müstehcenliğin hangi şartlarda ifade hürriyeti kapsamında değerlendirileceğine ilişkin ihtilaflar sona ermemiştir. Özellikle İnternetin yaygınlaşmasıyla birlikte ABD, müstehcenliğe ilişkin sınırlamaları yasal bir zemine kavuşturmak ve özellikle çocukların İnternette yer alan müstehcen içerikten etkin bir şekilde korumak amacıyla sırasıyla 1996 yılında Communications Decency Act ("CDA")[128] isimli kanun ile 1998 yılında Child Online Protection Act ("COPA")[129] isimli kanunları yürürlüğe koymuştur.

CDA müstehcen veya açık bir şekilde zararlı kabul edilen içeriğin 18 yaşından küçüklere iletilmesini veya bilinçli olarak bu tür içeriğin çocuklar tarafından erişilebilir şekilde sunulmasını yasaklamaktadır[130]. Bu doğrultuda, CDA çocukların müstehcenlik gibi zararlı içerikten korunması amacıyla kredi kartları veya benzeri teknolojiler kullanılarak yaş doğrulamasının sağlanmasını ve içerik sağlayıcıların çocukları bu tür içeriklerden korumak için gerekli tüm tedbirleri almalarını zorunlu kılmaktadır. Sorumluluk rejimi bakımından CDA makul bir yaklaşımı kabul etmiştir. Düzenlemenin 230. maddesine göre, İnternet hizmet sağlayıcıları yayımcılar ile eşdeğer kabul edilmemiş ve başkalarına ait içerikten gereken özeni gösterdikleri sürece sorumlu tutulmamıştır.

CDA, yürürlüğe konulmasından sadece bir yıl sonra, Amerikan Yüksek Temyiz Mahkemesi tarafından Reno v. American Civil Liberties Union kararıyla Anayasal güvence altında bulunan ifade hürriyetini ihlal

[128] Communications Decency Act, http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=104_cong_public_laws&docid=f:publ104.104.pdf.

[129] Child Online Protection Act, http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=105_cong_bills&docid=f:h3783eh.txt.pdf.

[130] CDA, m. 223.

ettiği gerekçesiyle iptal edilmiştir[131]. Mahkeme öncelikle CDA ile yasaklanan müstehcenlik fiilinin tanımını muğlâk bulmuştur[132]. Ayrıca, sakıncalı içeriğin çocuklar tarafından erişilebilir şekilde sunulması yasaklamasının kanunun uygulama olanını belirsiz hale getirdiğine hükmetmiştir.

Kararın gerekçesi incelendiğinde, hâkimlerin kararlarını İnternetin kendine özgü niteliğini göze alarak verdikleri anlaşılmaktadır. Karar gerekçesinde, İnternetin yetişkinler için özel bir alan yaratmaya elverişli olmadığı belirtilmiştir[133]. Nihayetinde İnternet yakınlık-uzaklık kavramlarını barındırmayan bir ortamdır[134]. Dünyanın neresinde barındırılırsa barındırılsın tüm web siteleri kullanıcılara karşı aynı uzaklıktadır. Mahkeme, bu gerçeği göz önüne alarak, müstehcen yayın yapan sinemaların ancak yerleşim yerlerinin uzağında yayın yapmalarına izin verilmesini öngören düzenlemelerden esinlenen CDA'nın bu hükmünün mevcut teknolojik düzey sebebiyle İnternet ortamında birebir uygulanamayacağına hükmetmiştir[135].

Öte yandan Mahkeme, sakıncalı içeriğin çocuklar tarafından erişilebilir şekilde sunulmasının fiilinin kanunun uygulama alanını belirsiz hale getirmesinin gerekçesi olarak İnternetin bu tür denetime imkân vermemesi gösterilmiştir[136]. Mahkeme İnternetin bir web sitesini ziyaret eden İnternet kullanıcısının gerçek yaşını kesin olarak tespit etmeye ola-

---

[131] Reno v. American Civil Liberties Union, 117 S.Ct. 2329, 138 L.Ed.2d 874 (1997). Karar için bkz. http://www.law.cornell.edu/supct/html/96-511.ZS.html; CDA'nın kaldırılmasıyla ilgili tartışmalar için bkz. The Battle for the Communications Decency Act 1996 is over, http://www.cyber-rights.org/battle.htm; Internet Censorship: Law & policy around the world, http://www.efa.org.au/Issues/Censor/cens3.html.

[132] Andrews Computer & Online Industry Litigation Reporter, Rep. 24416, 1 July 1997 ("*ANCOILR*"), s. 1.

[133] *ANCOILR*, a.g.e., s. 1.

[134] İnterneti klasik iletişim ve bilgiye erişim araçlarından ayıran temel nokta uzaklık-yakınlık kavramlarını kökten değiştirmesidir. Bir web sitesinin dünyanın hangi noktasında barındırıldığı erişen kullanıcı bakımından bir fark yaratmamaktadır. İki web sitesinin birbiriyle olan uzaklığı sadece kavramsal olarak bir değeri olup, fiziki yakınlıkla bir ilişkisi bulunmamaktadır. Sanal gerçeklik olarak ifade edilen bu durum İnterneti kendine özgü bir ortam haline getirmektedir. Daha fazla bilgi için bkz. *Bayamlıoğlu*, a.g.e., s. 34.

[135] *ANCOILR*, a.g.e., s. 2.

[136] *ANCOILR*, a.g.e., s. 2.

nak vermediğini; yaş doğrulaması gibi sistemler yanlış bilgiler verilmek suretiyle kolayca aşılabildiğine dikkat çekmiştir. Bu sebeple, yetişkinler için hizmet veren bir web sitesine sadece bir çocuğun erişmesini tüm içeriği hukuka aykırı hale getireceğini belirterek, düzenlemenin hukuka aykırılığına hükmetmiştir.

CDA yürürlükten kaldırıldıktan sonra doğan boşluğu doldurmak üzere 1998 yılında COPA yürürlüğe koyulmuştur. COPA, 1998 yılında kabul edilmesine rağmen çeşitli mahkemelerin verdiği ihtiyati tedbir kararları sebebiyle yürürlüğü belirli bir süre ertelenmiştir[137]. 22 Haziran 2000 tarihinde Amerikan Yüksek Temyiz Mahkemesi yapmış olduğu inceleme sonucunda COPA'nın CDA'ya nazaran makul bir sınırlama getirdiği gerekçesiyle kanunu iptal etmemiştir[138].

COPA, çocukların müstehcenlik gibi zararlı İnternet içeriğinden korunması amacıyla, çocukların İnternete yoğunlukla erişim yaptığı kütüphaneler ve devlet okullarında filtreleme yazılımlarını kullanma zorunluluğu getirmiştir. Bu sınırlamaların ifade hürriyetini ihlal ettiğine yönelik iddialar için Temyiz Mahkemesi, kütüphane ve yöneticilerin aşırı engelleme sebebiyle engellenen içeriği tekrar erişime açmaları mümkün olduğu için sınırlamanın ifade hürriyetini ihlal etmediğine karar vermiştir[139].

COPA, çocuklara zararlı içeriğin tespit edilmesi için yukarıda açıklanan Miller kararındaki kıstasların aynısını kullanmaktadır. Bu doğrultuda, yerleşik içtihada göre üçtü testin sonucuna göre bir içeriğin müstehcen olup olmadığına karar verilecektir. Öte yandan, COPA, içerik sağlayıcılara bazı yükümlülükler getirmiştir[140]. COPA, bir içerik sağlayıcının çocuklara zararlı içeriği sağlamaktan dolayı sorumlu tutulmaması için CDA'daki gibi kredi kartı, kimlik kartı veya mevcut teknolojilere göre

[137] COPA aleyhine yapılan iptal talepleri ve ilgili mahkemelerin kararları için bkz. COPA Litigation, http://www.cdt.org/speech/copa/litigation.php.

[138] US Court of Appeals for the 3rd Circuit, No. 99-1234, http://vls.law.vill.edu/locator/3d/Jun2000/991324.txt.

[139] *Stuckey*, §4.0.7, s. 6.

[140] Internet Censorship: Law & policy around the world, http://www.efa.org.au/Issues/Censor/cens3.html.

kullanılması makul kabul edilebilecek herhangi bir tekniği kullanmasını zorunlu kılmaktadır.

Temyiz Mahkemesi'nin 22 Haziran 2000 tarihli kararına rağmen COPA'nın ifade hürriyetini ihlal ettiğine yönelik tartışmalar sona ermemiştir. 2009 yılında konunun tekrar Temyiz Mahkemesi'nin önüne getirildiğinde Mahkeme kanunun yürürlük dönemindeki uygulamalarını da göz önüne alarak COPA'nın ifade hürriyetini ihlal ettiği gerekçesiyle Anayasaya aykırı bularak iptal etmiştir.

Amerikan Hukukunda CDA ve COPA dışında zararlı İnternet içeriğinden çocukların korunması amacını taşıyan bir diğer düzenleme ise Children's Internet Protection Act ("CIPA")[141] isimli düzenlemedir. CIPA, CDA ve COPA'nın aksine sınırlı bir uygulama alanına sahiptir. CIPA, okul ve kütüphanelerin İnternet güvenlik politikaları ağlarında filtreleme sistemleri kurmalarını zorunlu tutmaktadır[142]. CIPA ayrıca çocukların İnterneti bilinçli kullanmaları için gerekli bilgilendirmelerin yapılmasını öngörmektedir.

CIPA etkin bir şekilde uygulanmasını temin etmek amacıyla, bu tür filtreleme sistemlerin kurulmaması durumunda okul ve kütüphanalerin almış olduğu federal yardımların kesilmesini öngörmektedir. Bu sebeple, CDA ve COPA gibi CIPA da ifade hürriyetini anayasa aykırı bir şekilde kısıtladığı gerekçesiyle eleştirilere maruz kalmıştır. Tüm bu eleştirilere rağmen CIPA yürürlüğünü korumaktadır. CIPA dışında ayrıca çocukların korunması amacıyla İnternet içeriğine müdahale etmek için Amerikan Ceza ve Ceza Usul Kanunu'nun çocukların istismarının önlenmesine ilişkin 2256 numaralı maddesinde yer alan hükme dayanılmaktadır[143]. Bu hükme dayanılarak, içerik sağlayıcıların en azından müstehcen içeriğe ilişkin yaş doğrulaması gibi sistemleri kullanması zorunlu kılınmaktadır.

---

[141] Children's Internet Protection Act, http://ifea.net/cipa.pdf.

[142] Children's Internet Protection Act - FCC Consumer Facts, http://www.fcc.gov/cgb/consumerfacts/cipa.html.

[143] Crimes and Criminal Procedure - 18 USC Section 2256, http://law.onecle.com/uscode/18/2256.html.

ABD'nin İnternet içeriğine müdahale konusundaki bir diğer sebebi çocuk pornografisi oluşturmaktadır[144]. ABD çocukların istismarının önlenmesine ilişkin Birleşmiş Milletler Çocuk Haklarına Dair Sözleşme gibi temel uluslararası sözleşmelere taraftır[145]. Ancak ABD'de çocuk pornografisine ilişkin temel tartışmayı nüdizm oluşturmaktadır. Nüdizm, kişilerin vücutlarından utanmadan rahatlıkla sosyal olarak çıplak bir şekilde bir arada ve doğa ile bütünleşik bulunabilmeleri hali olarak tanımlanmaktadır[146]. ABD'de bu şekilde dolaşmanın farklı bir ifade şekli olduğu ve bu sebeple ifade hürriyeti kapsamında korunması gerektiği ileri sürülmektedir. Bu iddia Sunshine Book Co. v. Summerfield[147] isimli Amerikan Yüksek Temyiz Mahkemesi kararıyla desteklenmektedir. Yüksek Mahkeme bu kararında cinsellik içermeyen salt çıplaklığın bir ifade olarak korunacağına karar vermiştir. Bu karara dayanılarak nüdizm savunucuları, çocukların salt çıplak görüntülerinin çocuk pornografisi olarak kabul edilmemesi gerektiğini iddia etmektedirler. Bu konudaki, ABD uygulaması görsel içeriğin sunuş şeklinin her somut olayda değişmesi sebebiyle yeknesaklık göstermemektedir.

Müstehcenlik ve çocuk pornografisinden sonra İnternet içeriğine müdahale konusunda diğer odak noktasını uluslararası terörizmle mücadele oluşturmaktadır. ABD, 11 Eylül saldırılarından sonra terörler mücadele amacıyla İnternet politikasını radikal bir şekilde değiştirerek 2003 yılında Information Operations Roadmap[148] isimli bir düzenlemeyi yürürlüğe koymuştur. Söz konusu düzenleme, İnternet başta olmak üzere tüm iletişim araçlarının askeri amaçlarla kullanımını, düşman ağların çökertilmesi ve her türlü mecrada propagandalara karşı mücadele edilmesi amaçlamaktadır. Bu düzenleme, İnternet içeriğine keyfi müdahale

[144] Çocuk pornografisinin tanımı ve bu konudaki tartışmalar için bkz. aşa. §6 IV A 2.

[145] Sözleşme, Birleşmiş Milletlerin 20 Kasım 1989 tarihli 44/25 sayılı Genel Kurul kararıyla kabul edilmiş ve 49. maddesi uyarınca 2 Eylül 1990'da yürürlüğe girmiştir. Sözleşmenin tam metni için bkz. Convention on the Rights of the Child, http://www.unhchr.ch/html/menu3/b/k2crc.htm.

[146] Nüdizm, http://tr.wikipedia.org/wiki/Nudizm.

[147] Sunshine Book Co. v. Summerfield, Postmaster General, 355 U.S. 372, http://altlaw.org/v1/cases/799128.

[148] Information Operations Roadmap, http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB177/info_ops_roadmap.pdf.

niteliği taşıdığı ve ABD'nin İnternet yönetimi konusundaki yetkilerini kötüye kullandığı gerekçesiyle eleştirilmiştir[149]. Öte yandan bu düzenleme kaldırılmamasına rağmen, ABD ulusal bilgi ağlarını siber saldırılardan korumak ve siber güvenliğe yapılacak yatırımları ve araştırmaları teşvik edecek yeni bir strateji taslağı hazırlanmıştır[150].

Son olarak ABD fikri mülkiyet ihlallerine ilişkin yoğun bir şekilde İnternet içeriğine müdahale etmektedir[151]. ABD bireysel engellemelerin yanı sıra bu tür içerikle etkin bir şekilde mücadele etmek amacıyla İnternet ortamı dâhil her türlü ortamda fikri mülkiyet ihlalleri için ağır cezalar öngörmüştür. Böylece, bireyler üzerinde psikolojik baskı oluşturmak suretiyle bir sosyal engelleme tekniği kullanmış olmaktadır.

ABD bir federal devlet olduğu için her federe devletin kendi sınırları içerisinde Anayasada öngörülen sınırlamalara bağlı olmak kaydıyla farklı düzenlemeler getirmesi mümkündür. Bu sebeple ABD'nin İnternet içeriğine müdahale konusundaki yaklaşımının tespit edilebilmesi için federe devletlerin düzenlemelerinin de göz önünde bulundurulması gerekmektedir[152].

II. Avrupa Birliği

Avrupa Birliği, üye devletlerinin nüfus toplamı göz önüne alındığında 489 milyondan fazla nüfusu ve 297 milyondan fazla İnternet kullanıcısıyla İnternetin en büyük aktörlerinden birisidir[153].

---

[149] *Goldsmith/Wu*, a.g.e., s. 32; Bush administration annexes internet, http://www.theregister.co.uk/2005/07/01/bush_net_policy/.

[150] Obama Yönetimi Siber Güvenlik Stratejisinin Ana Çizgilerini Açıkladı!, http://www.leylakeser.org/2009/01/obama-yonetimi-siber-guvenlik.html.

[151] *Deibert/Palfrey/Rohozinski/Zittrain*, a.g.e., s. 9.

[152] New York, New Mexico, Michigan ve Virginia eyaletlerinin çocukların İnternet ortamındaki sakıncalı içerikten korumak amacıyla hazırladıkları düzenlemeler Anayasaya aykırı oldukları gerekçesiyle Amerikan Yüksek Temyiz Mahkemesi tarafından iptal edilmişlerdir. Bkz. Internet Censorship: Law & policy around the world, http://www.efa.org.au/Issues/Censor/cens3.html.

[153] Internet Usage in European Union, http://www.internetworldstats.com/stats9.htm.

Avrupa Birliği, İnternet içeriğinin düzenlenmesi ve erişim engelleme sebepleri konusunda bütünsel bir düzenleme yapmak yerine temel ilkeleri belirlemekle yetinmektedir. Bu yaklaşımın temelde iki nedeni olduğu kabul edilmektedir[154]. İlk neden, hangi alanlarda ve hangi yöntemin kullanılması gerektiği kesin olarak tespit edilmeden yasal bir düzenlemenin yapılmasının doğru bulunmamasıdır. Bu noktada, İnternetin yeni ve gelişmekte olan kendine özgü bir sistem olduğu göz önünde bulundurulmuştur. İkinci neden ise, Avrupa Birliği'nin ifade hürriyeti gibi temel insan hakları kazanımlarının zarar görmesini istememesidir. Buna rağmen, Avrupa Birliği hukuka aykırı ve zararlı içeriğe müdahalede belirli koşullar altında ifade hürriyetini korumaktan daha baskın bir kamu yararı olduğunu kabul etmektedir[155].

Avrupa Birliği İnternet gibi yeni gelişen teknolojileri Avrupa Bilgi Toplumu kapsamında değerlendirmektedir. Avrupa Bilgi Toplumu'nun esasları 1994 tarihli Avrupa Komisyonu Eylem Planında belirlenmiştir[156]. Planda, istenmeyen veya zararlı içeriğin İnternet ortamında yayılmasına ve çocukların korunması ihtiyacına ilişkin ilkeler yer almasına rağmen bu konuda kesin bir çözüm veya yöntem belirlememektedir[157].

İnternet içeriğine düzenlenmesine yönelik diğer bir düzenleme ise 1996 yılında Avrupa Komisyonu tarafından İnternetteki Hukuka Aykırı ve Zararlı İçerik[158] ("1996 Tebliği") adlı tebliğ altında gerçekleştirilmiştir. Ayrıca görsel ve iletişim araçlarında insan haysiyetinin ve çocukların korunması amacıyla Yeşil Belge diye anılan başkaca bir tebliğ yayınlamıştır[159].

[154] Penny Campbell/Emmanuelle Machet, European Policy on Regulation of Content on the Internet, Liberating Cyberspace: Civil liberties, human rights, and the Internet (Edited by Liberty), (s. 140 - 158), London 1999 ("*Campbell/Machet*"), s. 141.

[155] *Campbell/Machet*, a.g.e., s. 146.

[156] Eylem Planın odak notası telekomünikasyon sektörünün özel sektöre açılması ve sektöre ilişkin temel standartların belirlenmesidir. Communication on Europe's Way to the Information Society, an Action Plan, 1994. Ayrıca bkz. Europe's Information Society Portal, http://ec.europa.eu/information_society/index_en.htm.

[157] *Campbell/Machet*, a.g.e., s. 144.

[158] European Commission Communication on Illegal and Harmful Content on the Internet (1996). Tam metin için bkz. http://aei.pitt.edu/5895/01/001527_1.pdf.

[159] Green Paper on the protection of minors and human dignity in audiovisual and information services (1996), http://aei.pitt.edu/1163/01/minors_info_soc_gp_COM_96_483.pdf.

Avrupa Birliği'nin İnternet içeriğini düzenleme yönündeki temel odak noktasını çocuk pornografisi oluşturmaktadır. Çocuk pornografisinden sonra ise ikinci odak konusu ırkçı söylemdir. Avrupa Komisyonu'nun müstehcenlik veya diğer zararlı içeriğe ilişkin cezai bir düzenlemeyi içeren herhangi bir direktif yayınlama yetkisi bulunmamaktadır. Çocuk pornografisi, ırkçı söylem gibi suçlar ve zararlı içeriğin ne olduğu her devletin kendi iç hukukunda farklı bir şekilde düzenlemekte ve birçok üye devlette zaten suç olarak kabul edilmektedir. Bu sebeple, gerçek hayatta suç olan her şey zaten İnternette de suç olarak kabul edildiği için özel bir düzenleme yapılmasa bile üye devletlerin İnternet içeriğine müdahale etme olanakları bulunmaktadır[160]. Komisyon, bir ülkede sakıncalı olarak kabul edilen hususun başka bir ülkede hukuka uygun olabilmesi ve sakıncalı içeriğin tanımının ülkeden ülkeye değişebilmesi sebebiyle tek bir düzenlemeyle İnternet içeriğine müdahale etmekten çekinmektedir.

Komisyon, 1998 yılında yayınladığı Eylem planında sakıncalı İnternet içeriğini hukuka aykırı ve zararlı olarak ikiye ayırmaktadır[161]. Bu ayırım ile çocukların yetişkinler için olan içeriğe erişimi ile yetişkinlerin çocuk pornografisi gibi içeriğe erişimi konuları arasında ayrım yapılması amaçlanmaktadır[162]. Hukuka aykırı olsun veya zararlı olsun sakıncalı içerikle mücadele için Avrupa Birliği İnternet içeriğinin düzenlenmesinde erişim engelleme gibi bir yöntemi tercih etmemekte ve bunun gerekçesi olarak kapatılan web sitelerinin hızla yeniden ortaya çıkması ve erişim engellemenin sakıncalı içeriğin P2P ağları gibi diğer İnternet hizmetleri ile dağıtımının engellenmesinde yetersiz kalması gösterilmektedir[163]. Birlik erişim engelleme yerine, üye devletlerarasında işbirliğinin artırılması, özdenetim uygulamalarının yaygınlaştırılması ve erişim engelleme amacıyla filtreleme sistemlerinin kullanılmasının teşvik edilmesini öngörmektedir[164].

---

[160] *Campbell/Machet*, a.g.e., s. 145.

[161] Action Plan on promoting safer use of the Internet by combating illegal and harmful content on global Networks (1998).

[162] *Akdeniz/Altıparmak*, a.g.e., s. 76.

[163] *Akdeniz/Altıparmak*, a.g.e., s. 78.

[164] *Campbell/Machet*, a.g.e., s. 141.

Birliğin İnternet içeriğinin düzenlenmesine ilişkin asıl odak noktası olan özdenetim iki aşamada gerçekleştirilmektedir[165]. İlk aşama hukuka aykırı veya zararlı içeriğin yayınlanmasını önlemektir. İkinci aşama ise hukuka aykırı veya zararlı içeriğin filtreleme yazılımları gibi yöntemler kullanılarak çocuklar tarafından erişilmesini engellemektedir. Diğer bir deyişle, özdenetim yöntemiyle devlet müdahalesinin asgariye indirilmeye çalışılmakta ve her ebeveynin kendi çocuğuna ilişkin tedbirleri alması teşvik edilmektedir.

Avrupa Birliği'nin içerik filtreleme esasları, görsel ve iletişim araçlarda insan haysiyetinin ve çocukların korunması amacıyla hazırlanan Yeşil Belge'de düzenlenmektedir. Yeşil Belge ayrıca İnternet içeriğinin daha etkin bir şekilde filtrelenmesi için özel bir Avrupa içerik derecelendirme sisteminin kurulmasını öngörmektedir. Tüm bu hedefler 1999 yılında kabul edilen Daha Güvenli İnternet Kullanımı için AB Eylem Planı altında toplanmıştır[166].

Avrupa Birliği'ne üye devletleri kendi kurdukları sistemlerle İnternet içeriğine farklı sebeplerle müdahale edebilmektedir. 1999 tarihli Eylem Planı zararlı içeriğin ihbar edilmesi ve koordinasyonun sağlanması için bir Avrupa ihbar merkezinin kurulmasını öngörmektedir. Bu doğrultuda hem Avrupa Birliği nezdinde hem de her ülke kendi bünyesinde İnternet içeriğini takip eden ve sakıncalı içeriğe ilişkin ihbarlar alan merkezler kurulmuştur[167]. Ayrıca bazı sivil toplum örgütlerinin girişimi ve devletlerin bu konuda gösterdikleri işbirliğiyle, dünya genelinde faaliyet gösteren ihbar merkezleri arasında iletişimi sağlamak amacıyla bazı ana ihbar merkezleri kurulmuştur[168]. Nihayetinde, bir ülkede bir web sitesinin

---

[165] *Campbell/Machet*, a.g.e., s. 149.

[166] Action Plan on Promoting Safer Use of the Internet, Decision No 276/1999/EC of the European Parliament and of the Council of 25 January 1999, http://ec.europa.eu/archives/ISPO/legal/fr/internet/actplan.html.

[167] Avrupa Birliği kapsamında faaliyet gösteren ihbar merkezlerinin listesi için bkz. http://ec.europa.eu/information_society/activities/sip/projects/centres/index_en.htm.

[168] Bu birliklerden en yaygın ağa The International Association of Internet Hotlines ("Inhope") isimli birlik sahiptir. Birliğin, ABD, Almanya, Avustralya, Avusturya, Belçika, Bulgaristan, Çek Cumhuriyeti, Çin, Danimarka, Finlandiya, Fransa, Güney Kore, Hollanda, İngiltere, İrlanda, İspanya, İtalya, İzlanda, Japonya, Kanada, Kıbrıs, Letonya, Litvanya,

erişiminin engellenmesi o web sitesinin dünya genelindeki yayınını durdurmamaktadır. İçeriğin barındırıldığı sunucunun erişimi, bulunduğu ülke tarafından engellenmediği sürece kesin çözüm elde edilmiş olmamaktadır. Bu tür ana ihbar merkezleri, içeriği engellenen web sitelerine ilişkin verileri ortak bir veritabanı üzerinden paylaşılmasına olanak tanımaktadır. Örneğin, ABD'de barındırılan bir içerik sebebiyle Almanya tarafından erişim engellendiği durumda, engellemeden ABD haberdar ederek içeriğin ABD tarafından tamamen engellemesi ve bir suç varsa faillerin tespit edilerek cezalandırılması sağlanmaktadır.

Öte yandan, İSS'ler gibi hizmet sağlayıcıların hukuki sorumluluğu Avrupa Birliği İç Pazarda Bilgi Toplumu Hizmetlerinin Bazı Hukuksal Yönlerine, Özelliklere Elektronik Ticaret İlişkin Avrupa Birliği Yönergesi ("E-Ticaret Yönergesi")[169] altında düzenlenmektedir. Getirilen sorumluluk rejiminin uyarı temelli bir sorumluluk rejimi olarak kabul edilmektedir[170]. E-Ticaret Yönergesinin 14. maddesinde İSS'ler için koşullu bir sorumluluk getirilmiş ve yasadışı eylem veya içeriğin gerçekten var olduğu bilgisini edinmeleri üzerine sakıncalı içeriğin kaldırılması veya erişimin engellenmesi için derhal harekete geçmekle yükümlü tutulmuşlardır. İSS'ler genel bir izleme yükümlülüğü olmaksızın ancak gereken özeni göstermedikleri durumlarda sorumlu tutulmaktadır.

Avrupa Birliği belirli sebepleri üye ülkelerine dayatmadığı için her devlet kendi iç hukukunda sakıncalı görülen sebeplerle İnternet içeriğine müdahale etmektedir.

Almanya, çocuk pornografisi, her türlü pornografik içerik ve aşırı sağ görüşlü web siteleri ile özelde her türlü Nazi propagandasını kurmuş olduğu Jugendschutz[171] ihbar merkezinde takip etmektedir. Bu merkez

Lüksemburg, Malta, Macaristan, Polonya, Portekiz, Slovenya ve Yunanistan'dan üye ihbar birimleri bulunmaktadır. Daha fazla bilgi için bkz. The International Association of Internet Hotlines, https://www.inhope.org.

[169] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:EN:NOT.

[170] *Akdeniz/Altıparmak*, a.g.e., s. 80.

[171] Jugendschutz, http://www.jugendschutz.net.

tarafından çoğu aşırı sağcı yüzlerce web sitesinin erişimi engellenmiş, bazı içeriklerin de belirli bölümleri yayından çıkarılmıştır[172]. Bu merkezin engellemeleri dışında, hakaret ve fikri mülkiyet ihlalleri gibi sebeplerle bazı web sitelerinin erişimi engellenmiştir. Örneğin, Alman Sol Parti Federal milletvekili Lutz Heilmann, İnternet ansiklopedisi Wikipedia'da özgeçmişiyle ilgili asılsız bilgilerin yer aldığı gerekçesiyle İnternet ansiklopedisi Wikipedia'nın Almanca versiyonu http://www.wikipedia.de web sitesi için erişim engelleme kararı aldırmıştır[173]. Ücretsiz İnternet ansiklopedisindeki hukuka aykırı veya zararlı sadece bir sayfa için tüm ansiklopediye erişim engellenmiştir. Fikri mülkiyet ihlalleri sebebiyle dünyanın en büyük dosya paylaşım sitelerinden birisi olan rapidshare.com web sitesinin erişimi 2007 yılında Alman müzik telif hakkı sahipleri ittifakı GEMA tarafından engellenmiştir[174]. Rapidshare kullanıcıları tarafından yüklenen içerikten dolayı sorumlu tutulmayacağını belirtmesine rağmen, telif haklarını ihlal ettiği iddia edilen dosyaların Rapidshare sunucularından silininceye kadar erişim engellemesi kaldırılmamıştır.

Fransa da Almanya gibi aşırı sağ içerikle ve fikri mülkiyet ihlalleriyle ilgili yoğun bir şekilde İnternet içeriğine müdahale etmektedir. Fransa'nın İnternet içeriğine müdahalesi konusunda 2000 yılında LICRA tarafından Yahoo aleyhine Nazi ürünlerinin Yahoo'nun açık artırma sitesinde satılması sebebiyle açılmış dava oluşturmaktadır[175]. Fransa'nın Nazi içeriği gibi aşırı sağcı içeriğe karşı kesin tavrı Fransız kullanıcılara yönelik hizmet veren bazı web sitelerinin özdenetim mekanizmalarını işletmesine yol açmaktadır. Örneğin, Google arama motorunun Fransız sürümünün sakıncalı gördüğü bazı içerikleri kendisi filtrelemektedir[176]. Fransa'da İnternet içeriğine ilişkin ikinci temel müdahale nedeni fikri

---

[172] İstatistikler için bkz. *Akdeniz/Altıparmak*, s. 79; VHO - Index of Censorship, http://www.vho.org/censor/Censor.html#Web.

[173] German Politician Blocks Local Wikipedia, http://www.techcrunch.com/2008/11/16/german-politician-blocks-local-wikipedia/.

[174] GEMA obtains injunctions against data exchange services, http://www.heise.de/english/newsticker/news/83948.

[175] Davanın ayrıntıları için bkz. yuk. §3 V H.

[176] Benzer bir filtreleme Google'ın Almanya tarafından da gerçekleştirilmektedir. Bkz. Localized Google search result exclusions, http://cyber.law.harvard.edu/filtering/google/.

mülkiyet ihlalleridir ve Fransa caydırıcılığı sağlamak için içerik sağlayıcılar için ağır cezalar uygulamaktadır.

İngiltere'nin İnternet içeriğine müdahalede odak noktasını çocuk pornografisi, müstehcenlik ve ırkçılık söylemi oluşturmaktadır. İngiltere'de sakıncalı İnternet içeriğini Internet Watch Foundation ("IWF")[177] adlı birim tarafından takip edilmektedir. İnternet içeriğine müdahale müstehcen içeriğin düzenlenmesine ilişkin 1959 tarihli the Obscene Publications Act ve çocukların korunmasına ilişkin 1978 tarihli the Protection of Children Act isimli düzenlemelere dayanılarak gerçekleştirilmektedir[178].

IWF, çocuk pornografisine yönelik her türlü içeriği, içerik veya yer sağlayıcının İngiltere'de bulunmasına bakmaksızın engellemektedir[179]. Ancak suç oluşturan müstehcen içerik ile ırkçılık söylemi içeren içeriğin engellenmesi için içeriğin İngiltere'de barındırılması şartını aramaktadır. İngiltere'nin bu yaklaşımı yerinde bir yaklaşımdır. Çocukların istismarının önlenmesi uluslararası düzeyde kabul edilmiş standartlara sahip olmasına rağmen müstehcenlik ve ırkçılık söylemi için aynı ortak duyarlılık yoktur. Ayrıca, bu tür kavramların tanımı göreceli olduğu için İngiltere haklı olarak sadece kendi egemenlik alanında barındırılan bu tür içeriğe müdahale etmektedir.

Sonuç olarak, Avrupa Birliği'nin İnternet içeriğinin düzenlenmesine ilişkin temel yaklaşımı bilgi kâğıt kullanılarak nasıl erişiliyorsa aynı kolaylıkta ve sınırlama olmaksızın İnternet üzerinden erişilmesinin sağlanması ve çocukların korunması için özdenetim yöntemlerinin teşvik edilmesidir[180]. Genel kapsamlı bir düzenleme getirilmemesinin temel sebebi ise üye devletlerarası sosyal, kültürel ve tarihi sebepleler ortak bir yaklaşımın

---

[177] Internet Watch Foundation, http://www.iwf.org.uk.

[178] *Campbell/Machet*, a.g.e., s. 148; Diğer tüm düzenlemeler için bkz. Laws relating to the work of IWF, http://www.iwf.org.uk/police/page.22.htm.

[179] IWF çocuk pornografisinin önemi sebebiyle kullanıcılarına ihbar edilmek üzere çocuk pornografisi resimlerinin araştırılmasının dahi mahkemeler nezdinde geçerli bir savunma olarak kabul edilmeyeceği uyarısında bulunmaktadır. Bkz. The Hotline and the law, http://www.iwf.org.uk/public/page.31.htm.

[180] *Campbell/Machet*, a.g.e., s. 150.

sağlanamaması ve her devletin kendi toplumsal gereksinimine göre kendisinin harekete geçmesinin amaçlanmasıdır[181].

III. Çin

Çin Halk Cumhuriyeti 1milyarı aşkın nüfusu ve 298 milyon aktif İnternet kullanıcısı ile dünyanın en büyük İnternet aktörlerinden birisidir[182]. Çin anayasasında her ne kadar ifade hürriyeti, özgürlüğü, insan haklarına saygı korunsa da Çin Komünist Partisi İnternet dâhil tüm medya ve iletişim mecralarını kontrol altında tutmaktadır[183]. 1990 yılında İnternet ağına dâhil olan Çin, gerekli denetim sistemlerini kuruncaya kadar İnterneti kamusal kullanıma açmamıştır[184].

Çin dünyanın en gelişmiş İnternet erişim engelleme ve takip sistemini kullanmaktadır. Çin'in kurduğu İnternet takip ve erişim engelleme sistemi tüm ülke genelinde her bir İnternet noktasını kontrol edebildiği için Büyük Çin Seddi'ne benzetilerek Büyük Çin İnternet Duvarı olarak adlandırılmaktadır[185]. Çin İnterneti kamusal alanının bir uzantısı olarak görmekte ve İnternetin kullanılmaya başlandığı ilk dönemlerden beri İnternet erişimini engellemekte ve vatandaşlarının İnternet aktivitelerini takip etmektedir. Çin kalabalık nüfusuna rağmen sosyal engelleme yöntemleri ve her İnternet bağlantı noktasında yer alan takip sistemleri sayesinde ülke genelinde erişim engellemeyi başarıyla sürdürmektedir.

Çin ekonomik gelişimin teknolojik altyapının güçlü olduğuna bağlı olduğunun farkındadır. Her ne kadar komünist devlet sistemi sebebiyle kapalı bir yapıya sahip olsa da, İnternetin ekonomik kalkınmaya olan katkısından dolayı İnternet tamamen yasaklanmamakta ve dünyanın en gelişmiş ağ altyapısına sahip olmak için büyük yatırımlar yapmaktadır[186].

---

[181] *Akdeniz/Altıparmak*, a.g.e., s. 83.

[182] Internet Usage in Asia, http://www.internetworldstats.com/stats3.htm.

[183] *Deibert/Palfrey/Rohozinski/Zittrain*, a.g.e., s. 265.

[184] Sandhya Rao/Bruce C. Klopfenstein, Cyber Path to Development in Asia: Issues and Challenges, Connecticut 2001 ("*Rao/Klopfenstein*"), s. 68.

[185] *Goldsmith/Wu*, a.g.e., s. 92.

[186] Çin, Dünya Ticaret Örgütü'ne dâhil olma yolunda başta telekomünikasyon sektörü olmak üzere birçok alanda yabancı yatırımcılara karşı sınırlamaları kaldıracağı taahhüdün-

Ancak, Çin İnternet'in ülke genelinde yaygınlaşmasının ülkesine beraberinde kontrol edemeyeceği miktarda bilgi akışı getireceğinin farkındadır. Çin bir yandan gelişmekte olan ekonomisine katkıda bulunması için İnterneti yaygınlaştırmaya çalışmakta bir yandan da komünist düzenini korumaya çalışmaktadır. Bu sebeple vatandaşlarının İnternetteki her adımını izlemekte ve istenmeyen içeriğe anında müdahale etmektedir. Diğer bir deyişle, İnternet Çin'de devletinin komünist devletin ilkelerine aykırı olmadığı kadar özgür kabul edilmektedir[187].

Çin'in kurduğu İnternet duvarı çeşitli teknolojilerin bir araya getirilmesiyle ve CISCO, Yahoo, Google, Microsoft gibi Amerikan şirketlerinin çeşitli düzeylerdeki işbirliğiyle geliştirilmiştir. Çin routerların bir veriyi bir noktadan başka bir noktaya taşıyacak şekilde programlana bildiğine göre, taşınan veriyi ağda kaybetmek için de kullanılabileceğini keşfetmiştir[188]. Bu doğrultuda ülke genelindeki tüm İnternet çıkış noktaları kontrol altına alınarak, dünyanın en büyük router üreticisi olan CISCO firmasından tüm Çin'i kapsayacak bir İnternet duvarı geliştirilmesi istenmiştir. CISCO tarafından geliştirilen İnternet duvarı, çalışanların İnternette zararlı sitelere girmelerini engelleyen ve ziyaret ettikleri siteleri kaydeden klasik İnternet filtreleme sistemlerinden esinlenmiştir[189]. Diğer bir deyişle, filtreleme sistemi daha geniş bir coğrafyada daha geniş bir kitleyi kontrol edecek şekilde yeniden programlanmıştır. Oluşturulan sistem İnternet bağlantı hızında önemli bir yavaşlamaya da sebep olmamaktadır. Sistem kapsam bakımından hem İSS hem ana İnternet omurgası temelli; teknik bakımdan ise IP, URL, DNS ve içerik engelleme sistemlerini kombine bir şekilde kullanabilmektedir. Çin sistemin etkinliğini korumak amacıyla erişim engellemelerini aşma yöntemleri ile ayrıca mücadele edilmekte ve bu tür yöntemleri kullananları cezalandırmaktadır.

---

de bulunmuştur. Yabancı sermayenin Çin'deki yatırımlarının artması Çin İnternet yasaklamalarını belirli bir ölçüde yumuşatmıştır. Daha fazla bilgi için bkz. *Rao/Klopfenstein*, a.g.e., s. 73.

[187] Bu ikilem, birçok otoriter devletin İnternetle ilgili temel sorunudur. Bkz. *Goldsmith/Wu*, a.g.e., s. 89.

[188] *Goldsmith/Wu*, a.g.e., s. 93.

[189] *Goldsmith/Wu*, a.g.e., s. 93.

İnternete fiziksel erişim Enformasyon Bakanlığı tarafından kontrol edilmekte ve ülke genelinde 7 İSS faaliyet göstermektedir. İSS'ler kullanıcılarının İnternet tanıtma bilgilerini, ziyaret sürelerini ve yaptıkları aktiviteleri en az 60 gün saklamakla yükümlü tutulmuştur[190]. Benzer bir şekilde tüm İnternet kafelere filtreleme programı kullanma ve müşterilerinin kayıtlarını tutma zorunluluğu getirilmiştir. Ayrıca Çin'de İnternet bağlantısına sahip olabilmek için yerel polis karakoluna kişinin kendisini kayıt ettirmesi gerekmektedir[191].

Çin, Yahoo, Google, Microsoft gibi dev Amerikan bilişim şirketlerin işbirliği sayesinde erişim engelleme ve takip politikasını başarıyla sürdürmektedir. Çin bu gibi şirketlerin ülkede faaliyet gösterebilmesi için sistemlerini ülkenin İnternet politikalarıyla uyumlu hale getirmelerini zorunlu kılmaktadır[192]. Bir suç şüphesi olduğunda Çinli yetkililerin talebi üzerine gereken bilgiler iletişimin ve özel verilerin gizliliği gibi temel hak ve hürriyetler gözetilmeksizin bizzat ABD'li şirketler tarafından Çinli makamlara sunulmaktadır[193]. Sadece Yahoo'nun kendi kullanıcılara ait bilgileri Çin devleti ile paylaşması sonucunda 2006 yılında bir kısmı gazeteci 52 kişi İnternet aktiviteleri sebebiyle tutuklanmıştır[194]. Ayrıca, şirketlerin sunduğu arama motoru, blog gibi servislerde belirli kelimelerin kullanılmasının yasaklanması sağlanmaktadır[195].

Çin'in hangi İnternet içeriğine müdahale edeceği 25.11.2005 tarihli Provisions on the Administration of Internet News Information Services

---

[190] *Deibert/Palfrey/Rohozinski/Zittrain*, a.g.e., s. 265.

[191] *Rao/Klopfenstein*, a.g.e., s. 72.

[192] The Communist Cyber-Block, http://www.ifex.org/en/content/view/full/68881/.

[193] Söz konusu Amerikan şirketleri, Çin hükümeti ile İnternet üzerinden temel hak ve hürriyetleri kısıtlamak için işbirliği yapmaları sebebiyle çeşitli tepkiler almışlardır. Bu şirketler, faaliyet gösterdikleri ülkedeki kanunlara uymak zorunda oldukları gerekçesiyle yapmış oldukları sınırlamaları haklı kılmaya çalışmaktadır. Buna rağmen söz konusu şirketler Çin'de kendi kurumsal ilkelerini bile yok saymaktadırlar. Daha fazla bilgi için bkz. Kristen Farrell, Corporate Complicity in the Chinese Cencoprship Regime: When Freedom of Expression and Profitability Collide, Journal of Internet Law, January 2008 ("*Farrell*"), s. 1 vd.

[194] *Deibert/Palfrey/Rohozinski/Zittrain*, a.g.e., s. 266.

[195] 2005 yılında aktif edilen Microsoft'a ait ücretsiz blog servisinde özgürlük ve demokrasi kelimelerinin kullanılması yasaklanmıştır. Bkz. *Goldsmith/Wu*, a.g.e., s. 95.

isimli Enformasyon Bakanlığı düzenlemesinde belirlenmiştir[196]. Düzenlemenin 19. maddesine göre anayasada öngörülen ilkeleri ihlal eden, ulusal güvenliği ve bütünlüğü tehdit eden, devlet sırlarını ifşa eden, ulusal menfaatlere zarar veren, ırkçılığa sevk eden, dinle ilgili ulusal politikaları ihlal eden ve batıl inançlar yayan, asılsız söylentilere yol açan, kamu düzenini ve dirlik esenliği ihlal eden, müstehcenliği, pornografiyi, kumarı, şiddeti, terörü yayan veya suça teşvik eden, üçüncü kişileri hakaret eden veya aşağılayan, üçüncü kişilerin yasal hak ve menfaatlerini ihlal eden, sosyal düzeni bozan toplantı veya gösteriler düzenlenmesini teşvik eden, yasadışı bir oluşum adına hareket eden veya diğer kanunlarca yasaklanan her türlü içeriğin engelleneceği öngörülmüştür.

Bu düzenlemeye göre hukuka aykırı olarak kabul edilen içeriğin kapsamına devlet tarafından hassas görülebilecek her konu girebilmektedir. Engelleme devlet menfaatleri, ulusal güvenlik gibi muğlak ifadelerle belirlenmesi sebebiyle erişim engellemesi keyfi uygulamalara yol açmaktadır. Örneğin, Çin Uluslararası Çalışma Örgütü'ne üye olmasına rağmen işçi haklarına uygunluğunu takip eden sitelere erişim engellenmektedir[197]. Benzer bir şekilde Doğu Türkistan, Uygur, Tibet, Moğol gibi azınlık web siteleri ulusal güvenlik sebebiyle, Hıristiyan, Müslüman, Yahudi veya Hindu dinlerine ilişkin içerikler din politikalarına aykırılık sebebiyle engellenmektedir[198]. Çin ayrıca her türlü pornografik içeriği engellemektedir. Bu konudaki tavrı katı olan Çin, farklı kurumlarını yetkilendirerek bu tür içerikle mücadele etmektedir.

Çin İnternet Duvarı tarafından insan hakları, demokrasi, siyasal reform, gibi bine yakın kelime içerik engellemesi tekniğiyle otomatik olarak engellenmektedir[199]. Bu tür engellemelerin aşılması için içerik aldatması yaygın olarak kullanılmaktadır. İçerik aldatması bölümünde açıklandığı üzere, Çinli bir insan hakları sitesinde demokrasi kelimesi yerine "laha-

[196] Provisions on the Administration of Internet News Information Services, http://www.cecc.gov/pages/virtualAcad/index.phpd?showsingle=24396.

[197] *Deibert/Palfrey/Rohozinski/Zittrain*, a.g.e., s. 267.

[198] *Goldsmith/Wu*, a.g.e., s. 94.

[199] *Goldsmith/Wu*, a.g.e., s. 94.

na", çok partili sistem için ise "havuç" kelimesi kullanılarak engellemeler sıklıkla aşılmaktadır[200].

Çin ayrıca sosyal teknikleri yaygın olarak kullanmaktadır. Daha önce açıklandığı üzere, Çinli kullanıcılar hukuka aykırı bir içeriğe eriştiğinde, onlara İnternette yapılan her şeyin kaydedildiğini ve kuralları ihlal edenlerin ihbar edilmesi gerektiğini belirten bir uyarıyla karşılaşmaktadır. Ayrıca, Çin'de sohbet odalarında propaganda yapması için kamu görevlilerini ajan provakatör olarak kullanmaktadır[201]. Bu sebeple, bireyler oto-sansür uygulayarak sakıncalı veya muhalif içeriğe erişmekten çekinmektedir.

IV. Güney Kore

Doğu Asya'da yer alan Güney Kore, 48 milyonu aşkın nüfusu ve 36 milyonu aşkın İnternet kullanıcısıyla dünyanın en yoğun İnternet kullanım oranına sahip ülkelerden birisidir[202]. 1982 yılında İnternet ağına dâhil olan Güney Kore, dünyanın en gelişmiş İnternet altyapısını kullanmaktadır[203]. Ayrıca, ülke genelinde geniş ağ bağlantısına sahip yaklaşık 30.000 İnternet kafe yer almaktadır[204]. Güney Kore mevcut İnternet altyapısı sayesinde e-devlet projelerini de çok hızlı bir şekilde hayata geçirmiştir[205].

---

[200] Bkz. yuk. §4 I D.

[201] *Goldsmith/Wu*, a.g.e., s. 98.

[202] Internet Usage in Asia, http://www.internetworldstats.com/stats3.htm.

[203] Deibert/Palfrey/Rohozinski/Zittrain, a.g.e., s. 370.

[204] İnternet kullanım oranlarının yüksek olması bireylerin alışkanlıklarını da köklü bir şekilde değiştirmiştir. Güney Kore'de İnternet medyasının gündemi belirlemede önemli bir gücü bulunmaktadır. Bu konudaki örnekler için bkz. Deibert/Palfrey/Rohozinski/Zittrain, a.g.e., s. 371.

[205] Güney Kore'nin İnternet altyapısını güçlendirmek ve İnterneti yaygınlaştırmak amacıyla yatırımlar yapmasının kamusal yönetimde üretkenliğin artırılması ve saydamlığın sağlamasından başka sebepleri de bulunmaktadır. Güney Kore İnternetin yaygınlaşmasın elektronik ticareti artıracağı, bilgi hizmetlerini yaygınlaştıracağı, yazılım ve içerik alanlarında yeni iş kolları oluşturacağı ve İSS'lerin belirli bir istihdam sağlayacağını, bu şekilde İnternetin işsizliğin azalmasına yardımcı olacağını öngörmektedir. Bkz. *Rao/Klopfenstein*, a.g.e., s. 124.

Güney Kore'de İnternet içeriğine farklı mevzuatlarda bulunan hükümlere göre müdahale edilmektedir. Bu mevzuatlardan en çok uygulama bulanı 1948 tarihli Ulusal Güvenlik Kanunu'dur[206]. Güney Kore, Kuzey Kore'den ayrılarak 1948 yılında bağımsızlığını kazanmasından sonra 1987 yılına kadar otoriter bir rejim tarafından yönetilmiş ve bu tarihten sonra demokratikleşme sürecine girmiştir. Buna rağmen Güney Kore, hâlâ komünizmi yakın tehdit olarak görmekte ve komünist sisteme sahip komşusu Kuzey Kore ile ilişkilerini kuruluşundan beri sınırlı düzeyde tutmaktadır.

Ulusal Güvenlik Kanunu, devlet aleyhtarı, demokratik özgürlük karşıtı ve komünist propagandanın hangi ortamda yapılırsa yapılsın cezalandırmaktadır[207]. Tarihi refleksleri sebebiyle ülkede en hassas engelleme sebebi Kuzey Kore'ye ilişkin içerik oluşturmaktadır. Düzenlemenin devlet aleyhtarlığı veya komünist propaganda gibi muğlâk fiilleri cezalandırması ifade hürriyeti alanındaki dengeyi vatandaşlar aleyhine bozmaktadır.

Ulusal Güvenlik Kanunu dışında İnternet içeriğine müdahaleye ilişkin hükümler içeren bir diğer düzenleme ise Telecommunications Business Act ("TBA")[208] isimli kanundur. Kanun, kamu güvenliğini, düzenini veya genel ahlakı ihlal eden her türlü içeriğin telekomünikasyon hatları üzerinden iletilmesini yasaklamaktadır[209]. Öte yandan 2004 yılında Güney Kore Seçim Kanunu'nda yapılan değişikliklerle, seçim dönemlerinde İnternet aracılığıyla politikacıların ve kampanyaların karalanması yasaklanmıştır[210].

İnternet ile ilgili temel politikalar TBA'ya göre kurulmuş The Korean Internet Safety Comission ("KISCOM")[211] tarafından belirlenmektedir.

---

[206] South Korea's National Security Law, http://www.hartford-hwp.com/archives/55a/205.html.

[207] *Deibert/Palfrey/Rohozinski/Zittrain*, a.g.e., s. 371.

[208] The Telecommunications Business Act, http://www.itu.int/ITU-D/treg/Legislation/Korea/BusinessAct.htm.

[209] *Deibert/Palfrey/Rohozinski/Zittrain*, a.g.e., s. 371.

[210] Public Official Election Act, http://www.nec.go.kr/english/res/Public_Official_Election.pdf.

[211] The Korean Internet Safety Comission, http://www.icec.or.kr.

KISCOM'un sakıncalı İnternet içeriğini belirleme ve engelleme konusunda devlete tavsiyelerde bulunma yetkisi bulunmaktadır. KISCOM ayrıca İnternette hukuka aykırı ve zararlı içeriği düzenli olarak takip etmektedir.

Güney Kore, İSS temelli otomatik engelleme sistemini kullanmaktadır. Devlet sakıncalı gördüğü web sitelerinin listesini oluşturmakta ve engellemenin gerçekleştirilmesi için ülke genelinde faaliyet gösteren İSS'lere göndermektedir. Güney Kore, bu şekilde 120.000'den fazla web sitesinin erişimi engellemiştir[212].

Güney Kore, Ulusal Güvenlik Kanunu'nda yer alan yasaklı içerikten sonra en çok pornografi, kumar ve korsan yazılıma ilişkin erişim engelleme yoluna gitmektedir[213]. Güney Kore, ülkesinde faaliyet gösteren arama motorlarının pornografik içerikli web sitelerine erişim için yaş doğrulaması yapmalarını zorunlu tutmaktadır. Bu doğrulama sisteme vatandaşlık numarasının girilmesiyle yapılmaktadır. Her ne kadar bu düzenlemenin çocukların zararlı içeriğe ulaşmasını engellemeye hizmet ettiği iddia ediliyorsa da, düzenleme kişisel verilerin güvenliğini tehlikeye soktuğu ve özel hayatın gizliliğini ihlal ettiği gerekçesiyle eleştirilmektedir. Güney Kore, bu şekilde dolaylı olarak ve sosyal teknikler kullanarak erişim engellemesini gerçekleştirmektedir.

İnternet içeriğini kontrol etmede en temel sorun içeriğin tanımlanmasında ortaya çıkmaktadır. Her erişim engelleme tekniğinin kendine özgü güçlü ve zayıf yönleri bulunmaktadır. Bir alan adı barındırdığı içerikle ilgili kesin bilgi vermemektedir. Benzer bir şekilde bir resmin veya videonun adı da gerçek içeriğini her zaman yansıtmamaktadır. Erişim engelleme sistemlerinden kurtulmak için içeriğin adını değiştirmek sık rastlanan bir durumdur. Buna karşın, ilkeli web siteleri kendi içeriklerini kendilerini etiketleyerek, kullanıcıların web sitesine erişmeden içerik hakkında bilgi sahibi olmasını mümkün kılmaktadır. Bu tür girişimler gönüllük esasına göre gerçekleştirilmekte ve birer netiquette örneği oluşturmaktadır[214]. Ne-

---

[212] *Deibert/Palfrey/Rohozinski/Zittrain*, a.g.e., s. 371.

[213] *Deibert/Palfrey/Rohozinski/Zittrain*, a.g.e., s. 370.

[214] Netiquette için bkz. dn. 22.

tiquette tekniğinin etkili olabilmesi için bu ilkelerin güvenilir bir makam tarafından doğrulanması gerekmektedir. Güney Kore devleti, ülkesinde barındırılan web siteleri için bu hizmeti kendisi vermektedir[215]. KISCOM tarafından sunulan İnternet içerik derecelendirme, sistemi web sitelerinin erişkin olmayan kişilerin erişimine uygunluğu konusunda değerlendirme hizmeti sağlamaktadır[216]. Web siteleri böylece ebeveynler ve okullar tarafından yaygın olarak kullanılan filtreleme programlarına uyumlu hale getirilmekte ve filtrelemelerin etkinliğini artırılmaktadır.

V. Singapur

Singapur Cumhuriyeti, Uzak Doğuda yer alan 4.657.542 nüfuslu bir ada devletedir ve 3.104.900 İnternet kullanıcısıyla dünyada en yoğun İnternet kullanım oranına sahip ülkelerden birisidir[217]. İnternet kullanım oranlarının bu kadar yüksek olması sebebiyle İnternetin toplumsal hayatta önemi büyüktür. Bu sebeple, bu çalışma kapsamına alınmıştır. İnternet kullanım oranlarına paralel olarak Singapur e-devlet projelerini de büyük ölçüde hayata geçirmiştir[218].

Singapur'da İnternet, Media Development Authority ("MDA") isimli kamu kurumu tarafından Class Licence Notification[219] ("CLN") ve Internet Code of Practice ("ICP")[220] isimli düzenlemelerdeki esaslara göre yönetilmektedir. MDA İnternet dâhil tüm medya mecralarında kamu menfaatlerine, kamu düzenine, ulusal birliğe ve ahlaka aykırı içerikleri engellemek için gereken tedbirleri almakla görevlendirilmiştir[221].

---

[215] *Rao/Klopfenstein*, a.g.e., s. 126.

[216] *Deibert/Palfrey/Rohozinski/Zittrain*, a.g.e., s. 371.

[217] Internet Usage in Asia, http://www.internetworldstats.com/stats3.htm.

[218] Article 19: Global Campaign for Free Expression, Freedom of Expression and the Media in Singapore, London 2005 ("*Article-19*"), s. 28.

[219] Class Licence Notification (1996), http://www.mda.gov.sg/wms.file/mobj/mobj.487.ClassLicence.pdf.

[220] Internet Code of Practice, http://www.mda.gov.sg/wms.file/mobj/mobj.981.internet_code_of_practice.pdf.

[221] ICP, m. 1.

Singapur, İnternet içeriğine sınırlı bir düzeyde müdahale etmektedir[222]. Ancak Singapur'un İnternet içeriğine müdahale etmemesi, İnternette yayınlanan içerikten dolayı sorumluluğun doğmadığı manasına gelmemektedir. Singapur'da hukuka aykırı içerikten dolayı hukuki ve cezai sorumluluğun ağır olması vatandaşları oto-sansüre itmektedir[223]. Ayrıca, diğer sosyal teknikler yaygın bir şekilde kullanılarak İSS'ler başta olmak üzere, tüm medya mecraları için kombine lisanslama yöntemleri kullanılmakta ve İnternet içerik politikaları ayrıntılı bir şekilde düzenlenmektedir[224]. Ülkede İSS'ler dâhil yerel gazeteler, televizyonlar ve radyo istasyonlarını da devletle farklı şekillerde ekonomik bağı olan şirketler işletmektedir[225].

CLN, İSS'lerin ve içerik sağlayıcıların uyması gerek idari yükümlülükleri düzenlemektedir. CLN, içerik sağlayıcıyı ticari, siyasi, dini veya başka bir amaçla İnternette bir içeriği yayına koyan kişi, topluluk, kurum veya kuruluş olarak tanımlamıştır[226]. CLN'ye göre, içerik sağlayıcıların aksi belirtilmediği sürece MDA'dan izin veya lisans almaksızın İnternette faaliyette bulunabileceklerini öngörmektedir. Ancak, siyasi ve dini içerikli web sitelerinin faaliyetlerine başlamalarından itibaren 14 gün içinde MDA nezdinde kendilerini tescil etmelerini zorunlu tutmuştur[227].

Yukarıda açıklandığı üzere, İnternet kullanım oranının yüksek olması sebebiyle İnternetin sosyal hayatta etkisi büyüktür. Yapılan bu düzenlemenin gerekçesi olarak her ne kadar toplumu derinden etkileyen siyasi ve dini konularda İnternetin kötüye kullanımını engellemek gösterilse de, bu düzenlemenin muhalif görüşleri bastırmak için kullanıldığı iddia edilmektedir. MDA ise İnternet içeriğini sansürlemediğini ve Singapur vatandaşlarının İnternetteki aktivitelerini takip etmekten ziyade, pornografi, aşırı şiddet ve ırksal ve dinsel ayrımcılığı önleme gibi amaçlarla hareket ettiğini iddia etmektedir.

---

[222] *Deibert/Palfrey/Rohozinski/Zittrain*, a.g.e., s. 365.

[223] *Deibert/Palfrey/Rohozinski/Zittrain*, a.g.e., s. 366.

[224] *Article-19*, a.g.e., s. 31.

[225] *Article-19*, a.g.e., s. 39.

[226] CLN, m. 2.

[227] CLN, m. 3.

ICP, servis ve içerik sağlayıcıların sorumluluk rejimini düzenlemektedir. Singapur servis sağlayıcıların ve içerik sağlayıcıların sorumluluğunu gelişen İnternet teknolojilerini de göz önüne alarak ayrıntılı bir şekilde düzenlemiştir. Söz konusu düzenlemeye göre tüm İSS'ler bu düzenlemenin gereklerine uymakla ve yasaklı kabul edilen içeriğe Singapur kullanıcılarının erişimini engellemek ile yükümlü tutulmuştur[228]. Ayrıca, İSS'ler MDA tarafından kendilerine iletilecek erişim engelleme kararlarını eşzamanlı olarak uygulamakla sorumlu kılınmışlardır. Gereken özenin gösterilmesi, sorumluluğun doğmaması için yeterli görülmektedir[229].

İçerik sağlayıcıların kural olarak İnternette sunulan içerikten dolayı sorumlu olduğu belirlendikten sonra, sorumluluğu kaldıran haller web sitesinde kullanılan İnternet servisinin özellikleri göz önüne alınarak ayrı ayrı düzenlenmiştir.

Sohbet grupları gibi özel yazışma servislerinde ICP'de yasaklanmış konular dışında bir konunun seçilmesi ve doğrudan veya dolaylı olarak bu tür içeriğe müsaade edilmemesi içerik sağlayıcının sorumluluğunu ortadan kaldırmaktadır[230]. İçeriğin başkaları tarafından oluşturulduğu ve genel kullanıma açık duyuru sayfaları ve forum gibi servislerin kullanılması durumlarında, içerik sağlayıcının olağan editörlük faaliyetleri sonucunda yasaklı içeriği kendisinin tespit etmesi veya kendisine bu yönde bir bildirimde bulunulması sonucu bu tür içeriğin engellenmesi sorumluluğu ortadan kaldırmaktadır[231]. Diğer İnternet servisleri için ise içerik sağlayıcının yasaklı içeriği kasten oluşturmadığı ve yasaklı içeriğin kaldırılması için gereken çabayı göstermesi sorumluluğun ortadan kalkması için yeterli görülmektedir[232]. Son olarak tüm içerik sağlayıcıların MDA tarafından kendilerine ihtar yapılması durumunda, içeriği engellemekle yükümlü tutulmuşlardır. Ancak bu hükmün editörlük yetkisi olmayan İnternet yayımcıları ile web sunucuları yöneticileri için uygulanmayacağı öngörülmüştür.

---

[228] ICP, m. 2.

[229] ICP, m. 3.

[230] ICP, m. 3 f. 3 (a).

[231] ICP, m. 3 f. 3 (b).

[232] ICP, m. 3 f. 3 (c).

ICP yasaklı içeriği kamu yararına, genel ahlaka, kamu düzenine ve güvenliğine, ulusal birliğe veya Singapur Kanunlarına aykırılık teşkil eden her türlü içerik olarak tanımlamıştır[233]. Bu kavramların geniş ve yoruma açık olmaları sebebiyle, yasaklı içeriğin belirlenmesinde göz önünde bulundurulması gereken esaslar ICP'de ayrıntılı olarak düzenlenmiştir.

ICP'nin 4. maddesine göre "(a) çıplaklık veya bir cinsel organın tasvirine ilişkin içerik; (b) cinsel şiddet içeren veya rızaya dayanmayan tecavüz veya benzeri taciz görüntüleri; (c) kişi veya kişileri açık bir cinsel ilişki içerisinde gösteren içerik; (d) 16 yaşın altındaki kişileri etken veya edilgen her türlü şekilde cinsel bir şekilde tasvir eden içerik; (e) eşcinsel, lezbiyen, ensest, sapık, hayvanlarla veya ölülerle cinsel ilişkiyi içeren her türlü içerik; (f) her türlü şiddet ve vahşet içeriği; (g) etnik, ırksal veya dinsel kin, kavga veya her türlü tahammülsüzlüğü öven, teşvik eden veya destekleyen içerik" yasaklı içerik olarak kabul edilmiştir. Ancak bu tür içeriğin tıbbi, bilimsel, sanatsal veya eğitimsel bir değeri varsa, içeriğin yasaklı içerik olarak değerlendirilmeyeceği kabul edilmiştir[234]. Son olarak, ICP ilgililerin bir içeriğin yasaklı içerik olup olmamasına yönelik şüpheleri varsa, MDA'ya başvurarak bu konuda karar vermesini talep etmesine olanak tanımaktadır[235]. ICP'de yer alan tüm bu sebeplerin dışında CLN İSS'lerin sundukları hizmetlerin loto, at yarışı, her türlü şans oyunu, astroloji ve her türlü falcılık, fuhuş veya izinsiz danışmanlık servisleri için kullanılmaması için gereken tedbirleri almakla yükümlü tutmuştur[236].

CLN ve ICP dışında Singapur'un seçim kanunlarında seçim dönemlerindeki İnternet yayınları için özel düzenlemeler bulunmaktadır. Söz konusu düzenleme siyasi partilerin ve siyasi konularda içerik sağlayan tüm web sitelerinin uymaları gereken esasları düzenlemekte ve özel seçim yasakları öngörmektedir[237].

---

[233] ICP, m. 4 f. 1.

[234] ICP, m. 4 f. 3.

[235] ICP, m. 4 f. 4.

[236] CLN, m. 15.

[237] Seçim dönemlerinde web sitelerinin siyasi parti reklamlarını yayınlamaları, aday tanıtımı yapmaları ve her türlü seçim anketi yapmaları yasaklanmıştır. Bu tür bir düzenlemenin yapılmasının gerekçesi olarak İnternetin bilgi kirliliğini artırdığı ve seçim dönemlerinde kötüye kullanıldığı gösterilmektedir. Daha fazla bilgi için bkz. *Article-19*, a.g.e., s. 46.

Yapılan bir araştırmada Singapur'da çoğu pornografik içerikli sadece yüze yakın web sitesinin engellendiği tespit edilmiştir[238]. Ayrıca Singapur devleti tüm içeriği filtrelemek yerine, sakıncalı kabul ettiği içeriğe erişildiğinde, içeriğin sakıncalı olduğunu gösteren bir mesajı göstermekle yetinmektedir. Pornografik içerikli web sitelerine yönelik sınırlı sayıda engellemenin devletin bu tür içeriğe yönelik hoşnutsuzluğunun bir göstergesi olarak sembolik niteliğe sahip olduğu düşünülmektedir[239].

VI. Suudi Arabistan

Suudi Arabistan, 28 milyon nüfusa ve 7 milyon İnternet kullanıcısına sahip bir devlettir[240]. İnterneti düzenleme yönünde ilk resmi girişim Suudi Arabistan devleti tarafından gerçekleştirilmiştir[241]. Suudi Arabistan, İnternet içeriğine ilk kullanmaya başladığı tarihten itibaren müdahale etmektedir. Ayrıca, İnterneti ancak tamamen kontrol edebileceği hususunda tatmin olduktan sonra kamusal kullanıma açmıştır.

Suudi Arabistan'da İnternetin teknik yönetimi King Abdulaziz City for Science and Technology ("KACST") kurumuna bağlı İnternet Hizmetleri Birimi tarafından yönetilmektedir. Ülke genelinde 21 İSS faaliyet göstermekte ve tüm ülke ağı ile uluslararası ağ arası bağlantı KACST tarafından yönetilmektedir. Ayrıca içerik engelleme konusunda KASCT yetkilendirilmiştir ve bu tür içeriğe ilişkin re'sen erişim engelleme kararı verilebilmektedir[242]. Diğer içeriğin engellenebilmesi için devletin ilgili birimleri tarafından bu yönde bir talepte bulunulması gerekmektedir. KASCT, ayrıca İnternet kullanıcılarının sakıncalı içeriği bildirmesi etmesi için özel bir ihbar sistemi kurmuştur.

Suudi Arabistan devleti Çin gibi ülke geneline yayılmış gelişmiş bir erişim engelleme sistemi kullanmaktadır. Erişim engelleme için Ameri-

---

238 *Deibert/Palfrey/Rohozinski/Zittrain*, a.g.e., s. 367.

239 *Deibert/Palfrey/Rohozinski/Zittrain*, a.g.e., s. 367.

240 Middle East Internet Usage and Population Statistics, http://www.internetworldstats.com/stats5.htm.

241 *Deibert/Palfrey/Rohozinski/Zittrain*, a.g.e., s. 361.

242 *Deibert/Palfrey/Rohozinski/Zittrain*, a.g.e., s. 362.

kan Super Computing firmasının geliştirdiği SmartFilter yazılımı kullanılmaktadır. Bu yazılım sayesinde ülke genelindeki İnternet trafiğini her çıkış noktasında otomatik engelleme yöntemine göre denetlemektedir.

Devlet birçok batılı devletin aksine İnternet erişim politikasını gizlememekte ve kamuyla paylaşmaktadır. Suudi Arabistan'da İnternet içeriğine temelde sosyal ve siyasal iki sebeple müdahale edilmektedir. 2001 yılında Suudi Bakanlar Kurulu İnternet kullanıcılarının erişmesi ve yayınlaması yasak olan içeriğe ilişkin bir direktif yayınlamıştır[243]. Direktif, ulusal birliği ihlal eden, İslam aleyhtarı olan ve kamu düzenine aykırılığı teşkil eden her türlü içeriğe erişimi ve bu tür içeriğin her türlü ortamda yayınlanmasını yasaklamıştır. Ayrıca 2006 yılında yapılan başkaca bir düzenleme ile vatandaşların kişilik haklarını ihlal eden, Suudi Hukuku ve İslami değerlere aykırılık aykırı olan ve terör örgütlerine hizmet veren her türlü içerik sebebiyle cezai sorumluluğun doğacağı kabul edilmiştir[244].

Ülke genelinde erişimi engellenen içeriğin büyük bir kısmını pornografik içerik oluşturmaktadır[245]. Pornografik içerikten sonra kumar, içki ve uyuşturucu gibi konularla ilgili içerik barındıran web sitelerinin erişimi engellenmektedir. Ayrıca proxy sunucular ve online çeviri araçları da engelleme sistemine takılmaktadır. Ülke genelinde otomatik engelleme yöntemi kullanıldığı için bu tür web sitelerinin takibi ayrıca yapılmamakta, SmartFilter yazılımının veritabanında yer alan kara liste referans alınmaktadır[246].

Ulusal güvenlik ve kamu düzeninin ihlal edilmesi gibi muğlak sebeplerin erişim engellemesi için esas kabul edilmesi düzenlemenin siyasal iktidarlar tarafından istismarına yol açmıştır. Yapılan düzenlemenin ifade hürriyetini aşırı sınırladığı ve muhalif görüşleri susturmak

---

[243] Arab Media: Saudi internet rules, http://www.al-bab.com/media/docs/saudi.htm.

[244] Düzenlemenin asıl amacının e-devlet uygulamalarının etkin bir şekilde işlemesi için veri güvenliğini sağlamak olduğu iddia edilmektedir. Bkz. Saudi Arabia: New Act on Cyber-Crimes will Boost e-Governance, https://www.zawya.com/story.cfm/sidZAWYA20070410055304.

[245] *Deibert/Palfrey/Rohozinski/Zittrain*, a.g.e., s. 362.

[246] Bu yöntem engellenecek web siteleri için son kararı devletler yerine özel şirketler vermiş olduğu için eleştirilmektedir. Bkz. yuk. §3 IV A.

için kullanıldığı iddia edilmektedir. Benzer bir şekilde İnternet kafeler gibi İnternet toplu kullanım sağlayıcıları da sıkı denetime tabidir. Bu tür yerler devlet tarafından öngörülen filtreleme yazılımlarını kullanmakla yükümlü tutulmuştur.

§ 6. TÜRK HUKUKUNDA ERİŞİMİN ENGELLENMESİ

I. İnternet ile ilgili yetkili kurumlar

A. Bilgi Teknolojileri ve İletişim Kurumu

Türkiye'de telekomünikasyon sektörü 2813 sayılı Bilgi Teknolojileri ve İletişim Kurumunun Kuruluşuna İlişkin Kanun[247] ile kurulan Bilgi Teknolojileri ve İletişim Kurumu ("BTK") tarafından düzenlenmektedir[248]. Kurumun ilişkili olduğu bakanlık Ulaştırma Bakanlığı'dır.

Kurumun İnternet ile ilgili temel yetkileri İnternet içeriğine ilişkin müdahale yetkisi veren 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanununda[249] öngörülmüştür. Kanunla verilen görevler, Kurum bünyesinde bulunan Başkanlıkça yerine getirilmektedir[250]. Bu doğrultuda Başkanlık, İnternet içeriğinin takip ve engellenmesi, içerik, yer, erişim ve İnternet toplu kullanım sağlayıcılara ilişkin yetkilendirme, gözetim ve denetim faaliyetlerinin gerçekleştirilmesi ve filtreleme yazılımlarının standartlarının belirlenmesi gibi yetkilerle donatılmıştır.

---

[247] Kanun No: 2813, Kabul T.: 05.04.1983, RG 07.04.1983/18011.

[248] 5.11.2008 t. ve 5809 sayılı Elektronik Haberleşme Kanunun 67. maddesinin 2. fıkrası hükmü gereğince "Telsiz Kanunu" adı "Bilgi Teknolojileri ve İletişim Kurumunun Kuruluşuna İlişkin Kanun" ve "Telekomünikasyon Kurumu"nun adı "Bilgi Teknolojileri ve İletişim Kurumu" olarak değiştirilmiştir. RG 10.11.2008/27050(Mükerrer).

[249] Kanun No: 5651, Kabul T.: 04.05.2007, RG 23.05.2007/26530.

[250] 5651 sayılı Kanun, m. 10.

Öte yandan, 5809 sayılı Elektronik Haberleşme Kanunun 35. maddesi İnternet alan adlarının tahsisini yapacak kurum veya kurulusun tespiti ile alan adı yönetimine ilişkin usul ve esasları belirleme görev ve yetkilerini Ulaştırma Bakanlığı'na vermiştir. Ulaştırma Bakanlığı 03.03.2009 tarihli ve 321 sayılı kararı ile "İnternet Alan Adları" tahsisine ilişkin iş ve işlemlerin yürütülmesi hususunda BTK'yı yetkilendirmiştir. Ayrıca Bakanlık, alan adlarının yönetim esaslarına ilişkin İnternet Alan Adları Yönetmeliği Taslağı'nı hazırlamıştır[251]. Böylece, Türkiye'de alan adları yönetimi hukuki bir zemine kavuşturulmuştur[252].

Bu kanun dışında Kurumun 5369 sayılı Evrensel Hizmetin Sağlanması Hakkında Kanun[253] gereğince önceden belirlenmiş kalitede ve herkesin karşılayabileceği makul bir bedel karşılığında asgari standartlarda İnternet erişimi dâhil elektronik haberleşme hizmetlerinin ülke genelinde herkes tarafından erişilebilirliğini sağlamakla ilgili yetki ve görevleri bulunmaktadır. Son olarak kurum Telekomünikasyon Kurumunun Teşkilat ve Görevleri ile Çalışma Esas ve Usulleri Hakkında Yönetmelik[254] uyarınca İnternet hizmet sağlayıcılara ilişkin idari bazı faaliyetleri gerçekleştirmektedir.

B. Telekomünikasyon İletişim Başkanlığı

Telekomünikasyon İletişim Başkanlığı ("TİB"), 5397 sayılı Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun[255] uyarınca BTK bünyesinde 2005 yılında kurulmuştur. Başkanlığın oluşturulma amacı olarak 2559 sayılı Polis Vazife ve Salahiyet Kanunu[256], 2803 sayılı Jandarma Teşkilat, Görev ve Yetkileri Kanunu[257], 2937 sayılı Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanunu[258] ve 5271 sayılı Ceza Muhakemesi Ka-

---

[251] İnternet Alan Adları Yönetmeliği Taslağı, http://www.tk.gov.tr/Basin_Duyurular/Duyurular/kamuoyu/2009/Internet_Alan_Adlari_Yonetmelik_Taslagi.doc.

[252] ODTÜ'ye yönelik eleştiriler için bkz. *Canbay*, a.g.e., s. 155; Ayrıca bkz. dn. 82.

[253] Kanun No: 5369, Kabul T.: 16.06.2005, RG 26.06.2005/25856.

[254] RG 17.02.2001/24321.

[255] Kanun No: 5397, Kabul T.: 03.07.2005, RG 23.07.2005/25884.

[256] Kanun No: 2559, Kabul T.: 04.07.1934, RG 14.07.1934/2751.

[257] Kanun No: 2803, Kabul T.: 10.03.1983, RG 12.03.1983/17985.

[258] Kanun No: 2937, Kabul T.: 01.11.1983, RG 03.11.1983/18210.

nununa ("5271 sayılı CMK")[259] tabii iletişim izlenmesi ve tespit edilmesi uygulamalarında yetkileri merkezileştirmek ve tek bir birimde toplamak olduğu gösterilmektedir[260].

Başkanlığın İnternet ile ilgili temel yetkileri 5651 sayılı Kanununda öngörülmüştür. Başkanlık 5651 sayılı Kanunun kapsamına giren suçları oluşturan içeriğe sahip faaliyet ve yayınları önlemek ile yetkilendirilmiştir. Bu doğrultuda, İnternet ortamında yapılan yayınların içeriklerini izlemek ve ilgili suçların tespit edilmesi halinde 5651 sayılı Kanunda öngörülen tedbirleri almakla yükümlü tutulmuştur. Başkanlık içerik izlemenin hangi seviye, zaman ve şekilde yapılacağını kendisi tespit etmektedir. Başkanlık ayrıca İnternet sektöründe faaliyet gösteren, yer ve servis sağlayıcılara ilişkin yetkilendirmeleri ve filtreleme ve bloke etmede kullanılacak sistemlerinde kullanılacak donanım ve yazılımlara ilişkin tüm usul ve esasları belirlemektedir.

C. İnternet Kurulu

İnternet Kurulu, 3348 sayılı Ulaştırma Bakanlığı Teşkilat ve Görevleri Hakkındaki Kanunun[261] Ek-1 maddesi ve 5651 sayılı Kanunun 10. maddesi çerçevesinde Ulaştırma Bakanlığınca kurulmuştur. Kurulun ana işlevi Türkiye'de İnternetin alt yapıdan başlayarak tüm boyutları ile kısa, orta ve uzun vadeli hedeflerini belirlemek ve bu hedeflere erişmek için gerekli ulusal kararların uygulanması gibi konularda Ulaştırma Bakanlığı'na danışmanlık yapmaktır. Kurul, Adalet Bakanlığı, İçişleri Bakanlığı, çocuk, kadın ve aileden sorumlu Devlet Bakanlığı ile BTK ve ihtiyaç duyulan diğer bakanlık, kamu kurum ve kuruluşları ile İnternet servis sağlayıcıları ve ilgili sivil toplum kuruluşları arasından seçilecek bir temsilcinin katılımıyla teşkil edilmektedir[262].

---

[259] Kanun No: 5271, Kabul T.: 04.12.2004, RG 17.12.2004/25673.

[260] TBMM Dönem: 22, Yasama Yılı: 3, Yalova Milletvekili Şükrü Önder'in; Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun Teklifi ve İçişleri Komisyonu Raporu (2/546), http://www.tbmm.gov.tr/sirasayi/donem22/yil01/ss962m.htm.

[261] Kanun No: 3348, Kabul T.: 09.04.1987, RG 17.04.1987/19434.

[262] Kurul üyeleri için bkz. http://kurul.ubak.gov.tr/netkrl/ik_kurul_uyeleri.

D. Radyo Televizyon Üst Kurulu

Radyo Televizyon Üst Kurulu ("RTÜK"), 3984 sayılı Radyo ve Televizyonların Kuruluş ve Yayınları Hakkında Kanun[263] uyarınca radyo ve televizyon faaliyetlerini düzenlemek amacıyla, özerk ve tarafsız bir kamu tüzelkişisi olarak kurulmuştur.

RTÜK'ün İnternet içeriğine müdahalesi 2002 yılına kadar uydu ya da karasal vericilerden yapılan radyo ve televizyon yayınlarının İnternete aktarımı noktasında ortaya çıkmaktaydı[264]. Ancak, 2002 yılında 3984 sayılı RTÜK Kanununun 31. maddesinde değişiklik yapılarak[265] RTÜK'ün her türlü teknoloji ile ve her tür iletişim ortamında yapılacak yayın ve hizmetlerin usul ve esaslarını Haberleşme Yüksek Kurulunun belirleyeceği strateji çerçevesinde Üst Kurulca tespit edileceğini ve Haberleşme Yüksek Kurulunun onayına sunulacağı öngörülmüştür. Ayrıca bu yayın ve hizmetlerin mevzuata uygunluğunun Üst Kurulca denetleneceği kabul edilmiştir. Bu değişiklik yapıldığı dönemde "her türlü iletişim ortamında yapılacak yayın ve hizmetler" kapsamına İnternetin gireceğini ve sadece İnternet üzerinden yapılan radyo ve televizyon yayınlarının denetimi dışında RTÜK'ün İnternet içeriğine müdahale edebileceği düşünülmüştür[266]. Ancak, 3984 sayılı RTÜK Kanunun 1. maddesinde açıkça RTÜK'ün yetkisinin radyo ve televizyon yayınlarının düzenlenmesi ile sınırlı tutmasından dolayı 31. maddedeki düzenleme RTÜK'ün İnternet içeriğine kapsamlı olarak müdahalesine olanak vermemiştir. RTÜK de yetkilerini geniş yorumlayarak İnternet içeriğine herhangi bir müdahalede bulunmamıştır[267].

II. 5651 sayılı Kanunu öncesi erişim engellemeleri

1993 yılında İnternet ağına dâhil olan Türkiye, 2001 yılına kadar diğer devletlerin aksine İnternete önemli bir müdahalede bulunmamıştır.

[263] Kanun No: 3984, Kabul T.: 13.04.1994, RG 20.04.1994/21911.

[264] Gürsel Öngören, İnternet Hukuku, İstanbul 2006 ("Öngören"), s. 26.

[265] Radyo ve Televizyonların Kuruluş ve Yayınları Hakkında Kanun, Basın Kanunu, Gelir Vergisi Kanunu ile Kurumlar Vergisi Kanununda Değişiklik Yapılmasına Dair Kanun, Kanun No: 4756, Kabul T.: 15.05.2002, RG 21.05.2002/24761.

[266] *Öngören*, a.g.e., s. 26; Ayrıca bkz. *Akdeniz/Altparmak*, a.g.e., s. 6.

[267] *Öngören*, a.g.e., s. 27.

Türk Hukukunda, 5651 sayılı Kanundan önce erişim engellemesi farklı kanun hükümlerine dayanılarak gerçekleşmiştir. Bazı web siteleri TSK'ya hakaret, yolsuzluk söylentileri, Türklük karşıtı veya terörist propaganda, hakaret ve kumara ilişkin içerik bulundurdukları iddiasıyla engellenmiştir[268]. Ayrıca, çocuk pornografisine ilişkin yapılan çeşitli operasyonlarla eşzamanlı olarak bazı web sitelerinin erişimi engellenmiştir. Son olarak Türkiye Bağlantılı Hak Sahibi Fonogram Yapımcıları Meslek Birliği ("MÜYAP") Türk sanatçılarının bulunduğu korsan müzik ve videolar içeren 2005 yılında 153, 2006 yılında 886 ve 2007 yılında 549 web sitesinin erişimini engelletmiştir[269].

III. 5651 sayılı Kanunun hazırlık süreci

5651 sayılı Kanun yürürlüğe koyulmadan önce İnternet içeriğine müdahale amacıyla müdahale için farklı sebep ve usulleri öngören iki kanun tasarısı ve bir kanun teklifi hazırlanmıştır. 5651 sayılı Kanun, bu tasarı ve teklifler üzerinde gerçekleşen tartışmalar ile şekillenerek bugünkü halini almıştır.

A. Bilişim Ağı Hizmetlerinin Düzenlenmesi ve Bilişim Suçları Hakkında Kanun Tasarısı

İnternet içeriğinin özel bir kanunla düzenlenmesine yönelik ilk girişim 2006 yılında Adalet Bakanlığı tarafından gerçekleştirilmiştir. 5237 sayılı TCK'nın[270] aynı dönemde yürürlüğe girmesine ve 243 ila 246. maddeler arasında bilişim suçlarına ilişkin hükümler içermesine rağmen Adalet Bakanlığı İnternet suçlarıyla mücadele amacıyla yeni bir kanun taslağı üzerinde çalışmaya başlamıştır. Bilişim Ağı Hizmetlerinin Düzenlenmesi ve Bilişim Suçları Hakkında Kanun Tasarısı başlıklı taslak metin içerik, yer ve servis sağlayıcıların kurumsal sorumluluğunun yanı sıra 243 ila 246. maddelerin kaldırılması ve kimlik hırsızlığı, hacking, çocuk

---

[268] *Akdeniz/Altıparmak*, a.g.e., s. 9.

[269] Erişim engellemelere ilişkin diğer örnekler için bkz. Türkiye'de Site Erişime Kapatmalarının Tarihçesi, http://turk.internet.com/haber/yazigoster.php3?yaziid=20909.

[270] Kanun No: 5397, Kabul T.: 03.07.2005, RG 23.07.2005/25884.

pornografisi, kumar ve kamu güvenliği gibi hükümler içermekteydi[271]. Tasarı bu suçların zaten 5237 sayılı TCK'da yer alması ve bazı suçların cezasını orantısız olarak artırması sebebiyle eleştirilmiştir[272]. Ayrıca 5237 sayılı TCK yürürlüğe koyulduğu zaman, ceza hükümlerinin temel kanunlarda toplanacağı, özel ceza kanunları yapılmayacağı belirtilmiş olması sebebiyle Adalet Bakanlığının bu girişimi kamuoyunda gereken desteği bulmamıştır[273].

B. Bilişim Sistemi Üzerinden Suç Teşkil Eden Zararlı Yayınlarla Mücadele Hakkında Kanun Teklifi

Bilişim Sistemi Üzerinden Suç Teşkil Eden Zararlı Yayınlarla Mücadele Hakkında Kanun Teklifi ("Teklif"), İstanbul Milletvekili Gülseren Topuz tarafından 18.12.2006 tarihinde TBMM'ye sunulmuştur[274]. Teklif, Avrupa Birliği E-Ticaret Direktifinin hükümleri göz önüne alınarak, bilişim ağlarının ortaya çıkardığı hukuki sorunları çözme amacıyla hazırlandığı belirtilmiştir[275]. Bilgiye erişim hakkının ve ifade hürriyetinin esas olduğunu ve ancak kanunla sınırlanabileceğini belirten Teklif, içerik, servis ve İnternet toplu kullanım sağlayıcılarının sorumluluklarını ayrıntılı olarak düzenlemiştir. Ayrıca çocukların cinsel istismarı suçu, şiddet içerikli yayınlara yönelik suçları, kumar ve sahtecilik suçlarını yeniden tanımlamıştır.

Teklif bu haliyle 5237 s. TCK'da yer alan suçları yeniden tanımladığı için Adalet Bakanlığı'nın hazırlamış olduğu metinden nitelik olarak bir farkı bulunmamaktaydı. Buna rağmen Teklif 2007 yılında Elektronik Ortamda İşlenen Suçların Önlenmesi ile 2559 ve 2937 sayılı Kanunlarda Değişiklik Yapılmasına Dair Kanun Tasarısı ile birleştirilmiştir.

---

[271] Taslak metin için bkz. Bilişim Ağı Hizmetlerinin Düzenlenmesi ve Bilişim Suçları Kanun Tasarısı, Kişisel Verilerin Korunması Hakkında Kanun Tasarısı, http://bt-stk.org.tr/bilisim-hizmetler-suclari.html.

[272] *Akdeniz/Altıparmak*, a.g.e., s. 11.

[273] *Akdeniz/Altıparmak*, a.g.e., s. 11.

[274] Teklif metni için bkz. http://www2.tbmm.gov.tr/d22/2/2-0958.pdf.

[275] E-Ticaret Yönergesi için bkz. dn. 169.

C. Elektronik Ortamda İşlenen Suçların Önlenmesi ile 2559 ve 2937 sayılı Kanunlarda Değişiklik Yapılmasına Dair Kanun Tasarısı

Ulaştırma Bakanlığı 2007 yılında bilişim suçlarının önlenmesi amacıyla yeni bir Elektronik Ortamda İşlenen Suçların Önlenmesi ile 2559 ve 2937 sayılı Kanunlarda Değişiklik Yapılmasına Dair Kanun Tasarısı ("Tasarı") üzerinde çalışmaya başlamıştır. Hazırlanan Tasarı 12.02.2007 tarihinde TBMM'ye sunulmuştur[276].

1. Genel gerekçe

Bilişim suçlarıyla ilgili yeni bir tasarının hazırlanması ve bu doğrultuda yeni bir kurumsal yapının oluşturulmasının gerekçesi olarak elektronik ortamda işlenen suçların hızlı bir şekilde artması ve bu suçların işlenmesindeki kolaylığa rağmen tespit edilmesinin zor olması ve toplumsal açıdan doğabilecek zararların sonradan telafisinin mümkün olmaması gösterilmiştir[277]. Bu doğrultuda, 5237 sayılı TCK'nın bilişim suçlarını düzenleyen 243 ve devamında yer alan ilgili hükümlerin, 1117 sayılı Küçükleri Muzır Neşriyattan Koruma Kanunun[278], 4320 sayılı Ailenin Korunmasına Dair Kanunun[279] ve 5395 sayılı Çocuk Koruma Kanunun[280] bilişim teknolojilerinde yaşanan hızlı gelişmeler sebebiyle İnternet ortamında yapılan ve içerikleri suç teşkil eden yayınların önlenmesinde yetersiz kaldığı belirtilmiştir.

Tasarı, Anayasanın 41. maddesinde ailenin ve 58. maddesinde gençliğin korunmasına yönelik tedbirleri almakla ilgili devlete verdiği yetkiye dayanarak, aileyi, çocukları ve gençleri İnternet dâhil elektronik iletişim araçlarının kötüye kullanılmasıyla uyuşturucu ve uyarıcı madde alışkanlığı, intihara yönlendirme, cinsel istismar, kumar ve benzeri kötü alışkanlıkları teşvik eden içerikten korumak amaçlarıyla hazırlanmıştır.

[276] Tasarı metni ve genel gerekçesi için bkz. http://www2.tbmm.gov.tr/d22/1/1-1305.pdf.

[277] Genel gerekçe, s. 1.

[278] Kanun No: 1117, Kabul T.: 21.06.1927, RG 07.07.1927/627.

[279] Kanun No: 4320, Kabul T.: 14.01.1998, RG 17.01.1998/23233.

[280] Kanun No: 5395, Kabul T.: 03.07.2005, RG 15.07.2005/25876.

Tasarı bu hedeflere ulaşmak için Adalet Bakanlığı tarafından daha önce hazırlanan metin ve Gülseren Topuz tarafından sunulan teklifin aksine bilişim suçlarını yeniden tanımlamamıştır. Ayrıca, suçlar işlendikten sonra devreye girecek cezai ve idari yaptırımlar getirmemiştir. Bunun yerine Tasarıyı hazırlayanlar, 5237 sayılı TCK'da yer alan belirli suçların İnternet dâhil elektronik ortamda etkilerini sürdürmesinin önlenmesi için idari ve yargısal koruma tedbiri olarak iki yeni yöntemi düzenlemekle yetindiklerini belirtmişlerdir.

2. Adalet Komisyonu raporu

15.01.2007 tarihinde Adalet Komisyonuna gönderilen Tasarı, komisyonda usul ve esas açısından önemli değişikliklere uğramıştır[281]. Öncelikle Tasarının adı Komisyonda İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun Tasarısı olarak değiştirilmiştir. Değişikliğin gerekçesi olarak, elektronik ortamın mobil ve sabit telefonlar başta olmak üzere, telsiz, faks, telgraf gibi haberleşme araçları ile radyo ve televizyon gibi yayın araçlarını da kapsayan çok geniş bir ifade olduğu; bu durumun başta Anayasanın Cumhuriyetin nitelikleri başlıklı 2. maddesi olmak üzere, Haberleşme hürriyeti başlıklı 22. maddesine ve Basın hürriyeti başlıklı 28. maddesine aykırı olması gösterilmiştir.

Komisyonda içerik, yer ve erişim sağlayıcıların İnternet ortamındaki yayın içeriklerinde belirli bilgileri bulundurmak gibi bazı yükümlülükler getirilmiştir. Ayrıca içerik sağlayıcının İnternet ortamında kullanıma sunduğu içerikten dolayı hem hukuki hem de cezai sorumluluğu bulunduğuna ilişkin hüküm eklenmiş ve içerik sağlayıcının bağlantı sağladığı başkasına ait içerikten dolayı sorumluluğunun esasları belirlenmiştir.

Öte yandan, Avrupa Konseyi tarafından hazırlanarak 23 Kasım 2001 tarihinde Budapeşte'de imzaya açılan Siber Suç Sözleşmesi[282] ve

[281] Adalet Komisyonu raporu, Esas No: 1/305, 2/958 (12.04.2007), Karar No: 122; Rapor metni için bkz. http://www.tbmm.gov.tr/sirasayi/donem22/yil01/ss1397m.htm.

[282] Council of Europe - Convention on Cybercrime, http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm; Türkçe çeviri için bkz. http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/ConventionOtherLg_en.asp.

Almanya'nın 22 Temmuz 1997 tarihli Tele Hizmetler Kanunu[283] hükümleri göz önüne alındığı belirtilerek yer, erişim ve İnternet toplu kullanım sağlayıcıların cezai ve idari sorumluluklarına ilişkin hükümler getirilmiştir.

Tasarıda yer alan erişimin engellemesi kararlarının hangi suçlarla ilgili olarak uygulanabileceğine ilişkin hüküm Komisyonda aynı şekliyle benimsenmiş ve bu suçların sayma yöntemiyle belirlendiği açıkça belirtilmiştir. Bu doğrultuda 5237 sayılı TCK'da yer alan intihara yönlendirme (m. 84), çocukların cinsel istismarı (m.103, f.1), uyuşturucu veya uyarıcı madde kullanılmasını kolaylaştırma (m. 190), sağlık için tehlikeli madde temini (m. 194), müstehcenlik (m. 226), fuhuş (m. 227), kumar oynanması için yer ve imkân sağlama (m. 228) suçları erişim engelleme sebepleri olarak kabul edilmiştir. Bu sebeplere ilişkin engellenmesi kararı verilebilmesi için içerik veya yer sağlayıcının Türkiye'de veya yurtdışında bulunması arasında bir ayrım gözetilmemiştir.

Tüm bu aşamalarda, engellemelerin Anayasanın uluslararası sözleşmelerde belirlenen esaslarla güvence altına aldığı ifade hürriyetine kısıtlama oluşturmaması için suçların çocukların ve gençlerin olumsuz etkilenebileceği çocukların istismar edilmesi ve müstehcenlik gibi suçlarla sınırlı tutulduğu iddia edilmiştir. Ayrıca, erişim engelleme tedbir kararlarına karşı da yargı yolu açık olduğu için getirilen düzenlemelerin sansür olarak nitelendirilemeyeceği belirtilmiştir.

Komisyon müzakereleri sırasında 5816 sayılı Atatürk Aleyhine İşlenen Suçlar Hakkında Kanun'da[284] yer alan suçlar ile 5237 sayılı TCK'nın 302. maddesinde yer alan devletin birliğini ve ülke bütünlüğünü bozma suçu ve Anayasanın 174. maddesinde güvence altına alınan İnkilap Kanunların erişim engelleme sebepleri arasına alınması önerilmiştir. Bu önerilerden sadece 5816 sayılı Kanunda yer alan suçlara ilişkin olanı kabul edilmiştir. 302. madde ile İnkilap Kanunlarına ilişkin olan öneri söz konusu suçların İnternet ortamında yapılan yayınlar yoluyla işlenemeyeceği göz önünde bulundurularak kabul edilmemiştir.

---

[283] Gesetz über die Nutzung von Telediensten (Teledienstegesetz -TDG), http://net-law.de/gesetze/tdg.htm.

[284] Kanun No: 5816, Kabul T.: 25.07.1951, RG 31.07.1951/7872.

Son olarak Komisyonda, 5187 sayılı Basın Kanununun[285] cevap ve düzeltme hakkının kullanılmasına ilişkin hükümleri göz önünde bulundurularak, İnternet ortamında yapılan yayınlarla kişilik haklarına saldırıda bulunan kişilerin bu nitelikteki içeriğin yayından çıkarılması ve buna karşı cevap hakkını ne şekilde kullanabileceğine ilişkin yayından çıkarma ve cevap hakkı başlıklı ayrı bir hüküm eklenmiştir.

3. TBMM müzakereleri

Tasarı 04.05.2007 tarihli TBMM Genel Kurulunda gündeme alınmıştır[286]. Tasarı Meclis müzakereleri sırasında esaslı bir değişikliğe uğramamıştır. Genel Kurulda, Adalet Komisyonunda 302. madde ile İnkilap Kanunlarının erişim engelleme sebepleri arasına alınmasına ilişkin yapılan öneri yenilenmiş ancak kabul edilmemiştir[287].

Genel Kurul müzakereleri sırasında en çok 5187 sayılı Basın Kanunundan mülhem yayından çıkarma ve cevap hakkına ilişkin hüküm eleştirilmiştir. Öncelikle, hakaret suçunun katalog suçlar arasında yer almamasına rağmen cevap ve düzeltme hakkı kapsamında hakaret suçuyla ilgili bir usulün belirlenmesi yerinde görülmemiştir. Ayrıca, İnternetteki bazı faaliyetlerin basın faaliyeti olarak nitelendirilmesi kabul edilmesine rağmen İnternetin sadece basın faaliyeti gibi algılanması ve İnternetin kendine özgü yapısı göz önüne alınmadan Basın Kanunu hükümlerinin aynen Tasarıya işlenmesi eleştirilmiştir. Son olarak, basın yayın faaliyeti yapmayan kişilerin, sahip oldukları web siteleri sebebiyle basın yayın kuruluşlarını ilgilendiren bir sorumluluğa tabi tutulmalarının doğru olmadığı ifade edilmiştir. Tüm bu eleştirilere rağmen, içeriğin yayından çıkarılması ve cevap hakkına ilişkin hükmün kaldırılmasına yönelik öneri kabul edilmemiştir.

---

[285] Kanun No: 5187, Kabul T.: 09.06.2004, RG 26.06.2004/25504.

[286] 22. Dönem 5.Yasama Yılı 99. Birleşim; Genel Kurul Tutanağı için bkz. http://www.tbmm.gov.tr/develop/owa/tutanak_g_sd.birlesim_baslangic?PAGE1=1&PAGE2=1&p4=19906&p5=B.

[287] TCK'nın 302. maddesinin kapsama alınmasına gerekçe olarak İnternette Türkiye'nin bütünlüğü aleyhinde propagandalar yapılması gösterilmiştir. Bu doğrultuda, Google Earth programında Diyarbakır'ı Kuzey Kürdistan'ın başkenti yaptığı yönündeki haberler örnek gösterilmiştir. Bkz. Genel Kurul Tutanağı, s. 69.

Son olarak Genel Kurulda izleme, filtreleme ve sakıncalı İnternet içeriğine erişimin engellenmesi konusunda politika belirleyecek yeni bir kurulun oluşturulması önerilmiştir[288]. Bu öneri kabul görmüş ve Tasarının 10. maddesine bu yönde hüküm eklenmiştir.

04.05.2007 tarihli TBMM Genel Kurulunda kabul edilen Tasarı ve 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun olarak 23.05.2007 tarih ve 26530 sayılı Resmi Gazete'de yayımlanarak yürürlüğe girmiştir[289].

IV. 5651 sayılı Kanuna göre İnternet erişiminin engellenmesi

5651 sayılı Kanun yürürlüğe koyulmadan önce farklı esaslara göre İnternet içeriğine müdahale edilmekteydi[290]. 5651 sayılı Kanunun gerekçesinde belirtildiği üzere, geleneksel idari ve cezai önlemlerin İnternet içeriğini denetlemeye ve bilişim suçlarıyla mücadele için yetersiz kalması sebebiyle 5651 sayılı Kanun gibi özel bir kanun yürürlüğe konmuştur. Bu şekilde Türk Hukukundaki İnternet içeriğine müdahale politikası tek bir metin altında toplanmış bulunmaktadır. 5651 sayılı Kanun cezai ve idari hükümlerin yanı sıra yayından çıkarma ve cevap hakkı gibi özel hukuku ilgilendiren kurallar içerdiği için *sui generis* bir nitelik taşıdığı kabul edilmektedir[291].

5651 sayılı Kanunun uygulama esasları 30.11.2007 tarihli İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik'te ("Uygulama Yönetmeliği")[292] belirlenmiştir. Bu yönetmelik dışında Başbakanlık tarafından erişim ve yer sağlayıcılarla ilgili olarak 24.10.2007 tarihli Telekomünikasyon Kurumu Tarafından

---

[288] Kurul hakkında daha fazla bilgi için bkz. yuk. §6 I C.

[289] Kanunun 13. maddesi uyarınca, Kanunun 3. ve 8. maddeleri 23 Kasım 2007 tarihinde, diğer maddeleri yayım tarihinde yürürlüğe girmiştir.

[290] 5651 sayılı Kanun öncesi erişim engellemeleri için bkz. yuk. §6 II.

[291] *Akdeniz/Altıparmak*, a.g.e., s. 16.

[292] RG 30.11.2007/26716.

Erişim Sağlayıcılara ve Yer Sağlayıcılara Faaliyet Belgesi Verilmesine İlişkin Usul ve Esaslar Hakkında Yönetmelik ("Faaliyet Yönetmeliği")[293] ve İnternet toplu kullanım sağlayıcılarıyla ilgili olarak 01.11.2007 tarihli İnternet Toplu Kullanım Sağlayıcıları Hakkında Yönetmelik ("Toplu Kullanım Yönetmeliği")[294] yayımlanmıştır.

A. Engelleme kararlarının hukuki niteliği

5651 sayılı Kanun gerekçesinde yeni suç kategorileri oluşturulmadığı veya suçlar işlendikten sonra devreye girecek cezai ve idari yaptırımlar getirilmediği belirtilmiştir. Kanun, 5237 sayılı TCK'da yer alan bazı suçların İnternet ortamında işlenmesi durumunda söz konusu suçların etkilerini sürdürmesinin idari ve yargısal koruma tedbiri olmak üzere iki yöntemle önlenmesini amacıyla yürürlüğe koyulmuştur.

Erişim engelleme kararları bir ceza değil tedbir niteliğindedir. Erişim engelleme kararları, kararın adli makamlar tarafından verilmesi durumunda yargısal, idari makamlar tarafından verilmesi durumunda ise karar idari tedbir niteliğini alacaktır[295]. Koruma tedbirleri, yargılama süresince eski durumu yaşatmak ve verilecek kararın yerine getirilebilirliğini sağlamak için kullanılan geçici nitelikte araçlardır[296].

B. Engelleme sebepleri

5651 sayılı Kanunun 8. maddesinde belirtilen engelleme sebepleri sınırlı sayı prensibine göre belirlenmiştir. 5651 sayılı Kanun'un erişim engelleme hususunda özel kanun olması sebebiyle artık genel kanunlardaki koruma hükümlerine dayanılarak erişim engelleme yoluna gidilmesi mümkün değildir.

---

[293] RG 24.10.2007/26803; Bu yönetmelik 01.03.2008 tarihli Telekomünikasyon Kurumu Tarafından Erişim Sağlayıcılara ve Yer Sağlayıcılara Faaliyet Belgesi Verilmesine İlişkin Usul ve Esaslar Hakkında Yönetmelikte Değişiklik Yapılmasına Dair Yönetmelikle kısmi değişikliğe uğramıştır. Bkz. RG 01.03.2008/26803.

[294] RG 01.11.2007/26687.

[295] Bu tedbirlerin koruma tedbiri niteliğinde olmaları sebebiyle 5271 sayılı CMK altında düzenlenmesi gerektiği düşünülmektedir. Bkz. *Dülger*, a.g.e., s. 1482.

[296] *Kunter/Yenisey/Nuhoğlu*, a.g.e., s. 756.

5651 sayılı Kanunun 8. maddesine göre 5237 sayılı TCK'da yer alan intihara yönlendirme (m. 84), çocukların cinsel istismarı (m. 103, f. 1), uyuşturucu ve uyarıcı madde kullanılmasını kolaylaştırma (m. 190), sağlık için tehlikeli madde temini (m. 194), müstehcenlik (m. 226), fuhuş (m. 227), kumar oynanması için yer ve imkan sağlama (m. 228) suçları ile 5816 sayılı Atatürk Aleyhine İşlenen Suçlar Hakkında Kanun'da yer alan suçların İnternet ortamında yapılan yayınlarla oluştuğu yönünde yeterli şüphe bulunması durumunda erişim engelleme kararı verilebilecektir.

5651 sayılı Kanun dışında 7258 sayılı Futbol ve Diğer Spor Müsabakalarında Bahis ve Şans Oyunları Düzenlenmesi Hakkında Kanun'un[297] 5. maddesinde yer alan suçlar ile belirli koşullar altında 5846 sayılı Fikir ve Sanat Eseleri Kanunu ("5846 sayılı FSEK")[298] Ek 4. maddesinde yer alan sebeplerle erişim engelleme yoluna gidilebilecektir.

1. İntihara yönlendirme

5237 sayılı TCK'nın 84. maddesinde yer alan intihara yönlendirme suçunun İnternet ortamında yapılan yayınlarla oluştuğu yönünde şüphe bulunması durumunda erişim engellenmesi kararı verilebilecektir[299].

İntihar bireyin duygusal, ruhsal ya da sosyal sebeplerin etkisiyle kendi hayatına son vermesi olarak tanımlanmaktadır[300]. Türk Hukukunda intihar veya intihara teşebbüs fiilleri cezalandırılabilir olarak kabul edilmemektedir. İntiharın veya intihara teşebbüsün cezalandırılmaması suç politikası gereğidir. Nihayetinde intihara ölüm ile sonuçlanmışsa ölmüş bir kişiyi cezalandırmak mümkün değildir; ölüm gerçekleşmemiş ise de intihara kalkışanın bu eylemini tekrarlanmasından korkulmaktadır[301].

---

[297] Kanun No: 7258, Kabul T.: 29.04.1959, RG 09.05.1959/10201.

[298] Kanun No: 5846, Kabul T.: 05.12.1951, RG 31.12.1951/7981.

[299] 5651 sayılı Kanun, m. 8 f. 1(a).

[300] Türkiye'de intihar oranlarının düşük olduğu bildirilmektedir. 1997'de bu oran yüz binde 3.18'dir. Son yıllarda artış olduğu gözlenmektedir ancak bu değerlerin gerçeği ne kadar yansıttığı ise bilinmemektedir. Bkz. İntihar ve Şiddet, http://www.psikolog.org.tr/articles_detail.asp?cat=4&id=9; Dünya genelindeki intihar istatistikleri için bkz. Suicide rates per 100,000 by country, year and sex, http://www.who.int/mental_health/prevention/suicide_rates/en/index.html.

[301] Sahir Erman/Çetin Özek, Ceza Hukuku Özel Bölüm Kişilere Karşı İşlenen Suçlar (TCK

Kendisi suç olmayan bir fiile iştirak da suç olmadığı için intihara yönlendirme fiilleriyle bir kişinin kendisini öldürmesi fiiline asli (azmettirme) veya fer'i iştirak (yardım etme) şeklinde katılmak suç olmayacaktır[302]. Ancak intihara yönlendirme fiillerinin başka bir insanın hayatına saldırı niteliği taşıdığı kabul edilmektedir[303]. Bu tür fiillerin cezasız kalmaması amacıyla, intihara yönlendirme şeklinde müstakil bir suç oluşturulmuştur.

5237 sayılı TCK'nın intihara yönlendirme başlıklı 84. maddesi, başkasını intihara azmettiren, teşvik eden, başkasının intihar kararını kuvvetlendiren veya herhangi bir şekilde yardım eden kişilerin iki yıldan beş yıla kadar hapis cezası ile cezalandırılacağını öngörmüştür. İntihar sonucunda ölüm gerçekleşmese de fail cezalandırılmakta, ölüm sadece neticeyi ağırlaştırmaktadır[304].

Öte yandan intihara alenen tahrik ayrı bir suç olarak kabul edilmiştir[305]. Kanun gerekçesine göre aleniyet, gerçekleştiği koşullar itibariyle belirli olmayan ve birden fazla kişiler tarafından fiillerin algılanabilir olması şeklinde tanımlanmıştır[306]. Diğer bir deyişle suçun oluşması için belirli

448-490), İstanbul 1994 ("Erman/Özek"), s. 76.

[302] Faruk Erem, Türk Ceza Kanunu şerhi: Özel Hükümler, Cilt III, Ankara 1993 ("Erem"), s. 2067.

[303] Necati Meran, Yeni Türk Ceza Kanununda Kişilere Karşı Suçlar, Ankara 2005 ("*Meran*"), s. 73.

[304] 5237 sayılı TCK, m. 84 f. 2; 765 sayılı TCK'nın 454. maddesi failin cezalandırılması için intihara ikna ve yardımı yeterli görmeyip suçun oluşması için intihara kalkışan kişinin ölmesini şart olarak görmekteydi. Daha fazla bilgi için bkz. Ali Parlar/Güleç Demirel, Açıklamalı-İçtihatlı Kişilerin Hayatına ve Beden Bütünlüğüne Karşı Suçlar, Ankara 2002 ("*Parlar/Demirel*"), s. 469.

[305] 5237 sayılı TCK, m. 84 f. 3; 765 sayılı TCK döneminde bu hüküm yer almadığı için yapılan hareketlerin belirli bir mağdura yönelik olması şartı aranmaktaydı. Dolayısıyla, okuyanlarda veya seyredenlerde intihar arzusunu uyandıracak yayınların yapılması veya filmlerin gösterilmesi bunların etkisinde kalan kimselerin intihar etmeleri halinde dahi intihara ikna suçunu oluşturmadığı kabul edilmekteydi. Bkz. *Erman/Özek*, a.g.e., s. 77; Örneğin, bir gazetecinin yazılarının tesiri altında kalarak intihar edilmesi durumunda gazetecilerin intiharı azmettirme ve yardım kastı olmadığı için sorumlu olmadığı kabul edilmekteydi. Bkz. *Erem*, a.g.e., s. 2068.

[306] Remzi Özmen, Notlu-Gerekçeli-Karşılaştırmalı 5237 sayılı Türk Ceza Kanunu, Ankara 2004 ("*Özmen,* TCK gerekçesi"), s. 272.

bir kişilerin muhatap alınması gerekmemektedir. Bu hükümle paralel bir şekilde 5187 sayılı Basın Kanunu 20. maddesi intihar olayları hakkında haber vermenin sınırlarını aşan ve okuyucuyu bu tür fiillere özendirebilecek nitelikte yazı ve resim yayınlanmasını yasaklamıştır[307].

İntihara azmettirme, teşvik ve yardım etmenin amacı mağdurun hayatına son vermeye ikna etmektir[308]. Doktrinde bu fiiller bir kimseyi hayatına son vermedikçe rahata kavuşamayacağına inandırma ve bu kişide intihar kararını pekiştirme, mevcut olan intihar niyetini güçlendirme veya intihar niyeti olmayan bir kişiye bu kararı verdirme şeklinde tanımlanmaktadır[309]. Bu fiillerin her türlü telkin ve vasıtalarla işlenebileceği kabul edilmektedir. Dolayısıyla, İnternetin de hem bir iletişim hem de bilgiye erişim aracı olarak intihara yönlendirme suçunun işlenmesi için kullanılması mümkündür.

İnternette yer alan intihara ilişkin içerik bireylerin davranışlarını olumsuz etkilemekte ve intihara sürüklemektedir. Bu tür içerik yoğun olarak gençleri etkilemektedir[310]. Birçok devlet intiharın önlenmesi ve özellikle gençliğin korunması için çeşitli düzenlemeler yapmaktadır[311]. İntihara yönlendirme suçuyla ilgili İnternet içeriğinin engellenmesini öngören 5651 sayılı Kanunun 8. maddesi bu doğrultuda hazırlanmıştır.

---

[307] Benzer hüküm mülga 5680 sayılı Basın Kanununun 32. maddesinde yer almaktaydı. Öte yandan, 84. maddesinin 3. fıkrasında yer alan "Bu fiilin basın ve yayın yolu ile işlenmesi halinde, kişi dört yıldan on yıla kadar hapis cezası ile cezalandırılır." şeklindeki ifade 5377 sayılı Türk Ceza Kanununda Değişiklik Yapılmasına Dair Kanunun 10. m. hükmüyle kaldırılmıştır. Bkz. Kanun No: 5377, Kabul T.: 29.06.2005, RG 08.07.2005/25869.

[308] *Erman/Özek*, a.g.e., s. 77.

[309] *Parlar/Demirel*, a.g.e., s. 469.

[310] Keith Hawton/Kathryn Williams, Influences of the media on suicide, BMJ Vol. 325, 11 December 2002 ("*BMJ (2002/325)*"), s. 1374.

[311] Örneğin, İngiltere intiharların önlenmesi için eylem planı hazırlayarak başta medya olmak üzere tüm kesimlerin intihar konusunda duyarlılığını sağlamayı hedeflemiştir. Benzer bir şekilde Viyana'da intiharla ilgili yayınların sınırlanmasına ilişkin çalışma başarıya ulaşmış ve istatistiklere göre intihar vakıalarında azalma gözlemlenmiştir. Bkz. *BMJ (2002/325)*, a.g.e., s. 1375; Öte yandan, devletlerin intihara yönlendirdiği gerekçesiyle en çok Satanist içerikli web sitelerini engellemeleri dikkat çekmektedir. Bkz. Lucy Biddle/Jenny Danovan/Keith Hawton/Navneet Kapur/David Gunnell, Suicide and the Internet, BMJ Vol. 336, 12 April 2008 ("*BMJ (2008/336)*"), s. 802.

Bu hüküm ayrıca gençliğin korunması için gereken tedbirleri alması için devlete sorumluluk yükleyen Anayasanın 58. maddesine dayanmaktadır.

İntihara meyleden insanlar sorunlarını başkalarıyla paylaşmaktan çekinmektedir. Bu kişiler, kimliklerini rahatlıkça gizleyebildikleri İnterneti ya bu düşünceyi gerçekleştirmek için ya da bu düşünceden kurtulmak için kullanabilmektedir.

İntihar yöntemlerini anlatan web sitelerinin sayısı hızla artmaktadır[312]. Bu web siteleri intihar yöntemlerini ayrıntılı olarak açıklamakta ve hatta kullanılacak ilacın dozajını bile bildirmektedir. Yapılan bir araştırmada arama motorları intiharla ilgili psikolojik yardım bilgilerinden çok intiharı teşvik eden bilgiler içerdiği tespit edilmiştir[313]. Bu tür içerikleri barındıran web sitelerinin ilgilileri, çoğu zaman içeriğin bilimsel amaçlarla sunulduğunu, bu sebeple içeriğe müdahale edilmemesi gerektiğini savunmaktadırlar[314].

İnternette belirli odakların insanların intihara yönlendirmek için özel çaba gösterdikleri iddia edilmektedir[315]. Özellikle sohbet odaları ve forumlar gibi kişiler ile eşzamanlı iletişimin mümkün olduğu ve kimliğin kolayca izlenebildiği ortamlarda bu tür girişimler yoğunluk kazanmaktadır. Sohbet odalarında bireyler intihar için birebir teşvik edilebilmekte, intihar etmiş kişiler web sitelerinde kahramanlar olarak sunulabilmekte ve intihar tüm sıkıntılar için bir çözümmüş gibi pazarlanmaktadır. Kişileri bu şekilde intihara yönlendirmenin psikolojik bir rahatsızlık olduğu kabul edilmektedir[316].

İntihara yönlendirme İnternet üzerinden her zaman açıkça gerçekleştirilmemekte, dolaylı yöntemler kullanılmakta ve erişim engelleme

---

[312] Sundararajan Rajogopal, Sucide pacts and the Internet, BMJ Vol. 336, 4 December 2004 (*"BMJ (2004/329)"*), s. 1299; Dünyanın en çok ziyaret edilen web sitelerinden İnternet ansiklopedisi Wikipedia bile bu tür içerikler ayrıntılı olarak yayınlanabilmektedir, bkz. İntihar yöntemleri, http://tr.wikipedia.org/wiki/İntihar_yöntemleri.

[313] *BMJ (2008/336)*, a.g.e., s. 800.

[314] *BMJ (2008/336)*, a.g.e., s. 802.

[315] Suicide Promotion (Internet), http://www.iwf.org.uk/government/page.101.351.htm.

[316] Suicide Promotion (Internet), http://www.iwf.org.uk/government/page.101.351.htm.

yöntemleri çok kolay aşılabilmektedir[317]. Bazen bu mesaj bir edebi metnin bazen de bir videonun içine eklenmekte veya içerik aldatması tekniği kullanılabilmektedir[318]. Bu sebeple, içeriğin intihara azmettirildiğinin, teşvik edildiğinin veya intihar kararını kuvvetlendirdiğinin tespit edilmesi bireysel engelleme yöntemiyle ancak bir insan tarafından değerlendirilmesi sonucunda ortaya çıkabilmektedir. Otomatik içerik engelleme sistemleri bu konuda çaresiz kalmaktadır. Ayrıca, video paylaşım siteleri hukuka aykırı veya zararlı içeriği engellemek için çeşitli yöntemler kullansa da video paylaşım sitelerine milyonlarca videonun eşzamanlı olarak yüklenmesi tüm videoların site yöneticileri tarafından takibinin neredeyse imkânsız kılmaktadır.

Öte yandan, İnternet intihar eğilimi içinde olanların bu düşüncelerinden kurtulmak için de bir araç olarak kullanılabilmektedir[319]. İnternette çeşitli sivil toplum örgütleri kişileri intihar saplantılarından kurtarmak için ücretsiz danışmanlık hizmeti vermektedir. Daha önce açıklandığı üzere, erişim engelleme sistemlerinin masum web sitelerini engelleme şeklinde aşırı engelleme riski bulunmaktadır. İntiharla ilgili içeriğin uygun teknik kullanılmadan engellenmesi, sayısı zaten sınırlı sayıda olan gönüllü intiharı önleme çalışmalarına da engel olacaktır. Bu sebeple, intihara yönlendirmeyle ilgili içeriğin tespitinin zor olması sebebiyle otomatik engelleme sistemleri kullanılmayıp, bireysel olarak her bir web sitesinin münferit olarak engellendiği takdirde 5651 sayılı Kanunla öngörülen engelleme sebebi ailenin ve gençliğin korunması amacına hizmet edecektir.

[317] İnternet bireylerin intihar davranışlarını değiştirmektedir. Amerika'da 19 yaşında bir genç onu İnternet üzerinden 1500 kişi web kamerası üzerinden canlı olarak izlerken intihar etmiştir. Bkz. Teenager commits suicide live on internet as 1,500 watch, http://www.telegraph.co.uk/news/worldnews/northamerica/usa/3497263/Teenager-commits-suicide-live-on-internet-as-1500-watch.html; Öte yandan İnternet üzerinden gerçekleştirilen İntihar akitleri yeni bir olgu olarak ortaya çıkmaktadır. İntihar akdi iki veya daha fazla kişinin belirli zaman ve yerde intihar etmek üzere anlaşmaları olarak tanımlanmaktadır. Bu konudaki en çarpıcı örnek 2004 yılında Japonya'da gerçekleşmiştir. İnternette tanışan yedisi bir grupta, ikisi başka bir grupta 9 kişi aynı anda intihar etmiştir. Yapılan araştırmalarda intihar edenlerin İnternette tanıştıkları ve bu fikri intihar yöntemleri hakkında bilgi veren web sitelerinden edindikleri tespit edilmiştir. Bkz. *BMJ (2004/329)*, a.g.e., s. 1298.

[318] İçerik aldatması için bkz. yuk. §4 I D.

[319] *BMJ (2008/336)*, a.g.e., s. 802.

Aksi takdirde, aşırı engelleme riski ile masum web siteleri engellenecektir. Ayrıca web içeriğinin, forum sohbet odalarındaki yazışmaların intiharla ilgili içeriğin tespit edilmesi için takip edilmesi iletişimin ve özel hayatın gizliliğini ihlal eden bir nitelik taşıyacaktır[320].

TİB İhbar İstatistiklerine göre intihara yönlendirme suçuyla ilgili 542 ihbar yapılmış ve şu ana kadar 1'i re'sen, 3'ü de yargı kararıyla olmak üzere toplam 4 web sitesinin erişimi engellenmiştir[321].

2. Çocukların cinsel istismarı

5237 sayılı TCK, çocukların cinsel dokunulmazlıklarına karşı işlenen fiilleri 103. madde altında ayrı bir suç olarak düzenlemiştir. Ailenin ve gençliğin korunması temel amacıyla hazırlanan 5651 sayılı Kanun, bu suça ilişkin içeriklerin İnternet ortamındaki yayınlarla yayılmasını önlemek amacıyla bu suçu bir erişim engelleme sebebi olarak kabul etmiştir[322].

5237 sayılı TCK'nın 6. maddesinde çocuk henüz on sekiz yaşını doldurmamış kişi olarak tanımlanmıştır. Kanun erişkin kişilere karşı işlenen cinsel dokunulmazlık ihlallerini cinsel saldırı olarak, çocuklara karşı işlenen ihlalleri ise çocukların zayıflıklarını göz önüne alarak cinsel istismar olarak nitelendirmiştir. 5651 sayılı Kanun, sadece 5237 sayılı TCK'nın çocukların cinsel istismarı başlıklı 103. maddesinin birinci fıkrasında yer alan suçu bir erişim engelleme sebebi olarak kabul etmiştir.

103. maddenin birinci fıkrası çocuğu cinsel yönden istismar eden kişinin üç yıldan sekiz yıla kadar hapis cezası ile cezalandırılacağını öngörmüştür. Bu suçun çocukların vücudu üzerinde her türlü cinsel davranışla işlenmesi mümkündür. Suçun oluşması için failin veya mağdurun cinsiyetinin önemi bulunmamaktadır[323]. Fail herhangi bir kişi, mağdur çocuk ve suçun konusu ise istismar suçu üzerinde işlenen çocuğun bedenidir.

---

[320] *BMJ (2008/336)*, a.g.e., s. 802.

[321] 11.05.2009 Tarihli İhbar İstatistikleri, http://www.guvenliweb.org.tr/content/11052009-tarihli-ihbar-istatistikleri-yayınlanmıştır ("*İhbar İstatistikleri*").

[322] 5651 sayılı Kanun, m. 8 f. 1(a).

[323] *Meran*, a.g.e., s. 264.

Çocukların cinsel istismarı suçunun iki farklı görünümü bulunmaktadır. İlk durum birinci fıkrada tanımlanan cinsel nitelik taşıyan herhangi bir davranışın 15 yaşını tamamlamamış veya tamamlamış olmakla birlikte bu davranışların hukuki anlam ve sonuçlarını algılama yeteneği gelişmemiş olan çocuklara karşı işlenmesi halidir. Bu nitelikteki çocuklara karşı yapılan eylemlere mağdur çocuğun rıza göstermesi suçun oluşmasını önleyecek hukuki bir etkisi bulunmamaktadır[324]. Ayrıca, fiillerin cinsel ilişki aşamasına varmamış olması suçun oluşmasını önlememektedir.

Çocukların cinsel istismarı suçunun oluşacağı ikinci durum ise cinsel nitelik taşıyan davranışların 15 yaşının tamamlamış ancak cebir, tehdit, hile veya iradeyi etkileyen başkaca bir sebeple fiilin hukuki anlam ve sonuçlarını algılama yeteneği olmayan çocuklar üzerinde işlenmesi halidir[325]. Diğer bir deyişle, suçun oluşabilmesi için 15 yaşını tamamlamış mağdur çocuğun iradesinin zayıflatılarak cinsel davranışların gerçekleştirilmesi gerekmektedir.

Çocukların cinsel istismar suçu mağdur çocuğun vücudu üzerinde farklı fiiller ile işlenmesi mümkündür. Suçun oluşması için her iki fıkrada belirtilen cinsel davranışın objektif olarak şehevi nitelikte bulunmasının yeterli olup, failin şehevi arzuların fiilen tatmin edilmiş olması gerekmemektedir[326].

Çocukların cinsel istismarının önlenmesi küresel ölçekte güncel bir sorundur. Devletlerin iç hukuk farklılıklarından dolayı çocuklara yönelik yaklaşımlarının değişmesi sebebiyle, çocukların etkin bir şekilde korunması amacıyla çeşitli uluslararası sözleşmeler akdedilmiştir. İç hukuk farklılıklarının ortaya çıkardığı öncelikli sorun çocuğun tanımına ilişkindir[327]. Her devlet farklı yaşların altındaki bireyleri çocuk olarak kabul

---

[324] *Meran*, a.g.e., s. 264.

[325] Çocukların cinsel istismar suçunun oluşması için her durumda, mağdurun 18 yaşından küçük olması gerekmektedir. Aksi durumda çocukluk niteliği yitirileceği için 5237 sayılı TCK'nın 102. maddesinde yer alan cinsel saldırı suçu gündeme gelecektir.

[326] *Meran*, a.g.e., s. 267.

[327] George Ivezaj, Child Pornography On the Internet: An Examination of the International Communities Proposed Solutions For a Global Problem, Michigan State University - DCL Journal of International Law, Fall, 1999 ("*Ivezaj*"), s. 2.

etmektedir. Örneğin, Çin 14 yaşının arasındaki bireyleri, Singapur ise 16 yaşının altındaki bireyleri çocuk olarak kabul etmektedir[328].

Çocukların korunmasına ilişkin temel uluslararası metin Birleşmiş Milletler tarafından kabul edilen Çocuk Haklarına Dair Sözleşme'dir[329]. Türkiye bu Sözleşmeyi 14.09.1990 tarihinde imzalamış ve Sözleşme Türkiye için 27.01.1995 tarihinde yürürlüğe girmiştir[330].

Çocuk Haklarına Dair Sözleşme, 18 yaşının altındaki tüm bireyleri sözleşmenin uygulaması bakımından çocuk olarak kabul etmektedir. Sözleşme, çocuklara yaşam, kendi ad ve kimliğine sahip olma, kendi ailesi tarafından yetiştirilme gibi temel haklar ile ve her türlü istismardan ve sömüründe korunma gibi hakları tanımaktadır. Bu doğrultuda Sözleşme devletleri çocukların menfaatine en uygun yasal, idari, sosyal ve eğitimsel tedbirleri almakla yükümlü kılmıştır.

Sözleşmenin çocukların cinsel istismarı ve sömürülmesi alanlarındaki uygulamasını daha etkin bir hale getirmek amacıyla Birleşmiş Milletler 25.05.2000 tarihinde Çocuk Haklarına Dair Sözleşmeye Ek Çocuk Satışı, Çocuk Fahişeliği ve Çocuk Pornografisi İle İlgili İhtiyari Protokol'ü ("Protokol") kabul etmiştir[331]. Türkiye bu Protokolü 08.09.2000 tarihinde imzalamış ve Protokol Türkiye için 28.06.2002 tarihinde yürürlüğe girmiştir[332].

Protokolün temel amacı çocuk satışı, çocuk fahişeliği ve çocuk pornografisini önlemektir. Protokol her akit devletin bu fiilleri iç hukuk-

---

328 Devletlerin çocukların cinsel istismarına ilişkin iç hukuk düzenlemeleri ve ilgili çocukluk yaşı rakamları için bkz. Sexual Offences Laws - Countries, http://www.interpol.int/Public/Children/SexualAbuse/NationalLaws/Default.asp.

329 Bkz. dn. 145.

330 RG 27.01.1995/22184.

331 Protokol, Birleşmiş Milletlerin 25 Mayıs 2000 tarih 54/263 sayılı Genel Kurul kararıyla kabul edilmiş ve 18 Ocak 2002 tarihinde yürürlüğe girmiştir. Protokolün tam metni için bkz. Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography, http://www.unhchr.ch/html/menu2/6/crc/treaties/opsc.htm.

332 RG 28.06.2002/24799.

larında suç olarak kabul etmekle yükümlü kılmıştır[333]. Protokol ayrıca, suçların tanımı, devletlerin bu suçlarla mücadeleye ilişkin uluslararası işbirliği, devletlerin yargılama yetkisi, suçluların iadesi ve ceza yargılamasında gözetilmesi gereken ilkeler gibi hususları düzenlemektedir.

5651 sayılı Kanunun uygulaması bakımından önem taşıyan çocuk pornografisi Protokolde "çocuğun gerçekte veya taklit suretiyle bariz cinsel faaliyetlerde bulunur şekilde herhangi bir yolla teşhir edilmesi veya çocuğun cinsel uzuvlarının, ağırlıklı olarak cinsel amaç güden bir şekilde gösterilmesi" şeklinde tanımlanmıştır[334]. Yargıtay, çocuk pornografisine ilişkin vermiş olduğu kararlarda doğrudan Çocuk Haklarına Dair Sözleşme ve Protokole atıfta bulunarak uyuşmazlığı çözmektedir[335].

Çocuk pornografisine ilişkin önemli bir diğer uluslararası nitelikteki sözleşme Avrupa Konseyi'nin Siber Suçlar Sözleşmesidir[336]. Siber Suçlar Sözleşmesi çocuk pornografisini bir içerik suçu olarak kabul etmiştir. Sözleşmenin 9. maddesine göre çocuk, Çocuk Haklarına Dair Sözleşme'yle paralel bir şekilde 18 yaşından küçük kişi olarak tanımlanmıştır. Sözleşme, bilgisayar sistemleri üzerinden çocuk pornografisinin dağıtılmasını, üretilmesini, sunulmasını, erişim sağlanmasını, yayılmasını ve her türlü çocuk pornografisi içeriğinin bilgisayar sisteminde ya da bilgisayar verilerinin saklandığı herhangi bir cihazda bulundurulmasını yasaklamaktadır[337]. Sözleşme, çocuk pornografisini, cinsel anlamda müstehcen bir eyleme reşit olmayan veya reşit görünmeyen bir kişinin katılımını gösteren veya reşit olmayan bir kişinin böyle bir eyleme katıldığını gösteren gerçeğe benzer her türlü tasviri içeren pornografik içerik olarak tanımlanmıştır[338]. Bu şekilde hem doğrudan çocukların dâhil olduğu cinsel aktiviteler yasaklanmakta hem de herhangi bir pornografik içerikte reşit görünmeyen kişilerin veya çocukların sanal tasvirlerinin kullanılması yasaklanması suretiyle çocukların istismarının özendirilmesi önlenmektedir.

[333] Protokol, m. 3.

[334] Protokol, m. 2 f. 1(c).

[335] Bkz. Yargıtay 5. CD, K.T.: 01.10.2007, E: 2007/9856, K: 2007/6957 (Kazancı İçtihat Bankası).

[336] Bkz. dn. 282.

[337] Siber Suçlar Sözleşmesi, m. 9 f. 1.

[338] Siber Suçlar Sözleşmesi, m. 9 f. 2.

Çocukların cinsel istismarı pedofili olarak adlandırılan psikolojik bir rahatsızlıktır. Her yıl dünya genelinde iki milyondan fazla çocuğun cinsel istismara maruz kaldığı tahmin edilmektedir[339]. Çocuk pornografisinin istismar edilen çocuk üzerinde tecavüz ve şiddet dışında depresyon, travma sonrası stres bozukluğu ve davranış bozuklukları gibi psikolojik etkileri bulunmaktadır[340]. Çocuk pornografisinin diğer bir sonucu ise çocuk satışını ve bu amaçla çocuk kaçırmalarını artırmasıdır. Başta Uluslararası Polis Teşkilatı ("Interpol")[341] olmak üzere çeşitli örgütler çocuk ticareti ve pornografisinin önlenmesi amacıyla uluslararası düzeyde faaliyet göstermektedir[342].

Çocuk pornografisi çocuğun cinsel amaçlı istismarı ve bunun temsil edilmesi şeklinde iki farklı suçu ortaya çıkarmaktadır. 5237 sayılı TCK'nın 103. maddesinde yer alan hüküm çocuğun cinsel amaçlı istismarı fiilleriyle mücadeleye, 5651 sayılı Kanun'da bu hükmün erişim engelleme sebebi olarak sayılması ise temsil sorunuyla mücadeleye hizmet etmektedir.

Çocuk pornografisi milyon dolarlık bir uluslararası bir endüstridir. Yapılan bir araştırmaya göre, çocuk pornografisinin en büyük üretim merkezi Almanya, dağıtım merkezi Hollanda ve İngiltere ve en büyük pazarı ise ABD'dir[343]. Çocuk pornografisi içeriği İnternette şifreli kanallar üzerinden aktarılmaktadır. Ayrıca, bu tür içerik virüsler aracılığıyla yayılmakta ve masum kişiler bu suçta araç olarak kullanılabilmekte, gerçek

---

339 Commercial Sexual Exploitation of Children and Child Trafficking, http://www.yapi.org/csec/.

340 İnternet Üzerinde Çocuk Pornografisi 7, http://turk.internet.com/haber/yazigoster.php3?yaziid=13299.

341 International Criminal Police Organization, http://www.interpol.int; Türkiye Interpol'e 08.01.1930 t. ve 8761 sayılı kararname ile üye olmuştur. Bkz. Türk İnterpolü, http://www.egm.gov.tr/interpol/turkce/turkint.htm.

342 Interpol'un bu alandaki faaliyetleri için bkz. Crimes against children, http://www.interpol.int/Public/Children/Default.asp; Interpol dışında çocukların cinsel istismarının önlenmesi amacıyla Amerika, Avustralya, İngiltere, İtalya, Kanada Virtual Global Taskforce isimli uluslararası örgütü kurmuşlardır. Bu örgüt özellikle İnternet ortamında yer alan çocuk pornografisi içeriğiyle mücadele etmektedir. Bkz. Virtual Global Taskforce, http://www.virtualglobaltaskforce.com.

343 *Ivezaj*, a.g.e., s. 2.

failler kimliklerini gizleyebilmektedir. Bu durum İnternet üzerinden bu tür içerikle mücadeleyi zorlaştırmaktadır.

Faillerin tespiti dışında uygulamada pornografi içerikli bir imajdaki kişilerin çocuk olup olmadığının tespitinde sorunlar ortaya çıkmaktadır. Nihayetinde, bir kişinin yetişkin mi yoksa çocuk mu gösterdiği göreceli olduğu için kolluk kuvvetleri bazı durumlarda işlem yapmakta zorlanabilmektedir[344].

Çocuk pornografisine ilişkin bir diğer sorun ise temsili görüntülerde ortaya çıkmaktadır. Bilişim teknolojileri kullanılarak gerçek ile ayırt edilmeyecek kadar yüksek kalitede görüntüler oluşturulması mümkündür[345]. Bu yöntemler çocuk pornografisinde de kullanılmaktadır. Bu tür yöntemlerle dahi çocuk pornografisinin dağıtımı çocuklara yönelik cinsel istek oluşturması potansiyeli sebebiyle yasaklanması talep edilmektedir[346]. Buna rağmen, bu tür içeriğin engellenmesi yönünde uluslararası düzeyde yeknesak bir uygulama bulunmamaktadır. Özellikle, bu tür içeriğin engellenmesinin ifade hürriyetini orantısız sınırlayacağı iddia edilmektedir[347]. Ayrıca, sanal çocuk pornografisinin kişileri çocukların cinsel istismarı suçuna itmesi ile arasında doğrudan illiyet bağı bulunmadığı ileri sürülmektedir[348]. Buna rağmen, Çocuk Hakları Sözleşmesi ve Siber Suçlar Sözleşmesinde yer alan çocuk pornografisi tanımları ve bu sözleşmelerle korunan hukuki değerler göz önüne alındığında sanal çocuk pornografisinin engellemesi ifade hürriyetine aykırılık teşkil etmemektedir.

TİB İhbar İstatistiklerine göre çocukların cinsel istismarı suçuyla ilgili 4.845 ihbar yapılmış ve 1053'ü re'sen, 54'ü de yargı kararıyla olmak

[344] İnternet Üzerinde Çocuk Pornografisi 5, http://turk.internet.com/haber/yazigoster.php3?yaziid=13297.

[345] Bilgisayar ile üretilmiş kişilerin kullanılarak bilgisayar ortamında pornografi olayını canlandırma sözde ("pseudo") pornografi; gerçek görüntüleri doğrudan sanal görüntülere çevirmeye ise kesintisiz dönüşüm ("morphing") denilmektedir. Bkz. İnternet Üzerinde Çocuk Pornografisi 9, http://turk.internet.com/haber/yazigoster.php3?yaziid=13357.

[346] İnternet Üzerinde Çocuk Pornografisi 9, http://turk.internet.com/haber/yazigoster.php3?yaziid=13357.

[347] Dannielle Cisneros, "Virtual Child" Pornography on the Net: A "Virtual" Victim?, Duke Law & Technology Review, Rev. 19, 23 September 2002 ("*Cisneros*"), s. 1.

[348] *Cisneros*, a.g.e., s. 2.

üzere toplam 1.107 web sitesinin erişimi engellenmiştir[349]. Bu istatistikler göz önüne alındığında 5651 sayılı Kanun en çok çocukların cinsel istismarı suçu için uygulama alanı bulmuştur.

3. Uyuşturucu veya uyarıcı madde kullanılmasını kolaylaştırma

5237 sayılı TCK'nın 190. maddesinde yer alan uyuşturucu veya uyarıcı madde kullanılmasını kolaylaştırma suçunun İnternet ortamında yapılan yayınlarla oluştuğu yönünde şüphe bulunması durumunda erişim engellenmesi kararı verilebilecektir[350].

Uyuşturucu maddeler, "belirli dozlarda alındığı zaman, kişinin sinir sitemi üzerinde etkide bulunan, akli, fiziki ve psikolojik dengesini bozan, birey ve toplum için ekonomik ve sosyal problemler ortaya çıkaran, alışkanlık ve bağımlılık yapan, kanunların kullanılmasını, bulundurulmasını ve satışını yasakladığı maddeler"[351] olarak tanımlanmaktadır. Bu tür maddeler narkotik ve psikotrop maddeler olarak da anılmaktadır. Bazı uyuşturucu maddelerinin kullanımına asla izin verilmezken, bazılarının belirli şartlar altında ve ancak tıbbi gereklilikler durumunda kullanımına izin verilmektedir[352].

Uyuşturucu ve uyarıcı maddelerle mücadele uluslararası düzeyde gerçekleşmektedir. Bu doğrultuda devletlerarası işbirliğini geliştirmek için çeşitli uluslararası sözleşmeler imzalanmıştır. Türkiye 8 Ağustos 1975 tarihinde yürürlüğe giren 1961 tarihli Uyuşturucu Maddelere Dair Birleşmiş Milletler Tek Sözleşmesi ve 1972 Protokolü'ne 20.06.2001

---

[349] Bkz. *İhbar İstatistikleri*, dn. 321.

[350] 5651 sayılı Kanun, m. 8 f. 1(a).

[351] Türkiye'de Uyuşturucu Suçu, http://www.cte.adalet.gov.tr/kaynaklar/yayinlar/uyusturucu.pdf, s. 1.

[352] Esrar, eroin ve kokain gibi maddeler koşulsuz yasadışı maddelerdir. Ancak amfetaminler, benzodiazepinler, sedatif-hipnotik gibi maddeler belirli yasal sınırlamalara göre kullanılmasına izin verilen maddelerdir. Uyuşturucu maddelerin tasnifi ve çeşitleri için bkz. Şahin Kurt, Uygulamada Uyuşturucu Madde Suçları ve İlgili Mevzuat, İstanbul 1992 (*"Kurt"*), s. 14 vd.

tarihinde taraf olmuştur[353]. Ayrıca, 1971 Psikotrop Maddeler Sözleşmesi Türkiye tarafından 22.02.1971 tarihinde imzalanmış, 07.03.1981 tarihli Resmi Gazetede yayımlanarak yürürlüğe girmiştir[354]. Son olarak, 1988 Uyuşturucu ve Psikotrop Maddelerin Kaçakçılığına Karşı Sözleşmesi, Türkiye tarafından 20.12.1988 tarihinde imzalanmış ve 11.02.1996 tarihli Resmi Gazetede yayınlanarak Türkiye açısından bu tarihte yürürlüğe girmiştir[355].

Uyuşturucuyla mücadele devletlerarası işbirliğiyle Interpol ve Birleşmiş Milletler'e bağlı Uluslararası Narkotik Kontrol Kurulu ("INCB") tarafından gerçekleşmektedir. Interpol İnternet üzerinde gerçekleşen uyuşturucu trafiğini takip etmek için özel bir birim kurmuştur[356]. Ayrıca INCB uyuşturucu dâhil her türlü yasadışı kimyasalın ve ilacın İnternet üzerinden satılmasını önlemek amacıyla tavsiye kararlar yayınlamıştır[357]. Bu kararlarda, devletlerin İnternet üzerinden yasadışı kimyasalların satılmasını önlemek için gerekli mevzuat değişikliklerinin yapılmasını ve ülke çapında faaliyet gösteren servis sağlayıcıların bu tür içeriği barındırmasının engellenmesi öngörülmüştür.

5237 sayılı TCK'nın 190. maddesi uyuşturucu ve uyarıcı madde kullanımının yaygınlaşmasını önlemek için uyuşturucu veya uyarıcı madde kullanımını kolaylaştırmak ve kullanımı özendirmek fiillerini suç olarak kabul etmiştir.

Kullanımı kolaylaştırmak fiili söz konusu hükme göre üç farklı şekilde işlenmesi mümkündür. İlk durum, uyuşturucu kullanımı için özel yer, do-

---

[353] Single Convention on Narcotic Drugs, 1961, as amended by the Protocol amending the Single Convention on Narcotic Drugs, http://www.unodc.org/pdf/convention_1961_en.pdf; 2001/2577 Uyuşturucu Maddelere Dair 1961 Tarihli Tek Sözleşme'nin Tadiline İlişkin Protokol'un Onaylanması Hakkında Karar, RG 30.06.2001/24448.

[354] Convention on Psychotropic Substances, 1971, http://www.unodc.org/pdf/convention_1971_en.pdf.

[355] Convention against the Illicit Traffic in Narcotic Drugs and Psychotropic Substances, 1988, http://www.unodc.org/pdf/convention_1988_en.pdf.

[356] Psychotropics Desk, http://www.interpol.int/public/Drugs/synthetic/default.asp.

[357] Guidelines for Governments on Preventing the Illegal Sale of Internationally Controlled Substances through the Internet, http://www.incb.org/pdf/Internet_Guidelines/Internet_guidelines_English.pdf.

nanım veya malzeme sağlamaktır. Suçun oluşması için kişiye uyuşturucu veya uyarıcı madde verilmesi gerekmemektedir[358]. Ayrıca suçun oluşması için kendisine kolaylık sağlanan kişinin uyuşturucu veya uyarıcı madde kullanması da gerekmemektedir[359]. Kullanıma kolaylaştırmak fiilinin bir diğer görünümü ise uyuşturucu veya uyarıcı madde kullananların yakalanmalarını zorlaştırıcı önlemler almaktır. Son durum ise uyuşturucu veya uyarıcı madde kullanma yöntemleri konusunda başkalarına bilgi vermektedir.

Bu fiillerden kullanma yöntemleri konusunda başkalarına bilgi verme fiilinin İnternet ortamındaki yayınlarla işlenmesi mümkündür. İnternetin uyuşturucu türleri, üretim teknikleri ve üretim için hammaddelerin nasıl temin edilebileceğine ilişkin bilgi edinilmesi amacıyla yaygın olarak kullanılmaktadır. İnternetin sağladığı anonimlik İnterneti cazibeli kılmaktadır. Her ne kadar uyuşturucuya ilişkin bilgiler İnternette açık bir şekilde yayınlanmasa da, uyuşturucu satıcıları ve alıcılar İnternet forumlarında ve sohbet odalarında buluşmaktadırlar. Bu şekilde İnternet hem uyuşturucu ve uyarıcı maddeler hakkında bilgi vermek hem de suç failleri arasında iletişim aracı olarak kullanılmaktadır. Dolayısıyla, bu tür içerikli web sitelerinin erişimi 5651 sayılı Kanun'un 8. madde hükmü gereğince engellenebilecektir.

Öte yandan uyuşturucu ve uyarıcı madde kullanımını alenen özendirilmesi veya bu doğrultuda yayın yapılması ayrı bir suç olarak kabul edilmiştir[360]. Bu suçun oluşması için özendirme fiilinin aleni bir şekilde yapılması gerekmektedir. Kanunda aleniyete ilişkin bir tanım verilmemektedir. Özendirme fiili doğrudan veya dolaylı ifadelerle gerçekleşmesi mümkündür. Bu sebeple, uyuşturucu veya uyarıcı madde kullanma yöntemleriyle ilgili bilgi verme fiiline nazaran özendirme fiili belirsizlik taşımaktadır.

Uyuşturucu veya uyarıcı madde kullanımını özendirme fiiline ilişkin bir içeriğin salt İnternet ortamında yer alması aleniyet şartının gerçekleşmesi için yeterli değildir. İnternet üzerinden forum, sohbet odaları, eposta gibi farklı servisler kullanarak bilgi paylaşımını ve iletişimi

---

[358] *Özmen*, TCK gerekçesi, s. 500.

[359] *Özmen*, TCK gerekçesi, s. 500.

[360] 5237 sayılı TCK, m. 190 f. 2.

gerçekleştirmek mümkündür. Bir forum veya sohbet odasının erişiminin kısıtlanması ve bilgi paylaşımı ile iletişimin yalnızca izin verilen belirli kullanıcılarla gerçekleştirilmesi mümkündür. Bu sebeple, somut olayın özellikleri göz önüne alınarak, kullanılan servise göre erişim engelleme kararının verilmesi gerekmektedir.

Son olarak, bir web sitesinde uyuşturucu veya uyarıcı madde kullanılmasını kolaylaştırmaya ilişkin içeriğin yer alması sebebiyle tüm sitenin erişiminin engellenmesi özellikle bazı durumlarda hakkaniyete uygun olmayan sonuçlar doğurması mümkündür. Her şeyden önce uyuşturucu ve uyarıcı madde kullanılmasını kolaylaştırma fiilleriyle web sitesinin içerik sağlayıcısı ve diğer ilgilileri arasında bağlantı kurulması gerekmektedir. Bazı kullanıcıların web sitesini bu tür fiiller için araç olarak kullanması sebebiyle tüm web sitesinin cezalandırılması ceza sorumluluğunun şahsiliği ilkesine aykırılık oluşturacaktır.

TİB İhbar İstatistiklerine göre uyuşturucu veya uyarıcı madde kullanılmasını kolaylaştırma suçuyla ilgili 179 ihbar yapılmış ve 2'si re'sen, 1'i de yargı kararıyla olmak üzere toplam 3 web sitesinin erişimi engellenmiştir[361].

4. Sağlık için tehlikeli madde temini

Devlet, Anayasanın 58. maddesi gereğince gençliği alkol düşkünlüğünden ve benzeri kötü alışkanlıklardan korumak için gerekli tedbirleri almakla yükümlüdür. Bu doğrultuda 5237 sayılı TCK 194. maddesinde tehlike oluşturan maddelerin çocuklara, akıl hastalarına veya uçucu madde kullananlara verilmesini veya bu tür kişilerin tüketimine sunulması suç kabul etmiştir. Ayrıca, 5651 sayılı Kanun, bu suçun İnternet ortamında yapılan yayınlarla oluştuğu yönünde yeterli şüphe bulunması durumunda erişim engelleme kararı verilebileceğini öngörmüştür[362].

5237 Kanunda tehlikeli maddenin tanımını yer almamaktadır. 194. maddenin gerekçesinde suçun konusunun alkollü içkiler tütün ve tiner maddeleri gibi sağlık için tehlikeli olan her tür çeşit madde olduğu belir-

[361] Bkz. *İhbar İstatistikleri*, dn. 321.

[362] 5651 sayılı Kanun, m. 8 f. 1(a).

tilmişse de suçta ve cezada kanunilik ilkesi gereğince tehlikeli maddenin kanunda açıkça düzenlenmesi gerekmektedir[363].

Suç sağlık için tehlikeli olabilecek maddelerin çocuklara, akıl hastalarına veya uçucu madde kullananlara verildiği anda veya sayılan kişilerin tüketimine sunulduğu anda oluşmaktadır. Bu sebeple, suça teşebbüs de suç gibi cezalandırılmaktadır. Suçun mağduru çocuklar ve yaşlarına bakılmaksızın akıl hastası veya uçucu madde kullanıcılarıdır.

İntihara yönlendirme veya çocukların cinsel istismarı gibi suçlar İnternet üzerinden doğrudan işlenebilmesine rağmen, sağlık için tehlikeli madde temininin İnternet üzerinden işlenmesine mümkün değildir. Nihayetinde, bu suçun oluşması için sağlık için tehlikeli olabilecek maddelerinin fiziksel olarak çocuklara, akıl hastalarına veya uçucu madde kullanıcılarına verilmesi veya tüketime sunulması gerekmektedir. Bu sebeple, İnternet bu suçta sadece araç olarak kullanılması mümkündür.

5651 sayılı Kanun'un 8. maddesine göre, 5237 sayılı TCK'nın 194. maddesinde yer alan sağlık için tehlikeli madde teminine ilişkin suçunun İnternet ortamında yapılan yayınlarla oluştuğu yönünde şüphe bulunması durumunda erişim engellenmesi kararı verilebilecektir. Ancak, bu hükmün dar yorumlanması durumunda, sağlık için tehlikeli madde temini suçunun İnternet ortamındaki yayından dolayı oluşması mümkün olmadığı için erişim engelleme sebebi konusuz kalmaktadır. Ayrıca, tehlikeli maddenin tanımı 5237 sayılı TCK'da yer almaması suçun uygulamasında belirsizlik oluşturmaktadır.

194. madde hükmünün İnternet ortamında uygulanması önünde bir diğer sorun ise İnternet ortamında kullanıcıların yaşlarının veya diğer niteliklerinin tespit edilmesinin mümkün olmamasıdır. Daha önce açıklandığı üzere, İnternet ortamında kullanıcıların yaşının kesin tespit edilmesi her zaman mümkün olmamaktadır. Ayrıca mevcut teknolojiler İnternet ortamının kesif bir şekilde çocuklara ve erişkinlere özel alan oluşturacak şekilde ayrılmasına olanak vermemektedir. Nihayetinde 194.

[363] Bağımlılık yapan uyuşturucu veya uyarıcı maddelere ilişkin TCK'da özel hükümler yer aldığı için bu maddenin kapsamı dışında kalmaktadır. Bkz. *Özmen*, TCK gerekçesi, s. 507.

maddenin yasakladığı fiil tehlikeli maddelere çocukların, akıl hastalarının veya uçucu madde kullanıcılarının ulaşmaması olduğu için, tehlikeli maddelere ilişkin içerik barındıran bir web sitesine sadece bir çocuğun, akıl hastasının veya uçucu madde kullanıcısının erişmesi sitenin tüm içeriğini hukuka aykırı bir hale getirecektir.

Öte yandan, 4207 sayılı Tütün Ürünlerinin Zararlarının Önlenmesi ve Kontrolü Hakkında Kanun[364] gibi özel kanunlarda bazı sağlık için tehlikeli olabilecek bazı maddelere ilişkin hükümler yer almaktadır. Örneğin, 4207 sayılı Kanun 3. maddesinde tütün ürünlerinin ve üretici firmaların isim, marka veya alametleri kullanılarak her ne suretle olursa olsun reklam ve tanıtımı yapılamayacağını kabul etmiştir. Benzer bir şekilde, 4250 sayılı İspirto ve İspirtolu İçkiler İnhisarı Kanunu[365] 19. maddesi, alkol, bira ve şarap dâhil her çeşit alkollü içkinin televizyon, kablolu yayın, radyo ve kamu yayın araçlarıyla reklamının yapılması, ayrıca, içki satış yerleri ile tüm ticari ve kamuya açık yerlerde, tüketilmek veya beraberinde götürülmek üzere on sekiz yaşından küçüklere alkollü içecek satılması veya sunulmasını yasaklamıştır[366]. 3984 sayılı RTÜK Kanunun 22. maddesi ise alkol ve tütün ürünleri reklamlarına izin verilmeyeceğini kabul etmiştir.

5651 sayılı Kanun'un sayılan söz konusu düzenlemeler karşısında hem yeni tarihli hem de özel kanun olması ve ayrıca erişim engelleme sebeplerinin sınırlı sayı ilkesine göre belirlenmesi sebebiyle bu hükümlere dayanarak bir web sitesinin erişiminin engellenmesi mümkün bulunmamaktadır.

TİB İhbar İstatistiklerine göre sağlık için tehlikeli madde temini suçuyla ilgili 149 ihbar yapılmış ve 11'i re'sen 1'i de yargı kararıyla olmak üzere toplam 12 web sitesinin erişimi engellenmiştir[367].

---

[364] Kanun No: 4207, Kabul T.: 07.11.1996, RG 26.11.1996/22829.

[365] Kanun No: 4250, Kabul T.: 08.06.1942, RG 12.06.1942/5130.

[366] Daha fazla bilgi için bkz. Alkollü İçkilerde Reklam ve Satış Geliştirmede Uyulacak İlke ve Kriterler, http://www.tapdk.gov.tr/alkol_duyuru9.htm.

[367] Bkz. *İhbar İstatistikleri*, dn. 321.

5. Müstehcenlik

5651 sayılı Kanunda öngörülen bir diğer engelleme sebebi ise 5237 sayılı TCK'nın 226. maddesinde yer alan müstehcenlik suçudur. TİB İhbar İstatistiklerine göre müstehcenlik suçuyla ilgili 21.016 ihbar yapılmış ve 846'sı re'sen, 121'i de yargı kararıyla olmak üzere toplam 967 web sitesinin erişimi engellenmiştir[368]. Bu istatistikler göz önüne alındığında 5651 sayılı Kanun çocukların cinsel istismarı suçundan sonra en çok müstehcenlik suçu için uygulama alanı bulmuştur.

5237 sayılı TCK'nın 226. çocukların ve genel ahlakın korunması temel amacıyla müstehcen içeriğin suç olarak kabul edileceği halleri ayrıntılı olarak düzenlemiştir[369]. Bu maddeye göre suç kabul edilen ilk durum çocuklara görüntü, yazı veya sözler içeren ürünler vasıtasıyla müstehcen içeriğe erişim sağlanmasıdır. Erişim sağlama fiili doğrudan veya dolaylı olarak gerçekleştirilmesi mümkündür. Doğrudan erişim, müstehcen içeriğin çocuğa gösterilmesi, okunması, okutulması veya dinletilmesi gibi farklı fiillerle gerçekleştirilebilir. Dolaylı erişimin ise iki farklı görünümü bulunmaktadır. İlk görünüm müstehcen içeriklerin çocukların girebileceği veya görebileceği yerlerde ya da alenen sergilenmesi, okutulması, söylenmesi veya söyletilmesi şeklindedir. İkinci görünüm ise müstehcen içeriğe vakıf olunabilecek şekilde veya bu tür ürünlerin mahsus satış yerleri dışında satışa veya kiraya arz edilmesi veya ücretsiz dağıtılmasıdır.

---

[368] Bkz. *İhbar İstatistikleri*, dn. 321.

[369] Müstehcenliğe devletin müdahalesin lehinde ve aleyhinde farklı görüşler ileri sürülmüştür. İlk olarak, müstehcenliğin ahlak dışı olması sebebiyle toplumun kendi ahlak standartlarının korunması için egemen ahlak değerlerine uymayan içeriği sınırlandırması gerektiği ileri sürülmüştür. İkinci olarak, müstehcenliğin kişileri bazı toplum dışı davranışlara sürüklemesi iddiasıyla müdahale meşrulaştırılmaya çalışılmıştır. Son olarak, müstehcenliğin yasaklanmasının çevresel nedenlerle isabetli olduğu ileri sürülmüştür. Bu iddialara karşı müstehcenlik bireyin iç dünyasına ait bir husus olduğu için bu alanda herhangi bir devlet müdahalesinin olmaması gerektiği ileri sürülmektedir. Bu görüş, nihayetinde müstehcen içeriğin kullanılmasının ya gizli ya da başkalarına zarar vermeden gerçekleştirilmesi sebebiyle devletin müdahaleyi haklı kılacak bir menfaatinin olmadığı savıyla desteklenmektedir. Diğer bir deyişle, devletin hukuk sistemi aracılığıyla belirli bir ahlak anlayışını zorlamaması gerektiği düşünülmektedir. Daha fazla bilgi için bkz. Frederick Schauer, İfade Özgürlüğü: Felsefi Bir İnceleme (çeviren: M. Bahattin Seçilmişoğlu), Ankara 2002 ("*Schauer*"), s. 244 vd.

Tüm bunların yanı sıra, hüküm ayrıca müstehcen içeriğin reklamını da yasaklamaktadır.

Müstehcen içeriğin basın ve yayın yoluyla yayınlanması veya yayınlanmasına aracılık edilmesi cezayı ağırlatıcı bir neden olarak kabul edilmiştir. Çocukların daha etkin bir şekilde korunması amacıyla da müstehcen içeriğe sahip ürünlerin üretiminde çocukların kullanılması yasaklanmıştır. Tüm bunların yanı sıra, şiddet kullanılarak, hayvanlarla, ölmüş insan bedeni üzerinde veya doğal olmayan yoldan yapılan cinsel davranışlara ilişkin her türlü içerik müstehcenlik suçunun kapsamına alınmış ve yasaklanmıştır.

Kanun, bilimsel eserleri mutlak bir şekilde müstehcenlik suçunun kapsamı dışında tutulmuştur. Bu sebeple cinsel bir eğitim kılavuzu, ya da cinselliğin antropolojik, sosyolojik, tıbbi veya tarihi yönlerini içeren her türlü içerik müstehcenlik suçunun kapsamı dışında kalmaktadır[370]. Sanatsal ve edebi değeri olan eserler için ise koşullu muafiyet tanınmıştır. Kanun, bir sanatsal ve edebi değeri olan eserin 266. maddenin kapsamı dışında tutulabilmesi için her koşulda müstehcen içeriğe sahip ürünlerin üretilmesinde çocukların kullanılmasını yasaklayan hükme riayet edilmesini ve çocukların bu tür eserlere ulaşmasının engellenmesini zorunu kılmaktadır.

Her ne kadar 226. madde müstehcen içeriğe ilişkin fiilleri ayrıntılı olarak saymışsa da maddede müstehcenliğin tanımı yer almamaktadır[371]. Benzer bir şekilde sanatsal ve edebi değeri olan eserlerin nasıl belirleneceğine ilişkin bir kıstas koymamaktadır. Madde gerekçesinde de bir tanım verilmeyerek, müstehcenliğin belirlenmesinde hayâsızca hareketler başlıklı 225. maddesinin gerekçesinde yer alan ahlaka yönelik açıklamaların göz önünde bulundurması gerektiğini belirtmekle yetinilmiştir[372]. Ancak ne 225. maddede ne de gerekçesinde müstehcenliğin tanımı yer almamaktadır. 225. maddenin gerekçesinde hayatsızca davranışlar genel edep ve ahlaka alenen niteliği taşıyan hareketler, tutum ve davranışlar olarak

---

[370] *Schauer*, a.g.e., s. 251.

[371] Benzer bir tanım 765 sayılı TCK'da da yer almamaktaydı.

[372] *Özmen*, TCK gerekçesi, s. 574

tanımlanmıştır[373]. Kanun amacına uygun bir şekilde uygulanabilmesi için genel ahlakın ve müstehcenliğin tanımının yapılması gerekmektedir. Benzer bir şekilde sanat ve edebi kavramları da göreceli olabileceği için müstehcenlik gibi bu kavramların da açıklanması gerekmektedir.

Anayasa Mahkemesi 1964 yılında vermiş olduğu bir kararda genel ahlakı belirli zamanda, belirli bir toplumun büyük çoğunluğunca benimsenmiş kolayca anlaşılan ahlak kurallarının bütünü olarak tanımlamıştır[374]. Bu karar genel ahlakın sınırlarını kesin çizmemekte ve somut olayın özelliklerine göre bir değerlendirme yapılmasını tavsiye etmektedir.

Müstehcenlik kavramının zamana, kişilere ve yere bağlı olarak değişen bir kavram olduğu[375] ve müstehcenlik anlayışının toplumdan topluma değiştiği gibi, aynı toplum içinde kültürel değerlere bağlı olarak zaman içerisinde değişikliğe uğradığı kabul edilmektedir[376]. TDK, müstehcenliği "açık saçık, edebe aykırı, yakışıksız" olarak tanımlamaktadır. Müstehcenlik ayrıca "duygular açısından tiksindirici, nefret uyandıran, pis, açık-seçik, iğrendirici ve hoş olmayan şeyler" şeklinde de tanımlanmaktadır[377].

Yargıtay'ın müstehcenliğe ilişkin kararlarında yeknesaklık bulunmamakta ve müstehcenliğin belirlenmesine ilişkin koyulan kıstaslar her somut olayda farklı sonuçlar vermektedir. Yargıtay, 1993 tarihinde cinsel organın göründüğü bir kadın resmine ilişkin olarak vermiş olduğu kararda, resmin küçüklerin maneviyatı üzerinde olumsuz etki yaratacağı gerekçesiyle müstehcenlik suçunun oluştuğuna karar vermiştir[378].

---

373 *Özmen*, TCK gerekçesi, s. 572.

374 Anayasa Mahkemesi, K.T.: 28.01.1964, E: 1963/128, K: 1964/8, RG 17.04.1964/11685. Karar metni için bkz. http://www.anayasa.gov.tr/eskisite/kararlar/iptalitiraz/K1964/K1964-08.htm.

375 Cengiz Otacı, Genel Adap ve Aile Düzenine Karşı İşlenen Suçlar, Ankara 2000 ("*Otacı*"), s. 247.

376 Cevat Özel, 5651 sayılı İnternet ortamında yapılan yayınların düzenlenmesi ve bu yayınlarlar yoluyla işlenen suçlarla mücadele edilmesi hakkında kanun hakkında düşünceler, http://www.turkhukuksitesi.com/makale_626.htm ("*Özel*, Türk Hukuk Sitesi").

377 *Schauer*, a.g.e., s. 245.

378 Yargıtay 7. CD, K.T.: 21.10.1993, E: 1993/5454, K: 1993/5691; Bkz. *Özel*, Türk Hukuk Sitesi.

Yargıtay bu kararında müstehcenliği cinsel organların görünmesiyle ilişkilendirmesine rağmen, Yargıtay uygulaması bu doğrultuda gelişmemiştir. Yargıtay Ceza Genel Kurulunun 1996 yılında çıplak ancak cinsel organları görünmeyen iki kadın fotoğrafıyla ilgili vermiş olduğu bir kararda Anayasa Mahkemesinin genel ahlak esasına göre değerlendirme yapılması gerektiğini vurgulamış ve bir içeriğin müstehcen olup olmadığının tespit edilebilmesi için sübjektif ve objektif olmak üzere iki aşamalı bir değerlendirmenin yapılması gerektiğini belirtmiştir[379]. Sübjektif değerlendirmeye göre, fiilin işlendiği zamanki sosyal ve kültürel düzeyin göz önünde bulundurulmasının yanı sıra failin cinsel duyguları tahrik gayesi olup olmadığının araştırılması gerekmektedir. Bu değerlendirmeden sonra objektif olarak müstehcen olduğu iddia edilen içeriğin, içeriği okuyan, dinleyen veya izleyen kişiler üzerindeki etkisinin tespit edilmesi gerekmektedir. Yargıtay, yapmış olduğu inceleme sonucunda somut olayda çıplak kadın resminde kadının cinsel organının gösterilmediği, resmin estetik amaçlarla sunulduğu ve failin bu resimleri cinsi arzuları istismar amacıyla yayınlamadığı gerekçesiyle resmi müstehcen bulmamıştır.

Doktrinde, müstehcenlik erotizm ve pornografi olmak üzere ikiye ayrılmaktadır[380]. Müstehcenliğin tanımı ne kadar muğlâk ise, erotizm ve pornografinin de tanımı aynı derecede muğlâktır[381]. Erotizm şiddet içermeyen, aşağılayıcı olmayan ve rızaya dayalı cinsel aktivitelerin sözsel ya da görsel temsili şeklinde tanımlanmaktadır[382]. Erotizm, cinsellik içermesine rağmen cinsel uyarımın ön plana geçmediği ve cinsel organların görünmediği içerik olarak da tanımlanmaktadır. Pornografi ise cinsel organların uyarılmış biçimleriyle dile getirilmesi ya da gösterilmesi olarak tanımlanmaktadır[383]. Pornografinin temel amacının salt cinsel uyarılmayı sağlamak olduğu kabul edilmektedir.

[379] Yargıtay CGK, K.T.: 19.03.1996, E: 1996/5-27, K: 1996/47; Bkz. *Özel*, Türk Hukuk Sitesi.

[380] Melih Yürüşen, Pornografiyi İfade Özgürlüğü Bağlamında Düşünmek, Teorik ve Pratik Boyutlarıyla İfade Hürriyeti (Editör: Bekir Berat Özipek), (s. 209-244), Ankara 2003 ("*Yürüşen*"), s. 215.

[381] *Dülger*, a.g.e., s. 1522.

[382] *Yürüşen*, a.g.e., s. 215.

[383] Cemal Bâli Akal, İktidarın Üç Yüzü, 2. Baskı, Ankara 2003 ("*Akal*"), s. 278 ve orada dn. 216'da anılan *Beatrice Faust*, Kadınlar, seks ve pornografi, s. 23.

Erotik içerikte sanatsal veya edebi başkaca bir değerin ön plana çıkması sebebiyle bir ifade tezahürü olarak korunması gerektiği ileri sürülmektedir[384]. Ancak, pornografinin ifade hürriyeti kapsamında korunmasını gerekli kılacak meşru bir ifade içermemesi sebebiyle cinsel uyarımı sağlamak amacıyla yapılan hareketlerin bir toplamı olarak kabul edilen pornografi korunmaya değer görülmemektedir[385]. Ayrıca, pornografinin siyasal bir yönü olduğu düşünülmektedir. Pornografinin siyasallığı kadını nesneleştirmesi ve kadın/erkek ilişkisini tek yönlü bir erkek egemenliğine dönüştürmesidir[386]. Ayrıca, şiddet ve aşağılama içermesidir[387]. Pornografi bu sebeplerle de korumaya değer görülmemektedir.

Çocukların zararlı içerikten korunmasına ilişkin 5237 sayılı TCK'nın 226. maddesinde yer alan düzenleme dışında 1927 tarihli 1117 sayılı Küçükleri Muzır Neşriyattan Koruma Kanununda hükümler yer almaktadır. Daha önce açıklandığı üzere, 5651 sayılı Kanun'un hazırlanmasının temel nedeni olarak 1117 sayılı Kanun gibi bazı özel kanunların bilişim teknolojilerinde yaşanan hızlı gelişmeler sebebiyle İnternet ortamında yapılan ve içerikleri suç teşkil eden yayınların önlenmesinde yetersiz kalması gösterilmiştir[388].

1117 sayılı Kanun, muzır olarak adlandırdığı zararlı içeriğin belirlenmesi hususunda Başbakanlığa bağlı Küçükleri Muzır Neşriyattan Koruma Kurulu'nu yetkili kılmıştır. Kurul, Kanun'un 2. maddesine göre

---

384 *Schauer*, a.g.e., s. 251.

385 *Schauer*, a.g.e., s. 250;

386 *Akal*, a.g.e., s. 278.

387 *Yürüşen*, a.g.e., s. 215; Pornografinin cinsellik dışında şiddet pornografisi şeklinde farklı bir görünümü olduğu kabul edilmektedir. Şiddet pornografisi, şiddetin sansürlenmeden tüm vahşeti ile gösterilmesi olarak tanımlanmaktadır. Şiddet pornografisinin yaygın olarak sanatsal ve siyasi amaçlarla kullanılması bu tür içeriğin engellenmesinde tartışmalara yol açmaktadır. Örneğin, savaşın dehşetine vurgu yapmak amacıyla bir filmde şiddet sonucu ölümün canlı tasviri kullanılabilmektedir. Salt şiddet içeriğinin sanatsal veya siyasal bir mesaj içermediği sürece ifade hürriyeti kapsamında korunmayacağı kabul edilmektedir. Türk Hukukunda şiddet pornografisi müstehcenliğin bir görünümü olan pornografi altında kabul edilirse şiddet pornografisi için de erişim engellemesi gündeme gelebilecektir. Bu doğrultuda bir web sitesinin erişimi içeriğinde yer alan ceset teşhiri, idam veya cinayet görüntüleri sebebiyle engellenebilecektir. Bkz. *Schauer*, a.g.e., s. 252.

388 Bkz. yuk. §6 III C 1.

müstehcenlik suçu gibi suçlara ilişkin olarak adli makamlar için resmi bilirkişilik yapmakla görevlendirilmiştir. Ayrıca zararlı yayınların tespiti konusunda, hem re'sen hem de inceleme yapma yetkisini haizdir.

Kurul tarafından yapılan inceleme sonucunda bir içeriğin sakıncalı görülmesi durumunda, içeriğin yayınlanabilmesi veya gösterilebilmesi için herkesin kolayca görüp okuyabileceği şekil ve büyüklükte "küçüklere zararlıdır" ibaresinin ilgili içeriğin üzerine basılmasını zorunlu tutulmuştur[389]. Ayrıca, bu tür içeriğin ancak 18 yaşından büyüklere içi görülmeyen zarf veya poşet içinde, üzerinde "küçüklere zararlıdır" etiketiyle satılabilecektir. Kanun, 5237 sayılı Kanunun 226. maddesi gibi "fikri, içtimai ve bedii kıymeti haiz olan" eserleri kapsamı dışında tutmuştur.

Tüm bu düzenlemelere ve tanımlamalara rağmen, bir içeriğin ne zaman müstehcen sayılacağı; müstehcen bir içeriğin ne zaman erotik veya pornografik olarak nitelendirileceği veya müstehcen içeriğin ne zaman bilimsel veya sanatsal amaçlarla korunacağı her somut olayda ayrı ayrı değerlendirilmesi gereken bir sorundur. Kavramlardaki bu belirsizlik Türk Hukukunda olduğu kadar ABD Hukukunda da giderilmemiştir. Müstehcenliğin tespit edilmesi için psikolojik testlerin yapılması dahi önerilmektedir[390]. Buna göre, müstehcen içeriğin farklı kişilere gösterilerek fizyolojik tepkilerinin, hızının ve şiddetinin ölçülmesi ve çıkan sonunca göre içeriğin müstehcen olup olduğuna karar verilmesi tavsiye edilmektedir. Ancak, bu testler de pratik olmadıkları gibi her zaman tutarlı sonuçlar da vermeyeceklerdir. Amerikan Yüksek Mahkemesi Yargıcı Potter Stewart müstehcenliğe ilişkin vermiş olduğu bir kararda "onu tanımlayamam, fakat gördüğüm zaman tanıyabilirim"[391] demek suretiyle konunun ne kadar göreceli ve yoruma dayalı olduğunu özetlemiştir. Bu husus göz önüne alındığında, ahlak, müstehcenlik, erotizm, pornografi, sanat, edebi nitelik, toplum için kabul edilebilirlik gibi kavramların doğrudan mahkemeler tarafından yorumlanması gerekmektedir. Bu sebeple, TİB'in müstehcenlik suçuna ilişkin olarak re'sen erişim engelleme kararı

[389] 1117 sayılı Kanun, m. 4.

[390] *Yürüşen*, a.g.e., s. 216.

[391] *Yürüşen*, a.g.e., s. 216.

vermesi eleştirilmektedir[392]. Ancak, hukuka aykırı içeriğe ilişkin ivedi hareket etme zorunluluğu olduğu için bu tür yetkiler demokratik birçok düzende TİB gibi idari makamlara verilmiştir.

Öte yandan tanımındaki muğlâklığa rağmen, müstehcenliğe ilişkin ceza hükümleri ile 1117 sayılı Kanunun hükümleri göz önüne alındığında, ister pornografik ister erotik müstehcen içerik barındıran web sitelerinin içeriklerini ziyaretçilerine doğrudan sunmamaları gerekmektedir. Bu tür web sitelerinin en azından giriş sayfalarında müstehcen içerik taşıdıklarına ilişkin bir uyarı yayınlamaları ve yaş, kimlik, kredi kartı doğrulama gibi sistemler kullanarak içeriklerini erişime açmaları gerekmektedir.

6. Fuhuş

5651 sayılı Kanun, ailenin ve gençliğin korunması amacına uygun olarak kişilerin ve özellikle çocukların fuhşa teşvik edilmesini suç kabul eden 5237 sayılı TCK'nın 227. maddesini bir erişim engelleme sebebi olarak kabul etmiştir[393].

Türkiye fuhşun önlenmesine ilişkin çeşitli uluslararası sözleşmeye taraftır. Bu sözleşmelerden, 4 Mayıs 1910 tarihinde Paris'te imzalanan Beyaz Kadın Ticaretinin Zecren Men'ine Dair Milletlerarası Sözleşme ile 30 Eylül 1921 tarihli Kadın ve Çocuk Ticaretinin Men ve Zecrine Dair Beynelmilel Cenevre Mukavelesine Lozan Anlaşmasını kabul etmekle taraf olmuştur[394]. 1910 tarihli Sözleşme bir kişinin ihtiraslarını tatmin etmek amacıyla, rızası olsa dahi bir kadın veya küçük bir kızın fuhuş için hizmetlerinin taahhüt edilmesini, bu amaçla götürülmesini veya sevk edilmesini suçun kurucu unsurları farklı ülkelerde işlenmiş olsa da cezalandırmaktadır. 1921 tarihli Sözleşme ise devletleri hangi cinsiyetten olursa olsun, çocuk ticareti yapan kişilerin tespiti ve cezalandırılması için gerekli tedbirleri alma hususunda yükümlü kılmıştır.

---

[392] *Dülger*, a.g.e., s. 1522; *Özel*, Türk Hukuk Sitesi.

[393] 5651 sayılı Kanun, m. 8 f. 1(a).

[394] Bu sözleşmeler Lozan Anlaşmasının 99 ve 100. maddelerinde sayılan milletlerarası anlaşmalar kapsamında kabul edilmiştir. Bkz. *Özmen*, TCK gerekçesi, s. 579.

Bu sözleşmeler dışında Türkiye ayrıca 1933 yılında imzaya açılan Reşit Kadın Ticaretinin Men'ine Dair Beynelmilel Cenevre Mukavelesine 1935 yılında taraf olmuştur. Sözleşme, 1910 tarihli Sözleşmeyle benzer hükümleri içermektedir. Son olarak Türkiye, 2 Aralık 1949 tarihinde Birleşmiş Milletler Genel Kurulunca kabul edilen İnsan Ticaretinin ve Başkasının Fuhşunu Sömürmenin İlgası Hakkında Sözleşmeye taraftır. Birleşmiş Milletlerin bu sözleşmesi fuhşu kişiliğinin haysiyet ve değerleriyle, toplum, aile ve kişilerin selametiyle bağdaşmadığını ve tüm bu değerleri tehlikeye soktuğunu kabul etmiştir. Tüm sözleşmeler, fuhşu hem ulusal hem uluslararası düzeyde kabul görmeyen bir davranış olarak gördükleri için hem de devletleri bu konuda tedbirler almakla yükümlü tuttukları için önem taşımaktadır.

5237 sayılı TCK'nın 227. maddesi çocukların ve yetişkinlerin fuhşunu benzer hükümlerle ancak farklı ağırlıkta cezai sorumluluklarla düzenlemiştir. Hükmün birinci fıkrası, çocuğun fuhşa teşvik edilmesi, fuhuş yolunun kolaylaştırılması, bu amaçlarla tedarik veya barındırma yapılması veya çocuğun fuhşuna aracılık edilmesi fiillerini cezalandırmaktadır. Ayrıca, sorumluluk daha öteye götürülerek, bu suçun işlenmesine yönelik her türlü hazırlık hareketini tamamlanmış suç gibi cezalandırmaktadır. İkinci fıkra ise, yetişkinlerin fuhşa teşvik edilmesini, bu yolun kolaylaştırılmasını, aracılık edilmesini veya yer temin edilmesini cezalandırmaktadır.

227. maddede sayılan çocukları ve yetişkinleri fuhşa teşvik etme, bunun yolunu kolaylaştırma ve aracılık etme fiillerinin İnternet ortamında yapılan yayınlarla işlenmesi mümkündür. Dolayısıyla, 5651 sayılı Kanun'un 8. maddesi uyarınca bu suçun İnternet ortamında yapılan yayınlarla oluştuğu yönünde şüphe bulunması durumunda içeriği barındıran web sitesi aleyhine erişim engellenmesi kararı verilebilecektir.

Fuhşa teşvik etme fiili daha çok arkadaşlık, çöpçatanlık ve sohbet siteleri gibi sosyal ağ siteleri kullanılarak işlenmektedir. Teşvik fiilinin belirli kişi veya kişileri hedef alarak gerçekleştirilmesi mümkündür. Bu sebeple, fuhşa teşvik fiilinin belirli kişileri hedef almadan gerçekleştirilen fuhşa özendirme fiilinden ayrılması gerekmektedir. İnternette fuhşa aracılık fiili de teşvik fiili gibi daha çok arkadaşlık, çöpçatanlık ve sohbet

siteleri gibi sosyal ağ siteleri üzerinden gerçekleşmektedir. Bu siteler kullanılarak fuhşa aracılık işlemleri gizlenmektedir. Ancak, fuhşa aracılık alenen yapılmadığı ve genellikle şifreli yazışmalar yapıldığı için bu tür aracılık işlemlerinin tespit edilmesi kolay olmamaktadır. Yazışmaların dolaylı yollarla yapılması sebebiyle, bu tür aracılık işlemlerini önleyecek etkili bir erişim engelleme tekniği bulunmamaktadır.

Öte yandan bir web sitesinde fuhşa teşvik ediliyor veya fuhşa aracılık yapılıyor olması sebebiyle o sitenin erişim engellemesi bazı durumlarda hakkaniyete uymayan sonuçlar doğurması mümkündür. Her şeyden önce fuhşa teşvik ve aracılık fiilleriyle web sitesinin içerik sağlayıcısı ve diğer ilgilileri arasında bağlantı kurulması gerekmektedir. Nihayetinde, bazı sosyal ağ sitelerinin kullanıcı sayısı milyonları bulabilmektedir. Bazı kullanıcıların web sitesini bu tür fiiller için araç olarak kullanması sebebiyle tüm web sitesinin cezalandırılması ceza sorumluluğunun şahsiliği ilkesine aykırılık oluşturacaktır.

TİB İhbar İstatistiklerine göre fuhuş suçuyla ilgili 2.861 ihbar yapılmış ve 20'si re'sen, 5'i de yargı kararıyla olmak üzere toplam 25 web sitesinin erişimi engellenmiştir[395].

7. Kumar oynanması için yer ve imkân sağlama

Kumar, 5237 sayılı TCK'da kazanç amacıyla icra edilen ve kâr ve zararı talihe bağlı olan oyunlar olarak tanımlanmıştır[396]. Türk hukukunda kumar oynamak kabahat[397], kumar oynatmak ve bu doğrultuda yer ve imkân sağlamak ise suç[398] olarak kabul edilmiştir. Bu doğrultuda, Türkiye'de kumarhanelerin faaliyet göstermesi yasaklanmıştır.

Türkiye'de kumarhanelerin yasak olmasının doğurduğu boşluğu, online kumarhaneler doldurmaktadır. Çoğu yurtdışında bulunan online kumar siteleri üzerinden futbol, basketbol, at yarışı, boks ve tenis maçları için hem

---

[395] Bkz. *İhbar İstatistikleri*, dn. 321.

[396] 5237 sayılı TCK, m. 228 f. 4.

[397] 5326 sayılı Kabahatler Kanunu, m. 34.

[398] 5237 sayılı TCK, m. 228.

bahis hem de eşzamanlı olarak poker, rulet gibi oyunlar oynanmaktadır[399]. Kumar oynanması için gereken para vergi ödenmeyerek havale ve kredi kartı gibi yollarla yurtdışındaki online kumar sitesine aktarılmaktadır. Bazı durumlarda ise aracı kişiler kullanılarak paranın yurtdışındaki hesaplara aktarılması sağlanmaktadır. Bu şekilde İnternet üzerinden oynanan kumar oyunları hem kara para trafiğine açık bir zemin hazırlamakta hem de büyük ölçülerde vergi kayıp ve kaçağına yol açmaktadır[400]. Türkiye'de 1.5 milyon kişinin İnternet üzerinden kumar ve bahis oynadığı, online kumar işletmelerinin yıllık cirolarının 1 milyar doları aştığı tahmin edilmektedir[401]. Yazılımların uyumlu hale getirilmesi sayesinde, cep telefonu üzerinden dâhi kumar oynamak mümkün hale gelmiştir. Bu nedenle online kumar sitelerinin ziyaretçileri hızlı bir şekilde artmaktadır.

İnternette online kumarhaneler genellikle denetimin az olduğu ve vergi cennetleri olarak da bilinen okyanus adalarından hizmet vermektedir[402]. Bu şekilde hukuki sorumluluktan kurtuldukları gibi bürokratik vergi ve kara para aklama denetimlerine maruz kalmamaktadırlar. Online kumarhanelerin normal kumarhanelere göre yatırım giderleri fazla olmadığı için çok daha yüksek oranlarda ikramiye dağıtmakta ve bu da cazibelerini artırmaktadır[403].

5651 sayılı Kanun, 5237 sayılı TCK'nın 228. maddesinde yer alan kumar oynanması için yer ve imkân sağlama suçunun İnternet ortamında

---

[399] Ercan Alptürk, Hukuksal, Teknik ve Vergisel Boyutlarıyla İnternette Kumar Oyunları, Lebib Yalkın Mevzuat Dergisi, Yıl: 2005, Sayı: 2 (Şubat) ("*Alptürk*"), s. 1.

[400] Online kumar sistemlerinin kolay erişilir olması, İnternet üzerinden yüklü miktarlarda para transferinin hızlı bir şekilde gerçekleşmesi ve oyunların anonim olarak oynanması online kumar sitelerinin kara para aklanması için kullanıldığı yönündeki şüpheleri artırmaktadır. Bkz. Gerd Alexander, The U.S. On Tilt: Why The Unlawful Internet Gambling Enforcement Act Is A Bad Bet, Duke Law & Technology Review, Rev. 6, 30 June 2008 ("*Alexander*"), s. 2; Online kumar sitelerinin vergiler açısından doğurduğu sorunlar için bkz. *Alptürk*, a.g.e., s. 3 vd.

[401] Ankara Ticaret Odası, Sanal Tuzak: İnternet Kumarhaneleri, http://www.atonet.org.tr/turkce/index9.html.

[402] Örneğin, 68.000 nüfuslu Antigua ve Barbuda ada devletinde 119 online kumarhane bulunmakta ve bu kumarhanelerde adanın nüfusunun %7'sine tekabül eden yaklaşık 5.000 kişi istihdam edilmektedir. Bkz. *Goldsmith/Wu*, a.g.e., s. 172.

[403] *Alptürk*, a.g.e., s. 2; *Alexander*, a.g.e., s. 2.

yapılan yayınlarla oluştuğu yönünde şüphe bulunması durumunda erişim engellenmesi kararı verilebilmesini kabul etmiştir[404]. Kumar oynanması için yer ve imkân sağlama suçunun oluşması için aleniyet şartı aranmamaktadır. Suç başkalarının kumar oynayabilmesi için yer veya başka suretle imkân sağlandığı anda oluşmaktadır[405]. Ayrıca, çocukların kumar oynaması için yer ve imkân sağlanması ağırlatıcı bir sebep olarak kabul edilmiştir[406]. Sağlık için tehlikeli madde suçunda olduğu gibi bu hükmün de İnternet ortamında uygulanması önünde bazı engeller bulunmaktadır. Web sitelerinin ziyaretçilerinin kesin yaşlarını tespit etmeleri mümkün bulunmamaktadır. Birçok web sitesinin ana sayfalarında yer alan yaş doğrulama sistemleri ise yanlış bilgiler verilmek suretiyle aşılmaktadır. Bu sebeple, çocukların kumar oynaması için yer ve imkân sağlanıp sağlanmadığının tespiti kolay gözükmemektedir.

5651 sayılı Kanun ilk yürürlüğe girdiği dönemlerde kumar oynanması için yer ve imkân sağlama suçuna ilişkin engelleme sebebi fazla dikkat çekmemiştir. Ancak, online kumar sitelerinde dolaşan paranın miktarının artması ve bu sitelere yönelik başta Milli Piyango İdaresi olmak üzere kamu otoritelerinin denetimlerini artırması sonucunda TİB'in bu suça yönelik çalışmaları ivme kazanmıştır.

TİB İhbar İstatistiklerine göre kumar oynanması için yer ve imkân sağlama suçuyla ilgili 986 ihbar yapılmış ve 74'ü re'sen, 19'u da yargı kararıyla olmak üzere toplam 93 web sitesinin erişimi engellenmiştir[407]. Ekonomik getirisinin fazla olması nedeniyle erişimi engellenen web siteleri isim değiştirerek faaliyetlerini sürdürmeye çalışmaktadır.

8. Sabit ihtimalli veya müşterek bahis oynatılması

Futbol ve spor müsabakaları üzerine sabit ihtimalli ve müşterek bahisler ile şans oyunları düzenleme konusunda 7258 sayılı Kanun, Gençlik

---

[404] 5651 sayılı Kanun, m. 8 f. 1(a).

[405] *Özmen*, TCK gerekçesi, s. 583.

[406] 5237 sayılı TCK, m. 228 f. 2.

[407] Bkz. *İhbar İstatistikleri*, dn. 321.

ve Spor Genel Müdürlüğü'nü yetkili kılmıştır[408]. 7258 sayılı Kanun, izinsiz olarak spor müsabakaları ile ilgili sabit ihtimalli veya müşterek bahis oynatılmasını ve bu amaçla yer ve imkân sağlanmasını suç kabul etmiştir[409]. Düzenleme bu haliyle kumar oynanması için yer ve imkân sağlamayı suç sayan 5237 sayılı TCK'nın 228. maddesi ile uyum içerisindedir.

Sabit ihtimalli ve müşterek bahis oyunlarının tanımı 5738 sayılı Spor Müsabakalarına Dayalı Sabit İhtimalli ve Müşterek Bahis Oyunlarının Özel Hukuk Tüzel Kişilerine Yaptırılması Hakkında Kanun'da[410] verilmiştir. Kanun sabit ihtimalli bahis oyunlarını "yurt içinde ve yurt dışında tertiplenen spor müsabakalarına ait sonuçların veya etkinliklerin tahmin edilmesi esasına göre oynatılan ve iştirak edenler arasından doğru tahmin edenlere, önceden belirlenen bahis oranlarıyla ikramiye kazandıran oyunlar"[411] şeklinde tanımlamıştır. Müşterek bahis oyunlarını ise "yurt içinde ve yurt dışında tertiplenen spor müsabakalarına ait sonuçların tahmin edilmesi üzerine oynatılan, hâsılatın önceden belirlenen ikramiye yüzdesinin, doğru sonucu tahmin eden iştirakçiler arasında paylaştırıldığı bahis oyunları"[412] şeklinde tanımlamıştır.

7258 sayılı Kanun, bu tür oyunların İnternet üzerinden oynatılması ihtimalini göz önünde bulundurarak İnternet ortamına ilişkin özel bir hüküm getirmiştir. Bu doğrultuda, yurt dışında oynatılan her çeşit bahis ve şans oyunlarının İnternet yoluyla ve başka bir şekilde erişim sağlanarak Türkiye'de oynanmasına imkân sağlanması suç olarak kabul edilmiştir[413]. Bu hükümle paralel bir şekilde, bahis veya şans oyunlarını oynamaya teşvik edenler hakkında düzenleme yapılmıştır. Nihayetinde, İnternet ortamında bahis oynatanlar reklamlarını genellikle İnternet ortamı üze-

---

[408] 7258 sayılı Kanun, 6132 sayılı At Yarışları Hakkında Kanun ile 320 s. Milli Piyango İdaresi Genel Müdürlüğü Kuruluş ve Görevleri Hakkında Kanun Hükmünde Kararname hükümleriyle bu kuruluşlara verilen müşterek bahis ile şans oyunları oynatma hak ve yetkilerini saklı tutmuştur.

[409] 7258 sayılı Kanun, m. 5 f. 1.

[410] Kanun No: 5738, Kabul T.: 21.02.2008, RG 27.02.2008/26800.

[411] 5738 sayılı Kanun, m. 2 f. 1(n).

[412] 5738 sayılı Kanun, m. 2 f. 1(h).

[413] 7258 sayılı Kanun, m. 5 f. 2.

rinden gerçekleştirmektedir[414]. Hatta yeni bağımlılar yaratmak için siteler eğitim bile vermektedir. Bu tür sitelerin yaygınlaşmasını önlemek için 7258 sayılı Kanun kişileri her türlü bahis veya şans oyunları oynamaya teşvik edenlerin cezalandırılacağını kabul etmiştir[415].

Yukarıda sayılan suçlarla mücadeleyi daha etkili kılmak için 7258 sayılı Kanun, bu suçlarla ilgili olarak 5651 sayılı Kanuna göre erişim engellemesi hükümlerinin uygulanacağını kabul etmiştir[416]. Ayrıca, Maliye Bakanlığı 7258 sayılı Kanun ile 6132 sayılı Kanunlarında yer alan müşterek hariç olmak üzere talih oyunlarının kanun dışı olarak sanal ortam üzerinden oynatılmasının takibi, denetlenmesi ve ilan ve reklamlarının önlenmesi amacıyla Sanal Ortamda Oynatılan Talih Oyunları Hakkında Yönetmelik[417] adlı yönetmeliği yürürlüğe koymuştur. Yönetmelik bilgisayar, İnternet, interaktif televizyon, cep telefonu ve benzeri tümü bilişim ortamlarında oynatılan talih oyunlarının denetlenmesini kapsamaktadır[418].

TİB İhbar İstatistiklerine göre sabit ihtimalli veya müşterek bahis oynatılması suçuyla ilgili 191 ihbar yapılmış ve 117'si re'sen, 20'si de yargı kararıyla olmak üzere toplam 137 web sitesinin erişimi engellenmiştir[419].

9. Atatürk aleyhine işlenen suçlar

5816 sayılı Atatürk Aleyhine İşlenen Suçlar Hakkında Kanun'da yer alan suçların İnternet ortamında yapılan yayınlarla oluştuğu yönünde şüphe bulunması durumunda erişim engellenmesi kararı verilebilecektir[420]. 5816 sayılı Kanun'da iki farklı suç yer almaktadır. Birinci suç, Atatürk'ün hatırasına alenen hakaret edilmesi veya sövülmesi suçudur[421]. İkinci suç

[414] *Alptürk*, a.g.e., s. 2.

[415] 7258 sayılı Kanun, m. 5 f. 4.

[416] Yabancı bahis sitelerinin erişimlerini engellemenin bir diğer sebebi olarak, yasal bahis sitelerinin kullanımını teşvik etmek ve bu şekilde elde edilen geliri vergilendirmek olduğu düşünülmektedir. Bkz. *Alptürk*, a.g.e., s. 3.

[417] RG 14.03.2006/26108.

[418] Sanal Ortamda Oynatılan Talih Oyunları Hakkında Yönetmelik, m. 4.

[419] Bkz. *İhbar İstatistikleri*, dn. 321.

[420] 5651 sayılı Kanun, m. 8 f. 1(a).

[421] 5816 sayılı Kanun, m 1 f. 1.

ise Atatürk'ü temsil eden heykel, büst veya abidelerin veya Atatürk'ün kabrinin tahrip edilmesi, kırılması, bozulması veya kirletilmesi suçudur[422]. Kanun söz konusu suçların iki veya daha fazla kişi tarafından toplu olarak, aleni, umuma açık yerlerde veya basın vasıtasıyla işlenmesini ağırlatıcı neden olarak kabul etmiştir[423].

Bu suçlardan sadece Atatürk'ün hatırasına alenen hakaret veya sövme suçunun İnternet ortamında yapılan yayınlarla işlenmesi mümkündür[424]. 5651 sayılı Kanun hakaret suçunu bir erişim engelleme sebebi olarak kabul etmemesine rağmen, 5816 sayılı Kanun buna istisna teşkil etmektedir. 5651 sayılı Kanun hakaret gibi kişilik haklarına saldırı dolayısıyla oraya çıkabilecek mağduriyetleri gidermek için yayından çıkarma ve cevap hakkı gibi özel bir mekanizma öngörmüştür[425]. 5651 sayılı Kanun ailenin ve gençliğin korunması temel amacıyla hazırlanmıştır. Kanunda bu amaç dışında yer alan tek ideolojik engelleme sebebi 5816 sayılı Kanunda yer alan suçlara ilişkin engelleme sebebidir.

5651 sayılı Kanun'da yer alan erişim engelleme sebeplerine ilişkin en yoğun tartışma Atatürk'e hakaret sebebiyle Amerikan Google Grubuna ait Youtube video paylaşım sitesi engellendiğinde ortaya çıkmıştır. Youtube dünyanın en çok ziyaret edilen 3. web sitesidir ve siteyi bir gün içerisinde 100 milyonu aşkın kişi ziyaret etmektedir. Youtube web sitesinin erişimi 5651 sayılı Kanun yürürlüğe girmeden önce de erişimi Atatürk'ü ve diğer kutsal değerleri aşağıladığı ve şiddet içerdiği iddia edilen videolar yüzünden farklı mahkemeler tarafından engellenmiştir[426].

5651 sayılı Kanun yürürlüğe girdikten sonra, ilk engelleme Atatürk aleyhine işlenen suçlar kapsamında Ankara 11. Sulh Ceza Mahkemesi

---

[422] 5816 sayılı Kanun, m 1 f. 2.

[423] 5816 sayılı Kanun, m. 2.

[424] 5816 sayılı Kanun, 765 sayılı TCK yürürlükte olduğu dönemde hazırlandığı için 765 sayılı TCK'nın 480. maddesinde yer alan "hakaret ve sövme" fiillerini cezalandırmaktadır. 5237 sayılı TCK'da hakaret ve sövme ayrımı kaldırılarak 125. maddesinde hakaret ve sövme fiillerini hakaret başlığı altında toplamıştır.

[425] Bkz. aşa. §6 IV D.

[426] Engelleme geçmişi için bkz. *Akdeniz/Altıparmak*, a.g.e., s. 30 vd; Youtube, http://tr.wikipedia.org/wiki/YouTube.

tarafından verilmiştir[427]. Bu mahkeme dışında, Sivas 2. Sulh Ceza Mahkemesi[428], Ankara 12. Sulh Ceza Mahkemesi[429], Ankara 1. Sulh Ceza Mahkemesi[430] Atatürk aleyhine işlenen suçlar ve 5237 sayılı TCK'nın 301. maddesinde yer alan Türklüğü, Cumhuriyeti, Devlet kurumlarını ve organlarını aşağılama suçundan dolayı erişim engelleme kararı vermiştir[431]. Youtube aleyhine verilen erişim engelleme kararları farklı zamanlarda kaldırılmıştır. 1 Ekim 2009 itibariyle sadece Ankara 1. Sulh Ceza Mahkemesi'nin 05.05.2008 tarih ve 2008/402 numaralı engelleme kararı yürürlüktedir.

Youtube web sitesinin erişimin Türkiye tarafından engellenmesi Avrupa Birliği'nin Türkiye hakkında yayınladığı 2008 İlerleme Raporu'nda[432] eleştirilmiştir. Buna rağmen, engellemenin kaldırılmamasında Youtube şirketinin gereken işbirliğini göstermemesinin etkili olduğu ileri sürülmektedir[433].

Öte yandan, Youtube web sitesini engelleyen tek ülke Türkiye değildir. Türkiye dışında İran, Birleşik Arap Emirlikleri, Fas, Tayland, Irak, Brezilya, Avustralya (okullarda), Çin ve Hindistan gibi devletler farklı sebeplerle Youtube web sitesinin erişimini engellemiştir[434].

TİB, doğrudan erişim engelleme yoluna gitmek yerine uyarı mekanizmalarını işletmiş ve 5816 sayılı Kanun kapsamına giren içeriklerin 37 farklı web sitesinden kaldırılmasını sağlamıştır[435]. 5651 sayılı Kanunun

---

[427] Ankara 11. Sulh Ceza Mahkemesi, Değişik İş No: 2004/1431, K.T.: 17.12.2007.

[428] Sivas 2. Sulh Ceza Mahkemesi, Değişik İş No: 2008/11, K.T.: 16.01.2008.

[429] Ankara 12. Sulh Ceza Mahkemesi, Değişik İş No: 2008/55, K.T.:17.01.2008.

[430] Ankara 1. Sulh Ceza Mahkemesi, Değişik İş No: 2008/402, K.T.: 05.05.2008.

[431] Daha fazla bilgi için bkz. 5 Mayıs 2008 İtibariyle Son YouTube Erişime Kapatılma Olayı ve 5651 ile İlgili Gelişmeler, http://turk.internet.com/dosya/0809/yazilar/.

[432] Turkey 2008 Progress Report, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SEC:2008:2699:FIN:EN:PDF, s. 16.

[433] Youtube denetimi istemedi, http://www.tk.gov.tr/Basin_Duyurular/basintk/2008/02.08.2008/1d17f8.pdf.

[434] Censored: List of Countries that Banned YouTube, http://mashable.com/2007/05/30/youtube-bans/.

[435] Bkz. *İhbar İstatistikleri*, dn. 321.

asıl amacı engelleme yapmaktan ziyade sakıncalı görülen içeriğin İnternet ortamından çıkarılması olduğu için TİB'in bu yaklaşımı yerindedir.

TİB İhbar İstatistiklerine göre 5816 sayılı Atatürk Aleyhine İslenen Suçlar Hakkında Kanun'da yer alan suçlarla ilgili 2.972 ihbar yapılmış ve 2'si re'sen 54'ü de yargı kararıyla olmak üzere toplam 56 web sitesinin erişimi engellenmiştir[436].

10. Fikri mülkiyet ihlalleri

5651 sayılı Kanun dışında düzenlenen bir diğer engelleme sebebi ise 5846 sayılı Fikir ve Sanat Eserleri Kanunu'nda ("FSEK") yer almaktadır. 5846 sayılı FSEK'in Ek 4. maddesinde 2004 yılında yapılan değişiklikle fikri mülkiyet ihlalleri için İnternet ortamını da kapsayan özel bir erişim engelleme usulü getirilmiştir[437].

Ek 4. madde 5846 sayılı FSEK kapsamında eser sahibi veya bağlantılı hak sahibi sayılan kişilerin bu haklarının dijital ortamda ihlali halinde ihlale konu alan eserlerin içerikten çıkarılmasını öngörmektedir. Madde, İnternet ve dijital iletim dâhil işaret ses ve/veya görüntü nakline yarayan tüm araçları ve servis ve bilgi içerik sağlayıcıları tarafından yapılan tüm ihlalleri kapsamaktadır. Bu hükme göre, hak sahiplerinin herhangi bir ihlal ortaya çıktığı zaman öncelikle içerik sağlayıcıya başvurarak üç gün içerisinde ihlalin durdurulmasını istemeleri gerekmektedir. İhlalin içerik sağlayıcı tarafından durdurulmaması halinde yargısal sürecin başlatılması gerekmektedir. Bu doğrultuda Cumhuriyet savcısına başvurularak bu sefer servis sağlayıcıdan içerik sağlayıcına verilen hizmetin durdurulmasının talep edilmesi gerekmektedir. İhlalin durdurulması halinde bilgi içerik sağlayıcısına yönelik engelleme kaldırılacaktır. 5846 sayılı FSEK'te yer alan düzenleme bu haliyle *sui generis* nitelikte bir erişim engelleme yöntemi niteliğindedir.

---

[436] Söz konusu suçla ilgili toplam 55 adet erişim engellenme kararının 32'si aynı web sitesine ilişkin olarak farklı mahkemeler tarafından verilmiştir. Bkz. Bkz. *İhbar İstatistikleri*, dn. 321.

[437] Çeşitli Kanunlarda Değişiklik Yapılmasına İlişkin Kanun, Kanun No: 5101, Kabul T.: 03.03.2004, RG 12.03.2004/25400.

Öte yandan, Ek 4. maddede servis sağlayıcılara ilişkin bazı idari yükümlülükler getirilmiştir. Söz konusu hüküm, servis sağlayıcılara bilgi içerik sağlayıcılarının isimlerini gösterir listeyi her ay Kültür ve Turizm Bakanlığı'na[438] göndermekle yükümlü tutmuştur. Ayrıca servis ve bilgi içerik sağlayıcıların Bakanlıkça talep edilen her türlü bilgi ve belgeyi vermekle yükümlü oldukları esası öngörülmüştür. 5846 sayılı FSEK kapsamında genel yetkili Bakanlığın Kültür ve Turizm Bakanlığı olmasına rağmen, servis ve içerik sağlayıcılar gibi Ulaştırma Bakanlığı'nın görev ve yetki alanına giren bir konuda Kültür Bakanlığı'na görev ve yetkilerin verilmesi yerinde bir yaklaşım değildir.

C. Erişim engelleme yöntemi

1. Yetkili makamlar

Engelleme kararında yetkili makamlar engelleme sebebine göre ve içerik veya yer sağlayıcının ülke içinde olup olmamasına göre değişmektedir.

a. Adli makamlar

Erişim engelleme kararı, bir koruma tedbiri olarak soruşturma evresinde hâkim, kovuşturma aşamasında mahkeme tarafından verilecektir[439]. 5651 sayılı Kanun, ancak gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısı tarafından erişim engelleme kararı verilebileceğini kabul etmiştir[440]. Ancak, bu durumda Cumhuriyet savcısının kararı yirmi dört saat içerisinde hâkimin onayına sunması ve en geç yirmi dört saat içinde hâkimin kararını vermesini beklemesi gerekmektedir. Kararın bu süre içerisinde onaylanmaması durumunda erişim engelleme kararı hükümsüz hale gelecek ve uygulanan tedbir Cumhuriyet savcısı tarafından derhal kaldırılacaktır.

---

[438] Maddede geçen Bakanlık 5846 sayılı FSEK'in Tanımlar başlıklı 1/B maddesi gereğince Kültür ve Turizm Bakanlığı'dır.

[439] 5651 sayılı Kanun, m. 8 f. 2 c. 1.

[440] 5651 sayılı Kanun, m. 8 f. 2 c. 2.

b. TİB

TİB, iki durumda idari tedbir niteliğinde erişim engelleme kararı vermekle yetkilendirilmiştir. Birinci durum, içerik veya yer sağlayıcının bulunduğu yer esasına göre belirlenmiştir. Kanunun 8. maddesinin 1. fıkrasında sınırlı sayı prensibine göre sayılan suçları oluşturan yayınların içerik veya yer sağlayıcının yurt dışında bulunması halinde, TİB söz konusu web siteleri için re'sen erişimi engelleme kararı verebilecektir[441]. İkinci durum ise, işlenen suçun niteliğine göre belirlenmiştir. İçerik veya yer sağlayıcısı yurt içinde bulunsa bile, çocukların cinsel istismarı veya müstehcenlik suçlarını oluşturan yayınlara ilişkin TİB re'sen erişim engelleme kararı verebilecektir[442].

Bir web sitesinin 5651 sayılı Kanunun 8. maddesindeki suçlardan birisine ilişkin yeterli miktarda şüphe bulunup bulunmadığını belirleme yetkisinin yargısal bir işlem olması sebebiyle TİB gibi idari bir kuruma devredilmemesi gerektiği ileri sürülmektedir[443]. Bir konuda hem adli hem de idari makamlara yetkilendirmek yerinde görülmemektedir. Buna rağmen, hukuka aykırı içeriğe ilişkin ivedi hareket etme zorunluluğu olduğu için bu tür yetiler demokratik birçok düzende TİB gibi idari makamlara verilmiştir.

Eleştirilen bir diğer husus ise, 5651 sayılı Kanun ve ikincil düzenlemelerle TİB'e verilen erişim engelleme yetkisinde izlemesi gereken yöntemler arasındaki farklılıktır[444]. Yukarıda açıklandığı üzere, adli makamlar tarafından erişim engelleme kararları kural olarak hâkim tarafından gecikmesinde sakınca bulunan hallerde ise Cumhuriyet savcısı tarafından verilmektedir. Ancak bu durumda dahi kararın yirmi dört saat içerisinde hâkimin onayına sunulması zorunluluğu getirilmiştir. TİB tarafından verilen erişim engelleme sebeplerine ilişkin sadece çocukların cinsel istismarı ve müstehcenlik suçlarında içerik veya yer sağlayıcının yurtiçinde bulunması durumunda bir süre sınırı getirilmiştir. Bu suçlara ilişkin içe-

---

[441] 5651 sayılı Kanun, m. 8 f. 4.

[442] 5651 sayılı Kanun, m. 8 f. 4.

[443] *Dülger*, a.g.e., s. 1529.

[444] *Dülger*, a.g.e., s. 1530.

rik veya yer sağlayıcının yurtiçinde bulunması durumunda kararın, yirmi dört saat içinde hâkim onayına sunulması; kararın hâkim tarafından yirmi dört saat içerisinde onaylanmaması durumunda ise tedbirin TİB tarafından derhal kaldırılması öngörülmüştür[445]. Yurtdışı kaynaklı web siteleri için böyle bir onay zorunluluğu öngörülmemiştir. Cumhuriyet savcıları tarafından alınan kararların dahi hâkim onayına sunulması öngörülmüşken, yurtdışı kaynaklı web siteleriyle ilgili verilen kararlar için böyle bir zorunluluk getirilmemesi yerinde görülmemektedir[446].

Öte yandan, 5651 sayılı Kanun TİB tarafından verilen erişimin engellenmesi kararının konusunu oluşturan yayını yapanların kimliklerinin belirlenmesi halinde Cumhuriyet başsavcılığına suç duyurusunda bulunmasını öngörmektedir[447]. Kanun gerekçesinde, bu hükmün diğer kişilerin devletten suçluların cezalandırılmasını talep hakkı kapsamında suçu bildirme hak ve yetkisini, hatta görevini ortadan kaldırmadığı belirtilmiştir. Kimlik belirlemenin suç duyurusunda bulunanın üstüne düşen bir görev olmaması sebebiyle bu hüküm eleştirilmektedir[448]. Nihayetinde, suç duyuruları faili tespit edilsin edilmesin Cumhuriyet Savcılığına yapılmak zorundadır. Ayrıca, 5237 sayılı TCK'nın 278. maddesine göre işlenmekte olan bir suçu yetkili makamlara bildirmemesi zaten suç olarak kabul edilmiştir. Dolayısıyla, 5651 sayılı Kanundaki bu hüküm yeni bir düzenleme getirmiş olmamaktadır.

TİB bünyesinde 5651 sayılı Kanun'un 10. maddesinin 4. fıkrasında öngörülen esaslara göre bir ihbar merkezi kurmuştur. Bir suçun işlendiğine dair ihbarlar http://www.ihbarweb.org.tr adresli web sitesi üzerinden veya telefon veya cep telefonu mesajıyla İhbar Merkezi'ne iletilmesi mümkündür. Merkeze yapılan ihbarlar teknik ve hukuki incelemeye alındıktan sonra, yeterli şüphe bulunması durumunda diğer şartları varsa erişim engelleme yoluna gidilebilecektir[449]. Merkez kurulduğu günden bu yana

[445] Uygulama Yönetmeliği, m. 14 f. 1.

[446] *Dülger*, a.g.e., s. 1530.

[447] 5651 sayılı Kanun, m. 8 f. 6.

[448] *Akdeniz/Altıparmak*, a.g.e., s. 22.

[449] Uygulama Yönetmeliği, m. 16 f. 2.

81.691 ihbar yapılmış, 2.126 'sı re'sen ve 475'i de adli makamların kararıyla olmak üzere toplam 2.601 web sitesinin erişimi engellenmiştir[450].

2. Engelleme usulü

Adli makamlar tarafından erişim engelleme kararı verildiği zaman karar, kararı veren hâkim, mahkeme veya Cumhuriyet savcısı tarafından gereği yapılmak üzere TİB'e gönderilecektir[451]. Kararların doğrudan erişim sağlayıcılara gönderilmesi mümkün değildir[452]. Erişim engelleme kararı TİB tarafından erişim sağlayıcılara bildirilecektir. Uygulama Yönetmeliği, TİB'in erişim sağlayıcılara kararı elektronik ortamda bildirileceği esasını kabul etmiştir[453]. Bu şekilde hızlı bir şekilde içerik, yer veya erişim sağlayıcılara ulaşılarak kararın gereğinin yerine getirilmesi sağlanmaktadır.

Uygulama Yönetmeliği kararlarında belirtilmesi gerekli hususları 15. maddesinde belirlemiştir. Bu hükme göre, kararı veren merciinin adı, soruşturma veya mahkeme esas numarası, tedbirin hangi suç için istendiği ve yeterli şüphe sebeplerin neler olduğu, suça ilişkin bilgilerin bulunduğu URL ve alan adı, yer sağlayıcıya ait IP adresi ve alan adı veya IP adresi olarak erişim engelleme yönteminin kararda belirtilmesi gerekmektedir. Daha önce açıklandığı üzere, İnternet üzerinde farklı teknikler kullanarak bir web sitesinin erişiminin engellenmesi mümkündür[454]. 5651 sayılı Kanun belirli bir engelleme tekniğinin uygulanmasını zorunlu tutmamaktadır. Karar mercii, somut olayın özelliklerine göre hakkaniyete uygun ve etkili engelleme tekniğini kendisi belirleyebilecektir.

Aleyhinde erişim engelleme kararı uygulanan web sitesine erişilmeye çalışıldığında kullanıcılar "Bu siteye erişim engellenmiştir" mesajıyla karşılaşmaktadır. Bu mesajın altında, erişim engelleme kararını veren merci ve karar numarası hem Türkçe hem de İngilizce olarak yer almaktadır[455].

[450] Bkz. *İhbar İstatistikleri*, dn. 321.

[451] 5651 sayılı Kanun, m. 8 f. 3.

[452] Uygulama Yönetmeliği, m. 16 f. 1.

[453] Uygulama Yönetmeliği, m. 16 f. 3.

[454] Bkz. yuk. §3 V.

[455] Örneğin, http://www.youtube.com web sitesine erişilmeye çalışıldığında "Ankara 1.

5651 sayılı Kanun'un ilk dönemlerinde bu bilgiler erişim engelleme mesajında yer almamaktaydı. İçerik ve yer sağlayıcılar, kendi çabaları ile web sitesinin kimin tarafından engellendiğini araştırmakla uğraşmakta ve bu da hem zaman hem de bazı durumlarda hak kaybına yol açmaktaydı[456]. Engelleme kararını veren merci ve kararla ilgili bilgilerin engelleme mesajında yer alması işletilmesi gereken itiraz mekanizmalarını belirlemeye yardımcı olduğu için yerinde bir düzenlemedir. Uygulama bu şekliyle, Anayasanın 36. maddesinde herkesin meşru vasıta ve yollardan faydalanarak yargı mercileri önünde davacı veya davalı olarak iddia ve savunma yapması ile adil yargılanma hakkına sahip olduğu şeklinde düzenlenen hak arama hürriyetine hizmet etmektedir.

3. Engelleme kararının kaldırılması

Adli makamlar tarafından koruma tedbiri olarak verilen erişimin engellenmesine ilişkin kararlara 5271 sayılı CMK hükümlerine göre itiraz edilmesini mümkündür[457]. Ayrıca, kendisine yürütülmesi için gönderilen hâkim ve mahkeme kararlarına karşı TİB tarafından da itiraz edilebileceği kabul edilmiştir[458].

Uygulama Yönetmeliği, bu kararlara karşı TİB dışında 5271 sayılı CMK hükümlerine göre ilgililer tarafından da itiraz edilebileceğini öngörmektedir[459]. Ancak, ilgililerin kim olduğu yönünde bir açıklamada bulunmamaktadır. Bu doğrultuda, ilgili kişi kavramından menfaati etkilenen kişilerin anlaşılması gerektiği ve erişim engelleme kararına karşı

Sulh Ceza Mahkemesi, 05.05.2008 tarih ve 2008/402 nolu koruma tedbiri kapsamında bu internet sitesi (youtube.com) hakkında verdiği karar Telekomünikasyon İletişim Başkanlığı'nca uygulanmaktadır." ve "The decision no 2008/402 dated 05.05.2008, which is given about this web site (youtube.com) within the context of protection measure, of Ankara 1. Sulh Ceza Mahkemesi has been implemented by "Telekomünikasyon İletişim Başkanlığı"" mesajı ziyaretçilerin karşısına çıkmaktadır. Engelleme mesajının altında ayrıca TİB'e ait http://www.tib.gov.tr, http://www.guvenliweb.org.tr, http://www.ihbarweb.org.tr web sitelerinin bağlantısı yer almaktadır. Bkz. http://www.youtube.com.

[456] *Akdeniz/Altıparmak*, a.g.e., s. 67.

[457] 5651 sayılı Kanun, m. 8 f. 2.

[458] 5651 sayılı Kanun, m. 8 f. 13.

[459] 5651 sayılı Kanun, m. 10 f. 2.

bir web sitesinin kullanıcılarının dahi itiraz hakkına sahip olduğu ileri sürülmektedir[460].

5651 sayılı Kanun'da TİB tarafından re'sen alınan erişim engelleme kararlarına karşı nasıl itiraz edileceğine dair bir hüküm yer almamaktadır. Buna rağmen söz konusu işlemin idari işlem niteliğinde olması sebebiyle, işlemin iptali için 2577 sayılı İdari Yargılama Usulü Kanununda ("2577 s. İYUK")[461] öngörülen esaslara göre iptal davası açılması mümkündür.

4. Engellemenin sona erme halleri

Yapılan soruşturma sonucunda söz konusu suçun kavuşturulmasına yer olmadığına veya kovuşturma evresinde yapılan yargılama sonucunda beraat kararı verilmesi durumunda erişim engelleme kararı kendiliğinden hükümsüz hale gelecektir[462]. Bu durumda, engellemenin fiilen kaldırılması için kovuşturmaya yer olmadığı kararı Cumhuriyet savcısı tarafından, beraat kararı ise mahkemece gereğinin yapılması için TİB'e gönderilecektir. Ayrıca, erişim engelleme kararına konu olan içeriğin web sitesinden kaldırılması durumunda, soruşturma evresinde Cumhuriyet savcısı ve kovuşturma evresinde mahkeme tarafından engelleme kaldırılacaktır[463]. Öte yandan, TİB tarafından re'sen verilen erişim engellemesi kararı, hâkim tarafından onaylanmadığı takdirde hükümsüz hale gelecek ve engelleme TİB tarafından kaldırılacaktır[464].

5. Tazminat

Koruma tedbirleri, şüpheli veya sanığın hazır bulunmasını, delillerin karartılmaması ya da ileride verilecek hükmün yerine getirilmesini sağlamak gibi amaçlarla kesin hüküm olmadan temel hak ve hürriyetleri kısıtlanmaktadır[465]. 5651 sayılı Kanunda yer alan ve adli makamlar tara-

[460] 5651 Sayılı Kanun Çerçevesinde Erişim Engelleme Kararları – 5, http://turk.internet.com/haber/yaziyaz.php3?yaziid=20096.

[461] Kanun No: 2577, Kabul T.: 06.01.1982, RG 20.01.1982/17580.

[462] 5651 sayılı Kanun, m. 8 f. 7 ve f. 8.

[463] 5651 sayılı Kanun, m. 8 f. 9.

[464] Uygulama Yönetmeliği, m. 17 f. 3.

[465] Koruma tedbirleri hakkında daha fazla bilgi için bkz. *Kunter/Yenisey/Nuhoğlu*, a.g.e., s. 999.

fından verilen erişimin engellemesi kararları daha önce açıklandığı üzere koruma tedbiri niteliğindedir[466].

Koruma tedbirlerinin kötüye kullanıldığı durumlarda ortaya çıkan hak kayıplarının telafi edilmesi için 5271 sayılı CMK'nın 141. maddesi hangi hallerde tazminat istenebileceğini ayrıntılı olarak düzenlenmiştir. Ancak, bu koşullar arasında 5651 sayılı Kanun uyarınca uygulanan erişim engelleme kararları yer almamaktadır. Bu sebeple, 141. madde hükmü erişim engelleme kararları sebebiyle ortaya çıkan tazminat talepleri için uygulanamayacağı ileri sürülmektedir[467]. Engelleme kararları sebebiyle zarar uğrayanların karar aleyhine idare mahkemelerinde tam yargı davası açarak tazminat talep edebileceklerini görüşü ileri sürülmüşse de verilen karar bir idari bir karar olmadığı için bu talebin hukuki dayanağı bulunmamaktadır[468]. Öte yandan, TİB tarafından re'sen alınan erişim engelleme kararlarının idari işlem olması niteliği göz önüne alınarak, uğranılan zarar nedeniyle tam yargı davası ile tazminat istenebilmesi mümkündür.

İnternetin kullanım alanlarının artması olası bir erişim engelleme durumunda etkilenen temel hak ve hürriyetlerinin sayısı da aynı oranda artmaktadır. Web sitelerinin değerleri ziyaretçi sayılarına göre belirlenmektedir. Uzun süren yargılamalar boyunca erişimleri kapalı olan web siteler, davaların lehlerine sonuçlanması sonucunda tekrar yayına girdiklerinde eski kullanıcılarını toplayamamakta ve siteler değersiz hale gelmektedir. Web site sahipleri bu sebeple sitelerini kendileri kapatmak zorunda kalmaktadır. Haksız bir tedbir kararıyla tüm ziyaretçilerini kaybeden bir İnternet sitesi için etkili hukuk yolu oluşturulması gerekmektedir[469].

---

[466] Bkz. yuk. §6 IV A.

[467] *Akdeniz/Altıparmak*, a.g.e., s. 73.

[468] İlker Atamer, 5651 Sayılı Kanun Çerçevesinde Erişim Engelleme Kararları, http://turk.İnternet.com/haber/yazigoster.php3?yaziid=20078.

[469] *Akdeniz/Altıparmak*, a.g.e., s. 73.

D. Sorumluluk rejimi

1. İçerik sağlayıcılar

5651 sayılı Kanun içerik sağlayıcıyı İnternet ortamında kullanıcılara her türlü bilgi veya veriyi üreten, değiştiren ve sağlayan gerçek veya tüzel kişiler olarak tanımlamıştır[470]. Kanun içerik sağlayıcıları İnternet ortamında kullanıma sunduğu her türlü içerikten sorumlu olduğunu kabul etmiştir[471]. İçerik sağlayıcın bu doğrultuda "ürettiği, değiştirdiği veya sağladığı" her türlü içerikten dolayı hem cezai hem de hukuki sorumluluğu bulunmaktadır.

Bu hüküm "içerik sunma" fiilinden dolayı sorumluluğu öngördüğü için eleştirilmektedir[472]. Nihayetinde bu hüküm gereğince üretme ve değiştirme fiillerinde içerik sağlaya atfedilebilirliğin mümkün olduğu için sorumluluğun tabii olduğu, sunma fiilinde ise başkasına ait içerikten dolayı içerik sağlayıcının objektif olarak sorumlu tutulacağı sonucu doğduğu ileri sürülmektedir. Hükmün bu haliyle ceza sorumluluğunun şahsiliğini öngören ve kimsenin başkasının fiilinden dolayı sorumlu tutulmayacağını öngören 5237 sayılı TCK'nın 20. maddesine aykırılık oluşturduğu ve bir objektif sorumluluk hali oluşturduğu düşünülmektedir[473].

Objektif sorumluluk hallerinde kişiler icrai veya ihmali iradi hareketinin sonucu olan neticeden kusurları aranmaksızın, sırf nedensellik bağı dolayısıyla sorumlu tutulmaktadır[474]. 5237 sayılı TCK'da içerik sunma sebebiyle objektif sorumluluğu doğuracak herhangi bir hüküm yer almamaktadır. Bu tür bir sorumluluğu öngören 765 sayılı TCK'nın 162. maddesi 5237 sayılı Kanuna alınmamıştır. Söz konusu 162. madde, kanunun suç saydığı yayınların nakil etmeyi başlı başına bir suç kabul ederek, nakleden faillin aynı cezaya tabi olacağını öngörmekteydi. Aynı maddede, nakledilen yayının içeriğinin kabul edilmediğine, ihtiyatla

[470] 5651 sayılı Kanun, m. 2 f. 1(f).

[471] 5651 sayılı Kanun, m. 4.

[472] *Özel*, Türk Hukuk Sitesi.

[473] *Özel*, Türk Hukuk Sitesi.

[474] Timur Demirbaş, Ceza Hukuku Genel Hükümler, 3. Baskı, Ankara 2005 ("*Demirbaş*"), s. 358.

nakledildiğine veya sorumluluğun başkası tarafından üstlendiğine ilişkin çekincelerin kişiyi sorumluluktan kurtarmadığı kabul edilmekteydi.

Objektif sorumluluk hallerinin varlığı eleştirilmekte ve sadece belirli suçlar için kabul edilmektedir[475]. 5651 sayılı Kanunun gerekçesinde ve kanunla ilgili tüm müzakerelerde, bu kanunun yeni bilişim suçları getirmediği, kanunun Anayasanın 41. maddesinde yer alan ailenin ve 58. maddesinde yer alan gençliğin korunmasına amacıyla İnternete özgü tedbirler getirildiği ifade edilmiştir. Bu sebeple, objektif sorumluluğu doğuracak bir hükmün getirilmiş olması kanunun amaç ve kapsamıyla bağdaşmamaktadır.

Öte yandan 5651 sayılı Kanun bazı ülkelerdeki düzenlemelerin aksine, içerik sağlayıcının İnternette kullanıma sunduğu servisler bakımından bir ayrıma gitmemiştir[476]. Sorumluluğa ilişkin tek ayrım içerik sağlayıcının bağlantı sağladığı durumlar için öngörülmüştür. 5651 sayılı Kanun, içerik sağlayıcının bağlantı sağladığı başkasına ait içerikten belirli şartlar altında sorumlu olacağını kabul edilmiştir[477]. Sorumluluğun doğmasını belirleyen temel faktör bağlantılı içeriğin sunuluş biçimidir. Eğer ki, sunuş biçimi bağlantı sağlanan içeriğin benimsendiği veya kullanıcıların bu içeriğe ulaşmasını amaçladığı şeklinde açık şekilde belli oluyorsa, içerik sağlayıcı bu tür içerikten genel hükümlere göre sorumlu tutulacaktır. Kanunda genel hükümlerden neyin kastedildiği belirlenmemiştir. 5651 sayılı Kanunun gerekçesinde bağlantı sağlanılan içeriğin suç oluşturması halinde, bu içeriğe bağlantı sağlayan içerik sağlayıcısının, işlenen suça iştirakten dolayı sorumlu olacağı belirtilmiştir.

Ceza hukukumuzda iştirak asli ve fer'i iştirak olmak üzere ikiye ayrılmaktadır. Asli iştirak kendi içinde asli maddi ve asli manevi iştirak olarak ikiye ayrılmakta ve asli maddi iştirak 5237 sayılı TCK'nın 37. maddesinin 1. fıkrasında suçun kanuni tanımında yer alan fiilin birlikte gerçekleştirilmesi veya suçta başkasının araç olarak kullanılması olarak tanımlanmaktadır. Asli manevi iştirak ise aynı maddenin ikinci fıkrasında

---

[475] 5237 sayılı TCK'da yer alan objektif sorumluluk halleri için bkz. *Demirbaş*, a.g.e., s. 358.

[476] Bu konudaki en ayrıntılı düzenleme Singapur tarafından yapılmıştır. Bkz. yuk. §5 V.

[477] 5651 sayılı Kanun, m. 4 f. 2.

başkasını suç işlemeye azmettirmek şeklinde düzenlenmiştir. Fer'i iştirak ise 39. maddede suç işlenmesinde kullanılan araçları sağlamak, suçun işlenmesinden önce veya işlenmesi sırasında yardımda bulunarak icrasını kolaylaştırmak ve suç işlemeye teşvik etmek olarak tanımlanmıştır.

Bir suçun oluşması için yapılan hareketin kanunda öngörülen fiile uyması gerekmektedir. Tipiklik olarak adlandırılan ve temel bir ceza hukuku ilkesi olan suçta ve cezada kanunilik ilkesinin bir unsuru olan bu durum 5237 sayılı TCK'nın 2. maddesinde kanunun açıkça suç saymadığı bir fiil için kimseye ceza veya güvenlik tedbiri uygulanamayacağı şeklinde tanımlanmıştır. Her ne kadar 5651 sayılı Kanunun gerekçesinde bağlantı sağlayan içerik sağlayıcısının, işlenen suça iştirakten dolayı sorumlu olacağı belirtilmişse de, bu fiil yukarıda izah edilen asli ve fer'i hiçbir iştirak türünde öngörülen fillerle aynı nitelikte değildir[478]. Dolayısıyla, 5651 sayılı Kanunun 4. maddesinde öngörülen genel hükümlere göre sorumluluk ifadesi suça iştiraki yansıtmamaktadır. Suçta ve cezada kanunilik ilkesi gereğince bu sorumluluk halinin kanunda açıkça tanımlanması gerekmektedir. Bu hükme ilişkin herhangi bir içtihat da oluşmadığı için hükmün mahkemeler tarafından nasıl yorumlanacağı belirsizliğini korumaktadır.

Kanunun sorumluluk esasını yoruma açık bir şekilde tanımlaması sebebiyle, bir olayda bağlantı sağlanan içerikten dolayı sorumluluğun belirlenmesi için somut olayın özelliklerine göre değişecektir. Web 2.0 teknolojilerinin kullanıldığı web sitelerinde bu durum içinden çıkılamaz sorunlar oluşturabilecektir[479]. Daha önce açıklandığı üzere Web 2.0 teknolojileri içeriğin İnternet ortamında çok hızlı bir şekilde yayılmasını olanaklı kılmaktadır. Özellikle RSS abonelik sistemlerinin kullanılmasıyla içerik otomatik olarak web sitesinde yayınlanmakta ve web sitesi sahibinin müdahalesi olmaksızın otomatik olarak güncellenebilmekte-

---

[478] *Özel*, Türk Hukuk Sitesi.

[479] Benzer bir belirsizlik arama motorları için de geçerlidir. Arama motorlarında içerik sağlayıcılar web sitelerinin ilk sonuçlar arasında yer almasını sağlamak için ücret ödemektedirler. Benimseme hükmü geniş bir şekilde yorumlandığı takdirde Kanundaki belirsizlik sebebiyle arama motorlarının dahi sorumluluğuna gidilmesi gibi 5651 sayılı Kanunun amacını aşan bir durum ortaya çıkacaktır. Diğer örnekler için bkz. *Dülger*, a.g.e., s. 1486.

dir. Böylece bir içeriğin aynı anda binlerce web sitesinde yayınlanması mümkün olmaktadır.

Bu şekilde yayılan bir içeriğin suç oluşturması durumunda her bir web sitesinin ayrı ayrı değerlendirilmesi ve içerik sağlayıcının sunuş biçimi değerlendirilerek sorumluluğun tayin edilmesi gerekecektir. Web 2.0 teknolojilerinin yaygınlığı göz önüne alındığında, bazı durumlarda bir içerikten dolayı binlerce kişinin suça iştirak ettiği durumlar ortaya çıkabilecektir. Bu durumda eşitlik ilkesi gereğince ya tüm içerik sağlayıcıların sorumluluğuna gidilecek ya da suçta ve cezada şahsilik ilkesi gereğince sadece içeriği oluşturan veya bağlantının sahibi olan kişinin sorumluluğuna gidilmekle yetinecektir.

2. Yer sağlayıcılar

Yer sağlayıcılar 5651 sayılı Kanunda hizmet ve içerikleri barındıran sistemleri sağlayan veya işleten gerçek veya tüzel kişiler olarak tanımlanmıştır[480]. Türkiye'de yer sağlayıcı olarak faaliyette bulunmak için Faaliyet Yönetmeliğinde belirlenen esaslara göre faaliyette belgesinin alınması gerekmektedir. TİB, şu ana kadar itibariyle 481 yer sağlayıcıya faaliyet belgesi vermiştir[481].

5651 sayılı Kanun, yer sağlayıcıların, yer sağladıkları içeriği kontrol etmek veya hukuka aykırılığını denetleme konusunda yükümlü olmadıkları esasını getirmiştir[482]. Kanun gerekçesinde, bu düzenlemelerin Siber Suç Sözleşmesi ve Alman Tele Hizmetler Kanunu hükümleri göz önünde bulundurularak hazırlandığı belirtilmiştir. Düzenleme bu şekliyle Avrupa Birliği E-Ticaret Yönergesi'nin 15. maddesi ile de uyumlu niteliktedir[483]. Şüphesiz bu esasın benimsenmesinde yer sağlayıcıların yapmış olduğu işin teknik özellikleri belirleyici olmuştur[484]. Nihayetinde, yer sağlanan içeriğin takip edilmesi özellikle Web 2.0 teknolojilerinin kullanıldığı durumlarda

[480] 5651 sayılı Kanun, m. 2 f. 1(m).

[481] Faaliyet belgesine sahip yer sağlayıcıların listesi için bkz. http://www.tib.gov.tr/YS_listesi.html.

[482] 5651 sayılı Kanun, m. 5.

[483] *Akdeniz/Altıparmak*, a.g.e., s. 19; E-Ticaret Yönergesi için bkz. dn. 169.

[484] *Dülger*, a.g.e., s. 1486.

içeriğin çok hızlı bir şekilde değişmesi sebebiyle neredeyse mümkün olmamaktadır. Bu sebeple, yer sağlayıcının sorumluluğunun belirli koşullarda doğacağı kabul edilmiştir. Kanun 5. maddesinde ceza sorumluluğuna ilişkin hükümler saklı kalmak kaydıyla kendisine usule uygun bir şekilde ilgililer tarafından haberdar edildiği takdirde ve teknik olarak imkân bulduğu ölçüde yer sağlayıcının hukuka aykırı içeriği kaldırmakla yükümlü olduğunu belirtmiştir. Faaliyet Yönetmeliği, ilgililerin TİB, adli makamlar veya hakları ihlal edilen kişiler olduğunu açıklamıştır[485].

İlgililerin hukuka uygun bir şekilde kendine ilettiği erişim engelleme kararını teknik olarak imkânı olduğu halde yerine getiremeyen yer sağlayıcının cezai sorumluluğu doğacaktır. 5651 sayılı Kanun, erişim engelleme kararının yerine getirilmemiş olması durumunda fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde yer sağlayıcının altı aydan iki yıla kadar hapis cezası ile cezalandırılacağı kabul edilmiştir[486].

Tüm bunların yanı sıra, Kanun yer sağlayıcının sorumluluğuyla ilgili genel hükümlerin saklı olduğunu belirtmiştir. Kanun gerekçesinde saklı tutulan bu hallere ilişkin bir açıklama yapılmamaktadır. Yer sağlayıcının hukuka aykırı içeriğin yayınlanmasını bilinçli olarak sağlaması durumunda, yer sağlayıcının 5237 sayılı TCK'nın 38. maddesinde yer alan bir fer'i iştirak hali olan suçun işlenmesinden önce veya işlenmesi sırasında yardımda bulunarak icrasını kolaylaştırmak suçundan sorumlu tutulabilecektir. Bu hüküm dışında, işlenen suçun somut özellikleri göz önünde bulundurularak değerlendirilme yapılması gerekmektedir.

Yer sağlayıcılara getirilen bir diğer yükümlülük ise trafik bilgilerini saklamalarına ilişkindir. 5651 sayılı Kanunda yer sağlayıcıların trafik bilgilerini saklamalarına ilişkin bir hüküm yer almamasına rağmen, Faaliyet Yönetmeliği 16. maddesinde yer sağlayıcıların trafik bilgilerini altı ay saklamakla ve bu bilgilerin doğruluğunu, bütünlüğünü saklamak ve gizliliğini temin etmekle yükümlü tutulmuştur. Trafik bilgisi 5651 sayılı Kanunda İnternet ortamında gerçekleştirilen her türlü erişime ilişkin ola-

[485] Faaliyet Yönetmeliği, m. 3.

[486] 5651 sayılı Kanun, m. 8 f. 10.

rak taraflar, zaman, süre, yararlanılan hizmetin türü, aktarılan veri miktarı ve bağlantı noktaları gibi değerlerin bütünü olarak tanımlanmıştır[487].

3. Erişim sağlayıcılar

5651. sayılı Kanun, erişim sağlayıcıları kişilere İnternet ortamına erişim olanağı sağlayan gerçek veya tüzel kişiler olarak tanımlamaktadır[488]. Yer sağlayıcılar gibi erişim sağlayıcı olarak faaliyette bulunmak için Faaliyet Yönetmeliğinde belirlenen esaslara göre faaliyette belgesinin alınması gerekmektedir. TİB, şu ana kadar 95 erişim sağlayıcıya faaliyet belgesi vermiştir[489].

Erişim sağlayıcılar verinin içeriğine müdahale etmeksizin verinin kullanıcıdan İnternet trafiğine taşınması için bir aracı olarak hareket etmektedirler. Salt aracı olarak hareket ettikleri için sorumluluklarının da hafif olması işin niteliğine uygun düşecektir[490]. Bu alandaki Siber Suç Sözleşmesi ve Alman Tele Hizmetler Kanunu gibi düzenlemeleri göz önünde bulunduran 5651 sayılı Kanun 6. maddesinde erişim sağlayıcının kendi aracılığıyla erişilen bilgilerin içeriklerinin hukuka aykırılığını kontrol etmekle yükümlü olmadığı esasını benimsemiştir. Bu düzenleme yer sağlayıcılar gibi erişim sağlayıcıları da kapsayan Avrupa Birliği E-Ticaret Yönergesi'nin 15. maddesi ile de uyumlu niteliktedir[491].

5651 sayılı Kanun erişim sağlayıcıların sorumluluğunu yer sağlayıcılarla aynı esaslara göre düzenlemiştir. Kanun, tıpkı yer sağlayıcılar gibi erişim sağlayıcıların kendilerine usule uygun bir şekilde ilgililer tarafından haberdar edildiği takdirde ve teknik olarak imkân bulduğu

[487] 5651 sayılı Kanun, m. 2 f. 1(j).

[488] 5651 sayılı Kanun, m. 2 f. 1(e).

[489] Faaliyet belgesine sahip erişim sağlayıcıların listesi için bkz. http://www.tib.gov.tr/ES_listesi.html.

[490] Erişim sağlayıcıların sorumluluğu telefon şirketlerinin sorumluluğuna benzetilmektedir. Nasıl ki telefon şirketleri hatları kullanılarak işlenen suçlardan dolayı sorumlu tutulmuyorlarsa, İSS'lerin de sorumlu tutulmaması gerektiği kabul edilmektedir. Sorumlu tutulacaklar ise de, verinin içeriğine müdahale etmeksizin bir aracı olarak hareket ettikleri için sorumluluklarının da hafif olması gerektiği belirtilmektedir. Bkz. *Campbell/Machet*, a.g.e., s. 142.

[491] *Akdeniz/Altıparmak*, a.g.e., s. 19.

ölçüde erişim sağlayıcının hukuka aykırı içeriğe erişimi engellemekle yükümlü olduklarını öngörmüştür[492]. Bu yükümlülük yerine getirilmemesi durumunda ise adli makamlar tarafından verilen erişim engelleme kararlarının yerine getirilmemesi halinde fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde erişim sağlayıcının altı aydan iki yıla kadar hapis cezası ile cezalandırılacağı;[493] idari tedbir olarak verilmiş engelleme kararlarının yerine getirilmemesi durumunda ise de erişim sağlayıcıya onbin Türk Lirasından yüzbin Türk Lirasına kadar idari para cezası verileceğikabul edilmiştir[494]. Ayrıca, idari para cezasının verildiği andan itibaren yirmi dört saat içerisinde kararın yerine getirilmemesi halinde Başkanlığın talebi üzerine Kurum tarafından erişim sağlayıcının yetkilendirmenin iptaline karar verilebilecektir[495].

Erişim sağlayıcılara ilişkin bir diğer yükümlülük ise trafik bilgilerine ilişkindir. Erişim sağlayıcılar sağladıkları hizmete ilişkin tüm trafik bilgilerini bir yıl saklamakla ve bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini sağlamakla yükümlü tutulmuştur[496]. Ayrıca, faaliyetlerine son vermeden en az üç ay önce durumu Kuruma, içerik sağlayıcılarına ve müşterilerine bildirmekle bu tutmuş olduğu trafik bilgilerini Kuruma teslim etmekle yükümlü tutulmuştur. Erişim sağlayıcılar bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini sağlamakla ve bu bilgilerin başkaları tarafından elde edilmesini engellemekle yükümlü tutulmuştur. Bu yükümlülüklerin ihlali durumunda TİB tarafından onbin Türk Lirasından ellibin Türk Lirasına kadar idari para cezası verileceği öngörülmüştür[497].

---

[492] 5651 sayılı Kanun, m. 6.

[493] 5651 sayılı Kanun, m. 8 f. 10.

[494] 5651 sayılı Kanun, m. 8 f. 11.

[495] Adli makamlar tarafından verilen erişim engelleme kararlarının yerine getirilmemesinde yetkilendirmenin iptali şeklinde bir yaptırım olmamasına rağmen, TİB tarafından verilen erişim engelleme kararlarında böyle bir yaptırımın öngörülmesinin makul bir gerekçesi bulunmamaktadır. Bkz. *Dülger*, a.g.e., s. 1532.

[496] 5651 sayılı Kanunun 6. maddesinde bu süre alt aydan az veya iki yıldan fazla olmamak üzere yönetmelikle belirleneceği öngörülmüş ve Faaliyet Yönetmeliği 15. maddesinde bu süreyi 1 yıl olarak belirlemiştir.

[497] 5651 sayılı Kanun, m. 6 f. 3.

4. İnternet toplu kullanım sağlayıcıları

5651 sayılı Kanun, İnternet toplu kullanım sağlayıcıları belli bir yerde ve belli bir sürede İnternet kullanım olanağı sağlayanlar olarak tanımlamıştır[498]. Kanun İnternet toplu kullanım sağlayıcıları için ticari amaçla hareket edip etmemelerine göre farklı sorumluluklar öngörmüştür.

Ticari amaçlı İnternet toplu kullanım sağlayıcılar İnternet kafeler olarak da anılmaktadır. Ticari amaçlı İnternet toplu kullanım sağlayıcılar faaliyete başlayabilmek için yer ve erişim sağlayıcılar gibi izin belgesi almakla yükümlü tutulmuşlardır[499]. Ancak, yer ver erişim sağlayıcılardan farklı olarak, izin belgeleri Kurum tarafından değil bulundukları mahalli mülki amirden alınması ve aynı makam tarafından denetlenmeleri öngörülmüştür.

Toplu kullanım sağlayıcılarının en temel yükümlülükleri suç oluşturan içerikler için erişimi önleyici tedbirlerle almaktır. Bu yükümlülük bakımından toplu kullanım sağlayıcısının faaliyetlerini ticari amaçla sürdürmesinin bir önemi bulunmamaktadır[500]. Kanun gerekçesinde de belirtildiği üzere, Avrupa Konseyi 1999/246 ve 2005/854 sayılı Kararları ile üye ülkeleri İnternetin güvenli kullanılmasının sağlanması için filtreleme ve bloke etme programları geliştirmeye ve aynı amaçla eğitim ve tanıtım faaliyetlerini yaygınlaştırmaya davet etmektedir. İnternet kafeler gibi toplu kullanım sağlayıcılar çocuklar dâhil toplumun her kesimi tarafından İnternete erişim için yoğun olarak kullanılmaktadır. Bu sebeple, bu yerler nezdinde alınacak önleyici tedbirler İnternet ortamında suçla mücadele alanında önemli bir yer tutmaktadır.

Toplu Kullanım Yönetmeliği'nde toplu kullanım sağlayıcıların uymaları gereken usul ve esaslar ayrıntılı bir şekilde düzenlenmiştir[501]. Yönetmelik, erişim sağlayıcılar gibi İnternet toplu kullanım sağlayıcıları

---

[498] 5651 sayılı Kanun, m. 2 f. 1(i).

[499] 5651 sayılı Kanun, m. 7.

[500] Toplu Kullanım Yönetmeliği, m. 7.

[501] 5651 sayılı Kanun yürürlüğe girmeden önce İnternet kafelerin uymaları gereken usul ve esaslar İçişleri Bakanlığının yayınlamış olduğu "İnternet Kafeleri Genelgesi" ile belirlenmekteydi.

da trafik bilgilerini 1 yıl saklamakla ve bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini sağlamakla yükümlü tutulmuşlardır[502]. Ancak Yönetmelikte bu yükümlülüğe aykırı davranılmasının yaptırımı yer almamaktadır.

5. Ortak hükümler

5651 sayılı Kanun içerik, yer ve erişim sağlayıcıların Uygulama Yönetmeliği'nde belirlenen esaslar çerçevesinde tanıtıcı bilgilerini İnternet ortamında kullanıcılara erişilebilir ve güncel bir şekilde bulundurmakla yükümlü tutmuştur. Bu yükümlülüğe aykırı davranan içerik, yer ve erişim sağlayıcılara ikibin Türk Lirasından on bin Türk Lirasına kadar idari para cezası verileceği öngörülmüştür. Uygulama Yönetmeliği, bu yükümlülüğü sadece ticari veya ekonomik amaçlı içerik, yer ve erişim sağlayıcılar ile sınırlandırmış ve tanıtıcı bilgilerin neler olduğunu gerçek ve tüzel kişiler için ayrıntılı olarak açıklamıştır[503]. 5651 sayılı Kanunun getirmiş olduğu bu düzenleme basılmış eserlerde bulunması gereken zorunlu unsurları düzenleyen 5187 sayılı Basın Kanununun 4. maddesinden esinlenilmiştir[504]. Bu düzenlemeyle İnternet ortamında işlenen suçlara ilişkin faillerin tespit edilmesi amaçlanmaktadır.

E. Yayından çıkarma ve cevap hakkı

5651 sayılı Kanun, idari ve cezai hükümlerin yanı sıra, özel hukuka ilişkin hükümler de içermesi sebebiyle *sui generis* bir nitelik taşımaktadır. Kanuna bu niteliği sağlayan hükümlerin başında 9. maddede yer alan yayından çıkarma ve cevap hakkıyla ilgili düzenleme gelmektedir.

5651 sayılı Kanun 9. maddesi, İnternette yayınlanan içerik sebebiyle hakları ihlal edilen kişilere içeriğin yayından çıkarılması ve cevaplarını aynı yerde yayımlama hakkı tanımaktadır. 9. maddeye göre, hakları ihlal edilen kişiler, içerik sağlayıcısına; ona ulaşılamadığı takdirde yer sağlayıcısına başvurarak içeriğin yayından çıkarılmasını ve hazırladığı cevabı bir hafta sü-

[502] Toplu Kullanım Yönetmeliği, m.5 f. 1(e).

[503] Uygulama Yönetmeliği, m. 5.

[504] *Dülger*, a.g.e., s. 1483.

reyle İnternet ortamında yayımlanmasını sağlayabileceklerdir. Bu talebin, içerik veya yer sağlayıcısına ulaşmasından itibaren iki gün içerisinde yerine getirilmesi gerekmektedir. İki günlük sürenin geçmesine rağmen talebin yerine getirilmemesi talebin reddedildiği manasına gelmektedir.

Talebin reddedilmiş sayılması halinde, içeriğin yayından çıkarılmasını ve cevap yazısının yayınlanmasını sağlamanın tek yolu sulh ceza mahkemesine başvurmaktadır. Talebin reddedilmiş sayıldığı günden itibaren 15 gün içerisinde hakkı ihlal edilen kişi, yerleşim yerindeki sulh ceza mahkemesine başvurarak yayından kaldırma ve cevap hakkının yayınlanması yönünde karar verilmesi istemesi gerekmektedir. Kanun, sulh ceza hâkiminin duruşma yapmaksızın üç gün içinde kararını vereceğini öngörmektedir. Yargısal sürecin tüm aşamalarıyla tamamlanmasıyla İnternet içeriğine hâkimin kararıyla müdahale edilecektir.

5651 sayılı Kanun'un 9. maddesi Adalet Komisyonu'nda eklenmiştir. Komisyonda, 5187 sayılı Basın Kanununun cevap ve düzeltme hakkının kullanılmasına ilişkin hükümleri göz önünde bulundurularak, İnternet ortamında yapılan yayınlarla kişilik haklarına saldırıda bulunan kişilerin bu nitelikteki içeriğin yayından çıkarılması ve buna karşı cevap hakkını ne şekilde kullanabileceğine ilişkin açıklık sağlamak amacıyla bu hükmün getirildiği belirtilmiştir. Bu hüküm, İnternetteki bazı faaliyetlerin basın faaliyeti olarak nitelendirilmesini mümkün olsa da İnternetin sadece basın faaliyeti gibi algılanması ve İnternetin kendine özgü yapısı göz önüne alınmadan 5187 sayılı Basın Kanunu hükümlerinin 5651 sayılı Kanuna alınması sebebiyle eleştirilmiştir.

Öte yandan 5651 sayılı Kanundaki düzenleme 5187 sayılı Basın Kanunundaki düzenlemeden çeşitli yönlerden ayrılmaktadır. 5187 sayılı Basın Kanununu cevap ve düzeltme hakkını "kişilerin şeref ve haysiyetini ihlal edici veya kişilerle ilgili gerçeğe aykırı yayım yapılması" durumunda bu hakkın kullanılabileceğini öngörmüştür[505]. Kaldı ki, Anayasanın 32. maddesi de düzeltme ve cevap hakkını ancak kişilerin haysiyet ve şereflerine dokunulması veya kendileriyle ilgili gerçeğe aykırı yayınlar yapılması hallerinde tanınacağını öngörmüştür. Oysa 5651 sayılı Kanunun 9.

[505] 5187 sayılı Basın Kanunu, m. 14.

maddesinde "içerik nedeniyle hakları ihlal edildiğini iddia eden kişilere" bu hakkı tanımış ancak ihlal edilen hakkın niteliği hakkında herhangi bir atıfta bulunmamıştır[506]. Düzenleme bu sebeple uygulama alanını belirsiz bir hale getirmiş bulunmaktadır.

5187 sayılı Basın Kanunundan ayrılan bir diğer nokta ise öngörülen sorumluluk rejiminde yer almaktadır. 5651 sayılı Kanun, sulh ceza hâkiminin kararını gereğince ve süresinde yerine getirmeyen sorumlu kişinin, altı aydan iki yıla kadar hapis cezası ile cezalandırılacağını öngörmektedir[507]. 5187 sayılı Basın Kanunu ise düzeltme ve cevap yazısının mahkeme kararına rağmen yayınlanmaması durumunda, sorumlu kişilerin ağır para cezasıyla cezalandırılacağını öngörmektedir[508]. 5651 sayılı Kanunun 9. maddesi basın yayın faaliyeti yapmayan kişilerin, sahibi oldukları İnternet siteleri nedeniyle basın yayın kuruluşlarını ilgilendiren bir sorumluluğa tabi tutulmaları sebebiyle eleştirilmiştir[509]. Bu sorumluluğun ayrıca cezai olarak artırılmasının objektif bir gerekçesi bulunmamakta ve ne Kanun gerekçesinde ne de Adalet Komisyonu raporunda neden böyle hareket edildiğine dair bir açıklama yer almamaktadır. Bu düzenlemede eleştirilen son husus ise, sorumlu kişinin kim olduğuna ilişkin bir tanım vermemesidir[510]. Benzer bir şekilde, bilgilendirme yükümlülüğüne ilişkin getirilen düzenlemede sorumlu kişiye ilişkin bir atıf yer almamaktadır.

Öte yandan yayından çıkarma ve cevap hakkına ilişkin düzenleme içerik ve yer sağlayıcıyı odak noktası alarak hareket ettiği için yerinde görülmemektedir[511]. Düzenleme bu haliyle yurtdışındaki içerik veya yer sağlayıcıları yaptırıma bağlamak mümkün olmadığı için uygulama alanı yurtiçindeki içerik veya yer sağlayıcılarla sınırlı olacaktır.

Yayından çıkarma ve cevap hakkına ilişkin hükümle ilgili bir diğer tartışma konusu bu hükme dayanılarak erişim engelleme kararı verilip verilemeyeceğine ilişkindir. 5651 sayılı Kanun hakaret suçunu veya Medeni

[506] *Özel*, Türk Hukuk Sitesi.

[507] 5651 sayılı Kanun, m. 9 f. 4.

[508] 5187 sayılı Basın Kanunu, m. 18.

[509] *Özel*, Türk Hukuk Sitesi.

[510] *Dülger*, a.g.e., s. 1534.

[511] *Dülger*, a.g.e., s. 1533.

Kanunda yer alan kişilik haklarının ihlalini bir erişim engelleme sebebi olarak kabul etmemiştir. Ayrıca, bu ihlallere ilişkin erişim engelleme kararı verilebileceğini öngören özel bir düzenleme de bulunmamaktadır. Benzer bir şekilde 5651 sayılı Kanun'un 9. maddesinde erişim engellenmesine ilişkin herhangi bir atıf bulunmamaktadır. 9. madde, sadece özel hukuku ilgilendiren kişisel ilişkilerde daha sınırlı ve erişim engelleme içermeyen bir yaptırım getirmiştir[512]. Bu sebeple, kişilik haklarının ihlal edilmesi durumunda erişim engelleme yoluna gidilmesi mümkün değildir.

Uygulamada özellikle Medeni Kanun'da yer alan kişiliğin korunması hükümlerine dayanarak hukuk mahkemelerinden web siteleri için erişim engelleme kararları alındığı gözlemlenmektedir[513]. 5651 sayılı Kanun'un Medeni Kanuna göre hem yeni tarihli hem de özel kanun olması sebebiyle, hukuk mahkemelerinden kişilik haklarının ihlali sebebiyle erişim engellemesi koruma tedbirinin alınması mümkün değildir.

9. madde hükmüne benzer bir hüküm TİB için Uygulama Yönetmeliği'nde öngörülmüştür. Uygulama Yönetmeliği'nin 16. maddesinin 6. fıkrası Başkanlığa erisimin engellenmesi kararlarına konu olan içeriğin yayından kaldırılmasını yer sağlayıcıdan isteyebilmesi için yetki vermiştir. TİB, uyar-kaldır olarak adlandırılan bu yöntem sayesinde 514 adet içeriğin veya bölümün kaldırılmasını sağlamıştır[514]. Hükmün bu şekilde kullanılması yerinde bir girişimdir. Erişim engellemenin nihai amacı hukuka aykırı içeriğin web sitesinden kaldırılmasıdır. Uyar-kaldır yönteminin kullanılması sayesinde, web sitelerinin doğrudan engellenmelerinin sakıncaları ortadan kalkmaktadır.

V. 5651 sayılı Kanunun değerlendirilmesi

A. Sınırlama rejimi açısından değerlendirme

Anayasa, temel hak ve hürriyetlerin sınırlanması için 13. maddesinde genel bir sınırlama rejimi öngörmüştür. Bu genel sınırlama rejimi dışında

[512] *Akdeniz/Altıparmak*, a.g.e., s. 55.

[513] Örneğin, http://www.wordpress.com ve http://groups.google.com siteleri bu şekilde engellenmiştir. Daha fazla bilgi için bkz. *Akdeniz/Altıparmak*, s. 56.

[514] Bkz. *İhbar İstatistikleri*, dn. 321.

ayrıca her temel hak ve hürriyet için kendi maddesi altında özel sınırlama sebepleri öngörmüştür.

Anayasanın 13. maddesine göre, temel hak ve hürriyetler özlerine dokunulmaksızın yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabilir. Yapılan tüm sınırlamaların Anayasanın sözüne ve ruhuna, demokratik toplum düzeninin ve laik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olmaması gerekmektedir. Anayasanın bu maddesindeki sınırlamalar dışında her bir temel hak ve hürriyet Anayasada yer alan maddesindeki özel sınırlama rejimine tabidir. Bu özel sınırlamalar, hakkın bizzat kendi tanımında yer almakta ve onun anayasal sınırlarını oluşturmaktadır[515]. Diğer bir deyişle, anayasa o hakkı sadece o sınırlar içinde tanımaktadır.

1. Kanunla sınırlama

Temel hak ve hürriyetlere ilişkin sınırlamalar ancak kanunla yapılması gerekmektedir. Bu doğrultuda, erişim engellemesi yoluyla ifade ve iletişim hürriyeti gibi çeşitli hakların sınırlamasının 5651 sayılı Kanunla gerçekleştirilmesi sebebiyle kanunla sınırlama ilkesine uyulmuştur. Öte yandan, 5651 sayılı Kanun'un 8. maddesinde öngörülen erişim engelleme sebeplerinin her birinin 5237 sayılı TCK ve 5816 sayılı Kanun gibi kanunlarda düzenleniyor olması, kanunla sınırlama ilkesine uygunluk açısından yerinde bir düzenlemedir. Tüm bunların yanı sıra, 5651 sayılı Kanunun erişim engelleme sebeplerini sınırlı sayı ilkesine göre ve somut suçlar için belirlemiş olması mukayeseli hukuktaki örnekler göz önüne alındığında demokratik bir yaklaşımdır. Nihayetinde, bazı devletler İnternet içeriğine müdahale için ulusal güvenlik, kamu yararı gibi muğlâk sebepleri belirlemek suretiyle müdahalenin kapsamını genişletmiş ve keyfi uygulamalara yol açmıştır. 5651 sayılı Kanunda ise böyle genel erişim engelleme sebepleri yer almamaktadır.

2. Anayasanın sözüne ve ruhuna uygunluk

Temel hak ve hürriyetlere ilişkin sınırlamaların Anayasanın sözüne ve ruhuna uygun olması gerekmektedir. Bu gereklilik, Anayasanın temel

[515] Ergun Özbudun, Türk Anayasa Hukuku, 8. Baskı, Ankara 2005 ("*Özbudun*"), s. 102.

hak ve hürriyetler için "ek güvenceler" tanıdığı durumlarda önem taşımaktadır[516]. Anayasa bir temel hak ve hürriyete ilişkin kendi maddesi altında kanun koyucunun sınırlama yaparken yapamayacaklarını saymışsa, kanun koyucunun bu yasaklamalara aykırı düzenleme yapması Anayasanın sözüne ve ruhuna aykırılık oluşturacaktır.

İnternetin klasik bir iletişim aracı olarak görülmemesi gerekmektedir. İnternet kullanım olanları çok hızlı bir şekilde artmıştır. Kullanım alanlarının artması olası bir erişim engelleme kararı ile etkilenecek hakların sayısını da artırmıştır. Somut olayda engellenen web sitesinin özelliklerine göre bu hakların ayrı ayrı tespit edilmesi ve bu hakların teknolojik gelişmelere uygun bir şekilde yorumlanması gerekmektedir. Örneğin, elektronik ticaret hizmeti sunan bir web sitesi engellendiğinde iletişim ve ifade hürriyeti dışında web sitesi sahibinin mülkiyet hakkı da etkilenmiş olacaktır. Benzer bir şekilde bir sosyal ağ sitesi veya bir forum engellendiğinde iletişim ve ifade hürriyetleri dışında bireylerin toplantı hak ve hürriyeti de etkilenecektir.

Erişim engelleme kararlarının, bu şekilde çoklu sınırlamalara sebep olması sebebiyle, erişim engellemeye son çare olarak başvurulması gerekmektedir. Diğer bir deyişle, erişim engelleme kararı verilirken etkilenmesi muhtemel tüm temel hak ve hürriyetlere ilişkin ek güvencelerin göz önünde bulundurulması gerekmektedir. Aşağıda açıklanacağı üzere, ölçülülük, hakkın özü ve demokratik toplum düzeninin gerekleri gibi ilkeler de bu tür bir yaklaşımı zorunlu kılmaktadır.

3. Ölçülülük ilkesi

Ölçülülük ilkesinin tanımı Anayasada yer almamaktadır. Doktrinde ölçülülük sınırlamada başvurulan aracın sınırlama amacını gerçekleştirmeye elverişli olmasını; bu aracın sınırlama amacı açısından gerekli olmasını ve araçla amacın ölçüsüz bir oran içinde bulunmaması şeklinde tanımlanmaktadır[517]. Anayasa Mahkemesi bu ilkeyi bir kararında "(…)Yapılan sınırlamayla sağladığı yarar arasında hakkaniyete uygun bir dengenin

[516] *Özbudun*, a.g.e., s. 103.

[517] *Özbudun*, a.g.e., s. 104.

bulunması gerekir" şeklinde özetlemiştir[518]. Bu doğrultuda ölçülülüğün tespitinde getirilen düzenlemenin varılmak istenen amaca elverişliliğinin, zorunluluğunun ve orantılılığının tespit edilmesi gerekmektedir.

Kanun gerekçesinde açıklandığı üzere 5651 sayılı Kanunun temel amacı aileyi, çocukları ve gençleri İnternet dâhil elektronik iletişim araçlarının kötüye kullanılmasıyla uyuşturucu ve uyarıcı madde alışkanlığı, intihara yönlendirme, cinsel istismar, kumar ve benzeri kötü alışkanlıkları teşvik eden içerikten korumak amacıyla hazırlanmıştır. Bu amaca ulaşmak için 5651 sayılı Kanunun öngördüğü araç erişim engellemedir. Öncelikle bu aracın Kanunun öngördüğü amaca ulaşmak için elverişli, zorunlu ve orantılı olup olmadığının tespit edilmesi gerekmektedir. Bu tespit yapılırken TİB tarafından verilen idari erişim engelleme kararları ile mahkemeler tarafından verilen adli erişim engelleme kararlarının ayrı ayrı değerlendirilmesi gerekmektedir.

Üçüncü bölümde açıklandığı üzere, bir web sitesinin erişiminin farklı yöntem ve teknikler kullanılarak engellenmesi mümkündür. Erişim engelleme yöntem ve teknikleri ne kadar hızlı gelişiyorsa, bu yöntem ve teknikleri aşmak için kullanılan teknolojiler de aynı oranda gelişmektedir[519]. Örneğin, Youtube web sitesi 5651 sayılı Kanun kapsamında engellenmesine rağmen hâlâ Türkiye'de en çok ziyaret edilen web siteleri arasında kalmaya devam etmektedir. Bu sebeple, erişim engelleme yöntemi İnternet içeriğinin kontrol edilmesi açısından elverişli bir yöntem olarak kabul edilmemektedir[520].

---

[518] Anayasa Mahkemesi, K.T.: 22.05.1987, E: 1986/17, K: 1987/11, AMKD, Sayı: 23, s. 222; Karar metni için bkz. http://www.anayasa.gov.tr/eskisite/kararlar/iptalitiraz/K1987/K1987-11.htm; Bkz. *Özbudun*, a.g.e., s. 105.

[519] 5651 sayılı Kanunun sansüre yol açabileceğine yönelik gösterilen en temel örnek engelleme ve bunları aşma teknolojilerinin hızla artmasıdır. Bu doğrultuda 5651 sayılı Kanunun bir sansür yasası olmamakla birlikte aşma teknikleri gelişmesi sebebiyle engelleme seviyesinin artırılmak zorunda kalmasının belirli bir noktadan sonra sansüre yol açabileceği ileri sürülmektedir. Bkz. Genel Kurul Tutanağı, s. 76.

[520] *Akdeniz/Altıparmak*, a.g.e., s. 57; İnternet nükleer bir savaş sırasında bile veri iletişiminin gerçekleştirilmesi temel amacıyla hazırlanmıştır. Bu sebeple, nükleer bir savaşta bile çalışabilecek bir teknolojinin klasik, standart birtakım yayın araçlarını denetleme mekanizmalarıyla kontrol altına alınmasının yetersiz kalacağı düşünülmektedir. Bkz. Genel Kurul Tutanağı, s. 76.

5651 sayılı Kanun'daki erişim engelleme kararları ne bir ceza ne de bir idari yaptırım niteliğindedir. Daha önce açıklandığı üzere bu kararlar tedbir niteliğindedir[521]. Bir temel hak ve hürriyetlere geçici de olsa adli makamlar tarafından sınırlama getirilmesi hukuk devleti ilkesinin temellerindedir. Adli makamların sınırlama getirmesi asıl, idari makamların ise istisnadır. İdari makamlara belirli koşullar altında ve özellikle ivedi davranılması gerektiği durumlarda bu hak tanınmaktadır. Dolayısıyla, TİB'in kendisine verilen re'sen erişim engelleme kararı verme konusundaki takdir yetkisini amacına uygun bir şekilde kullanmalıdır. Erişim engelleme kararının amacı sakıncalı içeriğin İnternet ortamından kaldırılması olduğu için TİB'in bu amaca ulaşmak için gerekli olan başka yollar varsa öncelikle bunlara başvurulması gerekmektedir[522]. Örneğin, uyarı mekanizmalarını işletilerek içeriğin İnternet ortamından kaldırılmasını sağlaması bir çözümdür. Bu yöntem tercih edilirse içerik ve yer sağlayıcılarla doğrudan müzakere olanağı doğduğundan, içerik ve yer sağlayıcıların savunma haklarını da etkin bir şekilde kullanmaları mümkün olacaktır. Mahkemeler tarafından ise erişim engelleme kararı verilmek yerine, somut olayın özelliklerine göre içeriğin kaldırılması kararı verilmesi, içerik kararda öngörülen süre ve şartlarda kaldırılmadığı takdirde erişim engelleme yoluna gidilmesi gerekmektedir[523]. Aksi halde ölçülülük ilkesinin bir unsuru olan zorunluluk şartı yerine getirilmemiş olacaktır.

Orantılılık unsuruna uymak için ise hem TİB hem de adli makamlar tarafından erişim engelleme kararı verildiği zaman en etkili tekniğin belirlenmesi gerekmektedir. 5651 sayılı Kanun erişim engellemesi için zorunlu bir engelleme tekniği öngörmemektedir. Bir web sitesinin IP, DNS, URL ve içerik engellemesi gibi birçok teknik kullanılarak bir içeriğe erişim engellenmesi mümkündür. Bir içeriğin URL engellemesi tekniğiyle engellenmesi çözüm olacaksa, bununla yetinilmeli DNS engelleme tekniğiyle tüm web sitesinin erişimini engelleme yoluna gidilmemelidir[524]. Benzer bir şekilde bir web sitesindeki içerik sebebiyle sitenin alt alan adına erişim engelleme içeriği engellemek için yeterliyken tüm web sitesi engellenmemelidir. Bu

[521] Bkz. yuk. §6 IV A.

[522] *Akdeniz/Altıparmak*, a.g.e., s. 60.

[523] *Akdeniz/Altıparmak*, a.g.e., s. 61.

[524] *Akdeniz/Altıparmak*, a.g.e., s. 61.

son durumun özellikle blog hizmetlerinin ve Web 2.0 teknolojilerinin artmasıyla önemi artmış durumdadır. Bir blogda yer alan bir içerik sebebiyle tüm blogların erişimin engellenmesi ölçülülük ilkesi dışında ceza sorumluluğunun şahsiliği ilkesiyle de bağdaşmamaktadır.

4. Hakkın özü

Temel hak ve hürriyetlere ilişkin yapılacak sınırlamalarda uyulması gereken bir diğer esas ise hakkın özüne dokunmamaktır. Temel hak ve hürriyetlerin özünün ne olduğunun ve içeriğinin ne olduğunun bütün temek hak ve hürriyetler için genel olarak tanımlamak mümkün olmadığı, her temel hak ve hürriyet için ayrı ayrı tanımlanması gerektiği kabul edilmektedir[525]. Hakkının özü genel olarak bir hakkın vazgeçilmez unsuru, dokunulduğu takdirde söz konusu hürriyeti anlamsız kılacak asli çekirdeği olarak tanımlanmaktadır[526]. Anayasa Mahkemesi "bir hak ve hürriyetin gayesine uygun şekilde kullanılmasını son derece zorlaştıran veya onu kullanamaz duruma düşüren kayıtlara tabi tutulması halinde" sınırlamanın o temel hak ve hürriyetin özüne dokunduğu kabul etmektedir[527].

Hakkın özüne ilişkin bu esaslar göz önüne alındığında, İnternet içeriğine müdahale eden bir düzenlemenin bireyleri hareketsizliğe itmemesi, aksine İnternetin kullanımını teşvik etmesi gerekmektedir. Hakkın özü özellikle İnternet içeriğine sosyal teknikler kullanarak müdahale edildiğinde önem taşımaktadır. Üçüncü bölümde açıklandığı üzere, bazı sebeplerden dolayı doğrudan engelleme kararı almak yerine, başkaca yöntemler kullanmak suretiyle sitelere erişimi fiilen zorlaştırmakta veya kullanıcıların oto-sansür uygulamalarını sağlamaktadır. Örneğin, İnternet ortamında yapılan tüm işlemlerin takip edilmesi veya fiilen bu takip yapılmasa bile bu şekilde bir takibin yapıldığı izlenimi verilmesi veya İnternete bağlanmak için vatandaşlık bilgileri gibi bazı bilgilerin girilmesinin istenmesi yaygın kullanılan sosyal tekniklerdir. Takip edil-

---

[525] *Özbudun*, a.g.e., s. 105.

[526] *Özbudun*, a.g.e., s. 105.

[527] Anayasa Mahkemesi, K.T.: 08.04.1963, E: 1963/25, K: 1963/87, AMKD, Sayı: 1, s. 228; Karar metni için bkz. http://www.anayasa.gov.tr/eskisite/kararlar/iptalitiraz/K1963/K1963-087.htm; Bkz. *Özbudun*, a.g.e., s. 105.

diği düşüncesiyle bireyler devletçe sakıncalı görülebilecek web sitelerine girmekten kendileri vazgeçmektedirler. Erişim engelleme gibi somut bir teknik kullanmadığı için de fiili engelleme devlete atfedilememektedir.

5651 sayılı Kanunda sosyal teknik olarak nitelendirilebilecek temel husus yer, erişim ve İnternet toplu kullanım sağlayıcılara yönelik getirilen trafik verilerini saklama yükümlülüğüdür. Bu düzenleme suçla mücadele ve bu doğrultuda faillerin tespiti amacıyla getirilmiştir[528]. Suçla mücadele amacıyla bu tür verilerin elde tutulması zorunlu olmakla birlikte 5651 sayılı Kanun bu tür verilerin nasıl saklanacağı ve hangi şartlar altında kullanılacağına dair bir düzenleme içermemekte veya herhangi bir standarda atıf yapmamaktadır[529]. Örneğin Avrupa Birliği, kişisel verilerin Veri Saklama Yönergesi'ne[530] uygun olarak ve yalnızca çok özel durumlarda ve ancak kendi hukuk düzenlerinin yetkili kıldığı ulusal mercilere açıklanmasını öngörmektedir. Ayrıca, E-Ticaret Yönergesi verilerin trafik verilerinin servis sağlayıcılar tarafından belirli bir süre saklanmasını ve o süre geçtikten sonra tamamen silinmesini öngörmektedir[531].

Türk Hukukunda henüz özel verilerin korunmasını öngörecek özel bir düzenleme de yer almamaktadır. Kişisel Verilerin Korunması Kanununa yönelik çalışmalar henüz tasarı aşamasındadır[532]. Bu sebeple,

[528] *Dülger*, a.g.e., s. 1487.

[529] *Akdeniz/Altıparmak*, a.g.e., s. 73.

[530] Directive of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, http://register.consilium.eu.int/pdf/en/05/st03/st03677.en05.pdf.

[531] E-ticaret yönergesinin belirli bir süre saklanmasını öngörmesine rağmen İsveçli bazı servis sağlayıcılar kullanıcılarını korumak ve özel hayatlarının gizliliğini sağlamak amacıyla belirli bir aralıktaki tüm trafik verilerini silmeye karar vermişlerdir. Bkz. Swedish ISPs vow to erase users' traffic data, http://news.cnet.com/8301-1023_3-10229618-93.html; Öte yandan, ABD trafik bilgilerinin saklanmasına ilişkin yükümlülüğü Wi-Fi erişim noktası işleticilerinin, otellerin, kahve dükkanlarının, küçük-büyük işletmelerin, kütüphanelerin, okulların, üniversitelerin, devlet kurumlarının, Voice over IP servislerinin, uçaklardaki Aircell'lerin ve ev kullanıcılarının tamamını kapsayacak şekilde genişletmek için yeni bir yasal düzenlemeye gitmektedir. Bkz. İnternet Servis Sağlayıcıların, Wi-Fi'lerin Logları Polis İçin Saklamalarını Öngören Kanun Tasarısı!, http://www.leylakeser.org/2009/02/internet-servis-saglaycларn-wi-filerin.html.

[532] Bkz. Kişisel Verilerin Korunması Kanun Tasarısı, http://www.kgm.adalet.gov.tr/

5651 sayılı Kanundaki trafik bilgilerinin saklanmasına ilişkin hükümler belirsizlik taşımaları sebebiyle iletişimin ve özel hayatın gizliliği önünde tehdit oluşturmaktadır. Bu hükümler bireyler üzerinde psikolojik etki oluşturabilmeleri ve bireyleri oto-sansüre yöneltebilmeleri sebebiyle sosyal engelleme tekniği olarak kabul edilmektedir.

5. Demokratik toplum düzeninin gereklilikleri

Hakkın özü gibi demokratik toplum düzenin gereklilikleri de Anayasada tanımlanmamıştır. Ayrıca Anayasa, esas alınması gereken demokratik toplum düzenin 1982 Anayasası ile benimsenmiş demokratik toplum düzeni anlayışı mı, yoksa çağdaş hürriyetçi demokrasilerin genel ve evrensel nitelikleri mi olduğu hususunda da suskundur. Doktrinde çağdaş hürriyetçi demokrasilerin genel ve evrensel niteliklerinin göz önüne alınması gerektiği kabul edilmektedir[533]. Anayasa Mahkemesi'nin kararları da bu doğrultuda gelişmiştir. Ayrıca Anayasa Mahkemesi, demokratik toplum düzeninin gereklerini hakkın özünün korunması ile özdeşleştirmekte, bir temel hak ve hürriyetin özünü ortadan kaldırıcı bir düzenlemenin, aynı zamanda demokratik toplum düzeninin gereklerine de aykırı olacağı sonucuna varmaktadır[534].

5651 sayılı Kanunundaki İnternet içeriğine müdahale niteliği taşıyan erişim engelleme sebeplerinin demokratik toplum düzeninin gerekleriyle bağdaşıp bağdaşmadığının tespit edilebilmesi için mukayeseli hukuktaki yaklaşımların göz önünde bulundurulması gerekmektedir.

Beşinci bölümde açıklandığı üzere ABD çocuk pornografisi, müstehcenlik, ulusal güvenlik ve fikri mülkiyet ihlalleri gibi konularda İnternet içeriğine müdahale etmektedir. Avrupa Birliği ise genel bir müdahale politikası takip etmemekte ve bu konudaki tercihi üye devletlere bırakmaktadır. Müdahale sebepleri bakımından Avrupa ülkelerinin temel yaklaşım gerçek hayatta suç olan her şeyin sanal dünyada da suç kabul edilmesi

tbmmkom/kisiselveriler.pdf.

[533] *Özbudun*, a.g.e., s. 106.

[534] Anayasa Mahkemesi, K.T.: 22.05.1987, E: 1986/17, K: 1987/11, AMKD, Sayı: 23, s. 222. Karar metni için bkz. http://www.anayasa.gov.tr/eskisite/kararlar/iptalitiraz/K1987/K1987-11.htm. Bkz. *Özbudun*, a.g.e., s. 108.

ve üye devletçe uygun görülecek sebeplerle İnternet içeriğine müdahale edilmesi yönündedir. Almanya ve Fransa gibi Avrupa ülkeleri yoğun olarak ırkçı söylem ve çocuk pornografisi sebebiyle müdahaleyi gerçekleştirmektedir. Bir diğer Avrupa ülkesi İngiltere ise çocuk pornografisinin yanı sıra müstehcenlik konusunda katı tutumunu korumaktadır.

Müdahale konusunda en uç noktayı Çin oluşturmaktadır. Çin, ulusal güvenliğin, kamu düzenin ve kamu ahlakının korunması amacıyla çocuk pornografisi ve müstehcenlik dışında insan haklarıyla ilgili web sitelerini yoğun ve sistematik bir şekilde engellemektedir. Singapur ise iç hukuku birçok sebeple İnternet içeriğine müdahaleye olanak vermesine rağmen, çoğu pornografik sembolik sayıda web sitesinin erişimini engellemektedir. Ancak Singapur dini ve siyasi içerikli web sitelerini sıkı denetime tabi tutmaktadır. Ayrıca seçim dönemlerinde İnternet içeriğinin düzenlenmesine ilişkin özel yöntemler kullanmaktadır. Güney Kore ise Kuzey Koreli web sitelerinin erişimini engellemekle uğraşmaktadır. Arap dünyasında ise Suudi Arabistan genel ahlakın korunması amacıyla her türlü pornografik içeriği ve İslam aleyhtarı içeriği engellemektedir.

Her devlet kendi farklı bir gerekçeyle ve farklı düzeyde İnternet içeriğine müdahale etmektedir. Demokratik toplum düzeninin gereklerine uymak için belirleyici faktör erişim engelleme sebeplerinin sayısı değil nasıl kaleme alındığıdır. Bir kanunda çok sayıda erişim engelleme sebebi olmasına rağmen o kanun yine de demokratik kabul edilebilir. Mukayeseli hukuktaki bu örnekler göz önüne alındığı zaman devletlerin İnternet içeriğine müdahalesi konusunda ortak paydayı çocuk pornografisi oluşturmaktadır. 5651 sayılı Kanun da çocukların cinsel istismar suçunu bir erişim engelleme sebebi altında çocuk pornografisini bir erişim engelleme sebebi olarak kabul etmiştir. Diğer erişim engelleme sebepleri de ailenin ve gençliğin korunması ana ilkesine göre belirlenmiştir. Zaten erişim engelleme istatistikleri göz önüne alındığında, 5651 sayılı Kanun en çok çocukların cinsel istismarı ve müstehcenlik suçlarına ilişkin uygulama alanı bulmuştur[535].

[535] Bkz. *İhbar İstatistikleri*, dn. 321.

Kanunla sınırlama kısmında açıklandığı üzere ulusal güvenlik, kamu düzeni gibi muğlâk kavramların erişim engelleme sebebi olarak kabul edilmemesi demokratik toplum düzeninin gerekleriyle uyum gösteren bir tercihtir. 5651 sayılı Kanunda yer alan tek ideolojik engelleme sebebi 5816 sayılı Kanunda yer alan suçlara ilişkindir. Ailenin ve gençliğin korunmasıyla ilgili bir kanunda 5816 sayılı Kanundaki suçların erişim engelleme sebebi olarak kabul edilmesi kanunu *sui generis* bir niteliğe kavuşturmaktadır. Buna rağmen, Avrupa Birliği'nin gerçek hayatta suç olan her şeyi sanal dünyada da suç sayan ve bu şekilde bir ayrım gözetmeksizin İnternet içeriğine müdahale olanağı tanıyan yaklaşımı göz önüne alındığında, 5651 sayılı Kanunun İnternet içeriğine müdahalesi sınırlı bulunmaktadır. İnternetin küresel ağ niteliğini korumak ve ağ tarafsızlığını sağlamak amacıyla bir suçun İnternet üzerinden işlenebilmesi o suç için erişim engelleme kararı verilebilmesi için yeterli görülmemelidir.

5651 sayılı Kanunda yer alan engelleme sebeplerin azaltılmasını talep edenler olduğu gibi bu sebeplerin 5651 sayılı Kanunun temel amacı olan İnternet ortamında işlenen suçlarla mücadelede yetersiz olduğunu düşünenler de bulunmaktadır[536]. Tüm bu görüşlere rağmen, 5651 sayılı Kanunun Türkiye'nin İnternet içeriğine müdahalesi konusundaki temel ilkelerini belirlemiş olması sebebiyle yerinde bir düzenlemedir. Bu Kanun sayesinde Türk Hukukundaki erişim engellemeleri yasal bir zemine oturmuştur.

Öte yandan hukuka aykırı veya zararlı İnternet içeriğinden çocukları ve gençleri korumak için devletin olduğu kadar ebeveynlerin de üzerine düşen yükümlülükler bulunmaktadır. Bunların başında filtreleme yazılımlarını kullanmak gelmektedir. Erişim engelleme teknikleri gibi bu tür yazılımlar aşırı engelleme veya hiç engellememe gibi riskleri taşıdıkları için rağbet görmemektedirler[537]. Aşırı engelleme durumu nihayetinde ebeveynin müdahalesiyle kolaylıkla aşılması mümkün bir durumdur. Hiç engellememe durumunu ortadan kaldırmak için ise web sitesi sahiplerinin sosyal sorumluluk bilinciyle hareket etmesi gerekmektedir.

---

[536] *Dülger*, a.g.e., s. 1521.

[537] *Akdeniz/Altıparmak*, a.g.e., s. 90.

Sosyal sorumluluk bilincine sahip web siteleri, ilk erişim sayfalarında içerikleri hakkında genel uyarıları bulunduktan sonra içeriklerini kullanıcıların erişimine sunmaktadırlar. Bu şekilde hem filtreleme yazılımları tarafından tanınmaları kolaylaşmakta hem de sakıncalı olabilecek içeriğe erişimde tercih hakkı tamamen kullanıcıya bırakılmaktadır.

Web site sahiplerinin bu şekilde hareket etmemesi durumunda etkili bir filtrelemeyi sağlamak amacıyla devlet müdahalesi gündeme gelecektir. Bu doğrultuda, erişim engelleme yerine, puanlama ve içerik etiketleme tekniğinin kullanılması mümkündür. Bu teknik Singapur tarafından yaygın olarak kullanılmaktadır. Singapur, web sitesinin sakıncalı olduğunu tespit ettiğinde web sitesini tamamen engellemek yerine, web sitesinin sadece ilk erişim sayfasına müdahale etmektedir. Sakıncalı bir web sitesi ziyaret edildiğinde sitenin sakıncalı içerikli olduğu kullanıcı karşısına gelmekte ve bu şekilde web sitesini ziyaret etmeden kullanıcının bilgilenmesi sağlanmaktadır. Bu tekniğin diğer bir faydasıysa siteyi filtreleme yazılımları tarafından tanımlanacak bir şekilde sakıncalı içerik kategorisine almasıdır. Bu şekilde web sitesi filtreleme yazılımı kullanılmadan ancak ilgili uyarı görüntülendikten sonra açılmakta, filtreleme yazılımı tarafından erişiminde tercih ise ebeveyne bırakılmaktadır.

5651 sayılı Kanun sakıncalı site olarak etiketleme tekniğini kullanmasa da eğitim faaliyetlerini artırmak ve filtreleme yazılımlarının kullanılmasının yaygınlaştırılmak için TİB'i yetkilendirmiştir. TİB de bu doğrultuda gereken çalışmalarını sürdürmektedir[538]. Ayrıca, uluslararası işbirliğini artırmak ve İnternet ortamında işlenen suçlarla daha etkin bir şekilde mücadele etmek amacıyla INHOPE[539] birliğine üyelik süreci başlatılmıştır[540].

---

[538] Örneğin filtreleme yazılımları standardını belirlemiştir. Bkz. Onaylı İçerik Filtreleme Yazılımları, http://www.tib.gov.tr/onayli_filtreleme_yazilimlari.html; Ayrıca toplumu etkin bir şekilde bilinçlendirmek amacıyla Guvenliweb sitesini faaliyete sokmuştur. Bkz. http://www.guvenliweb.org.tr.

[539] INHOPE hakkında daha fazla bilgi için bkz. dn. 168.

[540] TİB İnternet Dairesi Başkanı Osman N. Şen İnternet Alanında Türkiye ve Dünya'da Yaşanan Gelişmeleri değerlendirdi, http://www.tib.gov.tr/etkinlikler_detay12.html.

B. İfade hürriyeti açısından değerlendirme

Anayasa ifade hürriyetini, herkesin düşünce ve kanaatini söz, yazı, resim veya başka yollarla tek başına veya toplu olarak açıklama ve yayma hakkına sahip olması şeklinde tanımlamaktadır[541]. Anayasa bu hakkın herhangi bir resmi makamın müdahalesi olmaksızın haber ya da fikir almak ya da vermek serbestliğini içerdiği kabul etmiştir. Bu hüküm göz önüne alındığında, ifade hürriyetinin bilgi edinme, düşünme ve ifadeyi yayma şeklinde üç farklı unsuru olduğu anlaşılmaktadır[542].

İfade özgürlüğünün sözlü ve yazılı anlatım, sanatsal gösterim, kişisel görünüm ve görüntü tercihi, gösteri, yürüyüş, toplantı yapma ve örgütlenme gibi özgürlüklerin her birini içine aldığı kabul edilmektedir[543]. Bu sebeple, ifade hürriyeti demokrasinin vazgeçilmez şartı olarak görülmektedir. Nihayetinde ifade hürriyetinin etkin bir şekilde kullanıldığı ortamlarda demokratik düşünce olgunlaşabilmekte ve bireyler kendi gelişimlerini sağlayabilmektedir.

Kişilerin kendilerini ilgilendiren her konuda haberdar olmaları en temel hakları olarak kabul edilmektedir[544]. İfade özgürlüğünün ilk aşaması olan bilgi edinme aşamasında bireyler, kitlesel veya bireysel iletişim araçlarını kullanarak fikir ve kanaatlerini oluşturmak için gerekli olan bilgiyi toplarlar. Kitlesel veya bireysel iletişim araçları ifadeyi veren açısından bilgi ve haber verme hakkını, ifadeyi alan için ise bilgi edinme hakkını kapsamaktadır[545]. Bireylerin bilgiye erişimleri engellendiği takdirde, hem bilgi edinme hakları hem de haber verme ve geniş anlamda iletişim özgürlükleri engellenmiş olmaktadır.

İfade özgürlüğünün bir diğer aşaması ise düşünce aşamasıdır. Düşünce aşamasının içsel bir durum olması sebebiyle her türlü müdahaleden

---

[541] Anayasa, m. 26.

[542] Adnan Küçük, İfade Hürriyetinin Unsurları, Ankara 2003 (*"Küçük"*), s. 13.

[543] Mustafa Erdoğan, Demokratik Toplumda İfade Özgürlüğü: Özgürlükçü Bir Perspektif, Teorik ve Pratik Boyutlarıyla İfade Hürriyeti (Editör: Bekir Berat Özipek), (s. 37-47), Ankara 2003 (*"Erdoğan"*), s. 37.

[544] *Erdoğan*, a.g.e., s. 40.

[545] *Küçük*, a.g.e., s. 25.

uzak olduğu iddia edilmektedir. Ancak resmi ideolojiler özgür düşüncenin ortaya çıkmasını engellemektedir. İdeolojik düşünce tüm yanlışlığına rağmen dokunulmazlığı sebebiyle toplum tarafından mutlak doğru olarak muamele görmekte ve bu toplumların ilerlemesini önlemektedir.

Demokrasiler bireysel tercihlerin üstünlüğüne dayanan ve neyin iyi ve neyin kötü olduğuna bireylerin kendisinin karar verdiği rejimlerdir[546]. Bireylerin, doğruyu tercih etmek kadar yanlışı da seçmeleri kendi haklarıdır. Bireysel tercih hakkı, devletin herhangi din dâhil her türlü ahlaki değeri topluma doğrudan veya dolaylı yollarla zorlamasına izin vermez. Bu sebeple, tercihin devlet tarafından yapılması o konu üzerindeki tüm düşünsel faaliyetleri de engellemektedir.

İfadeyi yayma aşamasında ise kitlesel veya bireysel iletişim araçlarından edinilen bilgiyle oluşturulmuş düşünce başkalarına aktarılmaktadır. Bu aşamanın etkinliği iletişim özgürlüğünün tanınmasını ve çoğulcu bir serbest tartışma ortamının varlığını gerekli kılmaktadır[547].

İfade özgürlüğünü yasaklamak hiçbir zaman başarılı olmamış; ifadeler bir şekilde kendilerini gösterecek alternatif yollar bulmuşlardır[548]. Bu alternatif yol şiddet olabileceği gibi mevcut sistemin sınırlarını zorlamak şeklinde de ortaya çıkabilmektedir. Bu durum İnternete ilişkin sınırlamalar için de geçerlidir. Erişim engelleme teknikleri ne kadar gelişiyorsa bunları aşma teknikleri de aynı hızla gelişmektedir. Bazen hiçbir teknoloji kullanmadan basit şifreli konuşma yoluna dahi başvurulabilmektedir. Bu sebeple engellemeler bilgiye erişimi zorlaştırmaktan başka bir amaca hizmet etmemektedir. Ayrıca erişim engelleme teknolojileri ekonomik olarak da külfetli oldukları için kamu kaynakları gereksiz yere kullanılmış olmaktadır.

İnternet hem bireysel ve kitlesel bir iletişim aracı hem de bir bilgiye erişim aracıdır. İnterneti kullanmak artık temel bir yetenek haline gelmiştir. İnternetin yaygınlaşması bireylerin alışkanlıklarını kökten değiştirmiş ve bilgi ve ağ toplumu gibi yeni kavramları ortaya çıkarmıştır. İnternet

[546] Erdoğan, a.g.e., s. 41

[547] *Küçük*, a.g.e., s. 42.

[548] *Erdoğan*, a.g.e., s. 42.

toplumların kabuklarını kırmalarına ve hem demokratik hem de ekonomik anlamda hızla gelişmelerine olanak vermektedir. İnternetin cazipliği ucuz ve hızlı bir bilgiye erişim ve iletişim aracı olmasıdır. Bu hız ifadeyi hızla yaymaya yaradığı gibi, örgütlenmeleri de hızlandırmaktadır. Tüm bu özellikleri sebebiyle İnternet ifade hürriyetinin en temel araçlarından birisi haline gelmiştir. İnternetin, insan hakları aktivizmindeki etkinliği "*Fare, kılıçtan keskindir*."[549] şeklinde özetlenmektedir.

İnternetin önlenemez bir özgürleştirme gücü vardır[550]. Devletler İnterneti vatandaşlarına sunmakla, önleyemeyecekleri kadar çok bilginin ülkelerine akacağının farkındadırlar. Ancak, İnternet ekonomik gelişmeye olan katkısından dolayı İnterneti hiçbir ülke tamamen engellememektedir. Bunun yerine, ulusal değerlerin, kamu düzeninin, ahlakın korunması gibi sebeplerle İnternet içeriğine müdahale etmektedir.

Bir web sitesine erişim engelleme kararı verildiği durumda bireylerin hem bilgiye erişim hakkı hem de iletişim hakkı engellenmiş olmaktadır. Daha önce açıklandığı üzere, erişim engelleme kararları birer tedbir niteliğindedir. Bu tedbirlerle, kesin hüküm olmadan temel hak ve hürriyetlerin geçici olarak sınırlanmasına olanak tanımaktadırlar. Geçici nitelikte olan bu koruma tedbirleri aleyhine itiraz mekanizmaları, bürokratik veya ekonomik sebeplerle veya yaptırıma uğrama korkusuyla çeşitli sebeplerle çoğu zaman işletilmemekte ve engellemeler kalıcı hale gelebilmektedir. Bu da ifade ve iletişim hürriyetinin kesin hüküm olmadan kalıcı olarak kısıtlanması gibi bir sonuç doğurabilmektedir. İdari tedbirlerin varlığı durumda, idare bir temel hak ve hürriyeti kalıcı olarak kısıtlamış olmaktadır.

Öte yandan, 5651 sayılı Kanun'daki sınırlama sebeplerinin muğlâklığı kanunun uygulama alanını belirsiz bir hale getirmektedir. Bu muğlâklık sebebiyle, içerik, yer ve hizmet sağlayıcılar herhangi bir hukuki veya cezai sorumluluk altına girmemek için İnternet ortamında bilgi yayınlamaktan veya iletişim kurmaktan çekinebilmektedir. Düzenleme bu haliyle bireyleri İnterneti kullanmaya teşvik etmekten ziyade uzaklaştırmaya hizmet etmektedir. Yukarıda açıklandığı üzere, devlet resmi ideoloji veya genel

[549] *Hick/Halpin/Hoskins*, a.g.e., s. 41 vd.

[550] *Goldsmith/Wu*, a.g.e., s. 89.

ahlak adı altında herhangi bir değeri bireylere zorla benimsetmemelidir. Erişim engellemenin etkisiz ve kolay aşılabilir bir yöntem olduğu da göz önüne alındığında, bir içeriğin sakıncalı olup olmadığı konusundaki tercih hakkı tamamen bireylere bırakılmalıdır. Devlet, sadece mahkemeler eliyle ve kesin bir hükümle suç teşkil eden içeriğe müdahale etmelidir.

Bir yasaklamanın sansür olarak kabul edilip edilmemesi için etkilenen hakların sayısı ve yasaklama gerekçelerinin keyfi uygulamaya yol açıp açmadığının tespit etmesi gerekmektedir. Daha önce açıklandığı üzere, İnternetin kullanım alanlarının artmış olması engelleme sebebiyle etkilenen hakların sayısını da artırmaktadır. Ayrıca, engelleme sebeplerinin muğlâklığı 5651 sayılı Kanunun uygulamasını sübjektif bir hale getirmektedir. Devletin sosyal ve ekonomik hayata doğrudan kurallar koyarak müdahale etmesi sansürdür; ancak bunu teknoloji kullanarak gerçekleştirmesi İnternetin kullanım alanlarının bu kadar artması sebebiyle sansürden ve bireyler üzerinde siyasal veya fiziksel güç kullanmaktan daha ağır bir etki oluşturduğu kabul edilmektedir[551]. Bireyler İnternetin bu kadar yaygınlaşması ve ona bağımlı hale gelmeleri sebebiyle bu tür sınırlamalara karşı direnç de gösterememektedirler.

[551] *Deibert/Palfrey/Rohozinski/Zittrain*, a.g.e., s. 2.

§ 7. SONUÇ

Bilgiye erişimin ve iletişimin aracı olan İnternetin kullanım alanları ve oranları günbegün artmaktadır. 1960'lı yıllardaki askeri bir projenin ürünü olan İnternet, zamanla onu geliştirenlerin belki de hiç öngörmedikleri bir hale gelmiştir. İnternetin bu derece yaygınlaşması İnternetin yönetimi konusundaki devletlerarası menfaat çatışmalarını ve mücadeleyi derinleştirmiştir.

İnternete önceleri suçla mücadele amacıyla müdahale eden devletler, İnternetin sosyal, siyasal ve ekonomik hayatı yönlendiren modern hayatın en etkili aracı olduğunun farkına varmışlardır. Bu doğrultuda, devletler kendi ideolojilerini İnternete teşmil etmeye ve daha çok sebeple İnternete müdahale etmeye başlamışlardır. Teknolojinin gelişmesiyle birlikte farklı yöntemleri kullanarak etkinliklerini artırmaya çalışmışlardır.

Devletlerin İnternet içeriğine müdahale politikaları onların demokrasi ve insan hakları anlayışını yansıtmaktadır. Her devlet bulunduğu ekonomik, sosyal ve siyasal koşullar sebebiyle İnternet içeriğine farklı yöntem ve teknikler kullanarak müdahale etmektedir. Bununla beraber tüm teknolojik gelişmişliğe rağmen İnternet içeriğine müdahale için mükemmel bir teknik bulunmamakta; her tekniğin kendine has güçlü ve zayıf noktaları bulunmaktadır. Hatta bazı durumlarda kullanılan teknik o kadar kolay aşılabilmektedir ki, müdahale sadece erişimin zorlaştırılmasına hizmet etmektedir. Buna rağmen, devletler belirli içeriğe karşı hoşnutsuzluklarını göstermek amacıyla bu tür teknikleri kullanmaya devam etmektedirler. Teknolojinin yetersiz kaldığı durumlarda ise devletler sosyal teknikleri kullanarak bireylerin oto-sansür uygulamalarını

sağlamaktadırlar. Bu doğrultuda, bireylerin İnternet ortamındaki her adımlarını izlenmekte ve ihlaller ağır yaptırımlara bağlanmaktadır.

1993 yılında İnternet ağına dâhil olan Türkiye, 2001 yılına kadar İnternete önemli bir müdahalede bulunmamıştır. Ancak İnternetin kullanım oranlarının ve buna bağlı olarak sosyal etkilerinin hızla artmasıyla birlikte Türkiye İnternette yer alan hukuka aykırı ve zararlı içeriğe karşı duyarsız kalmamış ve çeşitli sebeplerle erişim engellemeleri gerçekleştirmiştir. Bu dönemde gerçekleştirilen erişim engellemelerinin İnternet içeriğine müdahale yetkisi veren özel bir kanuna dayanmayışı ve yalnızca genel hükümlerle gerçekleştirilmesi birtakım hukuki tartışmalara yol açmıştır. Mevcut gereklilik ve eleştiriler göz önünde bulundurularak 2007 yılında İnternet içeriğine müdahale politikasını hukuki zemine oturtulmak istenmiş ve artan bilişim suçlarıyla etkin bir şekilde mücadele etmek amacıyla 5651 sayılı Kanun yürürlüğe koyulmuştur.

5651 sayılı Kanunla, yeni bilişim suçları getirilmemektedir. Sadece sınırlı sayı prensibine göre belirlenen 5237 s. TCK'da yer alan intihara yönlendirme, çocukların cinsel istismarı, uyuşturucu ve uyarıcı madde kullanılmasını kolaylaştırma, sağlık için tehlikeli madde temini, müstehcenlik, fuhuş, kumar oynanması için yer ve imkân sağlama suçları ile 7258 sayılı Kanunda ve 5816 sayılı Kanunda yer alan suçlara ilişkin "erişimi engelleme" şeklinde özel bir tedbir öngörülmüştür. Ayrıca, içerik, yer, erişim ve toplu kullanım sağlayıcıların hukuki ve cezai sorumluluklarına ilişkin düzenlemeler getirilmiştir. Avrupa Birliği'nin gerçek hayatta suç sayılan her konuda İnternet içeriğine müdahaleye imkân veren yaklaşımı ile ABD, Çin gibi devletlerin ulusal güvenlik gibi muğlâk sebeplerle İnternet içeriğine müdahaleye imkân veren yaklaşımları göz önüne alındığında, 5651 sayılı Kanunun getirmiş olduğu düzenleme İnternetin küresel ağ niteliğine uyan sınırlı bir düzenlemedir.

5651 sayılı Kanunda eleştirilen temel husus TİB gibi idari bir kuruma adli makamların muhakemesini gerekli kılacak konularda yetki verilmiş olmasıdır. Eleştirinin temelinde TİB'e böyle bir yetki verilmiş olmasına rağmen yurtdışı kaynaklı web siteleri için TİB tarafından verilen kararlarının adli makamların onayına sunulmaması veya bu tür kararlar

için süresel bir sınırlamanın koyulmaması yer almaktadır. Bu yaklaşım, tedbirlerin geçiciliği ilkesine aykırılık oluşturan bir durum olarak kabul edilmektedir.

Eleştirilen bir diğer husus ise 5651 sayılı Kanunun hukuka aykırı veya zararlı İnternet içeriğinin önlenmesine ilişkin temelde erişimin engellenmesi gibi katı bir yöntemi öngörmesidir. Kanun, uyarı yöntemleri ile filtreleme yöntemlerine ilişkin hükümler içermesine rağmen temel yöntem olarak erişimin engellenmesi yönteminden hareket etmektedir. Kanunun temel amacının hukuka aykırı veya zararlı kabul edilen içeriğin İnternet ortamından kaldırılması olduğu göz önüne alınırsa, haklı olarak öncelikle uyarı mekanizmalarının işletilmesi; buradan bir sonuç alınamaması durumunda erişim engelleme kararlarının verilmesi gerekmektedir. Her ne kadar adli makamlar ve TİB bu tür mekanizmalara belirli durumlarda başvursa da, tercihlerin ihtiyari olması gerekli güvenceyi sağlamamaktadır.

Diğer yandan, 5651 sayılı Kanun youtube.com web sitesine koyulan erişim engellemesi ile gündem oluşturmuş; ancak Kanunun erişim engelleme konusu dışındaki hükümleri yeterince tartışılmamıştır. Bu hükümlerin başında yer, erişim ve İnternet toplu kullanım sağlayıcılarına getirilen trafik bilgilerini saklama yükümlülüğü gelmektedir. Her ne kadar 5651 sayılı Kanun trafik bilgilerini saklama yükümlülüğünü öngörmüşse de, Türk Hukukunda özel verilerin korunmasına ilişkin düzenlemelerin henüz tasarı aşamasında olması trafik bilgisine ilişkin uygulamada belirsizliğe sebep olmaktadır.

5651 sayılı Kanun yeni bir kanundur ve henüz kanunun uygulamasına ilişkin mahkeme içtihatları oluşmamıştır. Bu sebeple, Kanunun uygulaması birçok alanda belirsizliğini korumaktadır. Buna rağmen, kötü kaleme alınmış bir kanunun öngörülü uygulayıcılar tarafından doğru bir şekilde uygulanması mümkündür. Bu doğrultuda uygulamanın yerindeliğini denetlemek için uygulamanın İnternetin kendine özgü küresel ağ niteliğiyle bağdaşıp bağdaşmadığının değerlendirilmesi ve denetlenmesi gerekmektedir. Bu doğrultudaki uygulamanın, son aşamada bireyleri hareketsizliğe itmemesi gerekmektedir. Devletlerin İnternete ilişkin

düzenlemelerde başarısız olmalarının temelinde İnternetin dinamik niteliğini göz ardı etmeleri ve İnterneti egemenliklerini icra ettikleri klasik mecralarla eşdeğer tutumları yer almaktadır.

İnternetin bireylerin davranışlarını etkileyen önlenemez bir özgürleştirme gücü vardır. Bireylerin sosyal ve kültürel olarak kişiliklerinin gelişmesine yardımcı olan İnternet, ekonomik kalkınmanın hızlanmasında da önemli bir etkendir. İnternet kamusal yönetimde üretkenliği ve saydamlığı sağlerken, elektronik ticareti artırmakta ve bilişim alanında yeni iş kolları oluşturmak suretiyle istidahdam yaratmaktadır. İnternetin tüm bu faydaları göz önüne alındığında, İnternete ilişkin düzenlemelerin sınırlayıcı değil teşvik edici olması gerekmektedir.

TİB, İnternetin günlük hayattaki önemini "İnternet hava gibidir. Varlığı ancak yokluğunda hissedilir." şeklinde özetlemektedir[552].

[552] İnternet Daire Başkanlığı, 23 Kasım 2007 – 23 Kasım 2008 Faaliyet Raporu, http://www.tib.gov.tr/dokuman/faaliyet_raporu.pdf, s. 2.