5651 SAYILI KANUN VE BİLGİ GÜVENLİĞİ İLİŞKİSİ

Mehmet Salih GÖK

109615044

İSTANBUL BİLGİ ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
HUKUK YÜKSEK LİSANS PROGRAMI
(EKONOMİ HUKUKU)

Danışman: Yard. Doç. Dr. Leyla Keser BERBER

2012

5651 SAYILI KANUN VE BİLGİ GÜVENLİĞİ İLİŞKİSİ

LAW NUMBER 5651 AND ITS RELATION TO INFORMATION SECURTY

Mehmet Salih GÖK

109615044

Yard. Doç. Dr. Leyla Keser BERBER :

Öğr. Gör. Yasin BECENİ :

Öğr. Gör. Tuğrul SEVİM :

Tezin Onaylandığı Tarih :

Toplam Sayfa Sayısı : 62

Anahtar Kelimeler (Türkçe)

1) 5651 Sayılı Kanun
2) Engelleme aşma
3) İnternet içeriği düzenleme
4) İnternete erişimi engelleme
5) Youtube

Anahtar Kelimeler (İngilizce)

1) Law Number 5651
2) Filter circumvention
3) Internet content regulation
4) Blocking Access to the Internet
5) Youtube

Özet

İnternet kullanım oranı tüm dünyada hızla artmaktadır. Bu nedenle günümüzde iletişimin hem sınırları genişlemiş, hem hızı artmış, hem de iletişim büyük oranda İnternet üzerine kaymış durumdadır. Bunun sonucunda, yeryüzünde her zaman olagelmiş olan, yöneticilerin kitleleri etkileme ve yönlendirme arzusu İnternetin dünya toplumları içinde elde etmiş olduğu konumu görmezden gelmemektedir. İnternet bugün dünyanın hemen her yerinde sansüre uğramaktadır. Ayrıca bazı ülkelerde sansürden ileri geçilmekte, İnternet manipüle edilmektedir. İnternetin kendine has doğası göz önünde bulundurulduğunda İnternetin tamamen kontrol dışında kalmasının da insanlık için çok iyi sonuçlar doğurmayacağı düşünülebilir.

Bütün dünyada olduğu gibi Türkiye'de de İnternetin sansürlendiğine yönelik iddialar vardır. Türkiye'de İnternete müdahale 2007 yılına kadar birçoğu TCK maddelerine dayanarak verilen kararlara dayanılarak yapılmaktaydı. Ancak Anayasa'nın 13. maddesine göre temel hak ve hürriyetleri sınırlayıcı düzenlemelerin ancak kanunla yapılması gerektiği ilkesi bu uygulamayı hukuka aykırı kılmaktaydı. Ayrıca açıkça İnternet ortamını zikreden ve İnternetin kendine özgü niteliğini ve aktörlerini göz önüne almayan düzenlemelerle müdahale edildiği için kamuoyunda tartışmalara yol açmaktaydı. Bu nedenle, 2007 yılında 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun çıkarılmıştır. Kanun'un kabulünden sonra erişim engellemelerin sayısında ciddi bir artış meydana gelmiştir. Zira Kanun, hukuka aykırı olarak tanımladığı içerikle mücadele yöntemini erişim engelleme olarak belirlemiştir. Kanun'un uygulaması ile ilgili olarak da üç tane yönetmelik çıkarılmıştır. Kanun genel olarak, çizdiği net çerçeve ve – diğer birçok ülkedeki uygulamalardan farklı olarak - uygulamadaki şeffaflıktan ötürü takdirle karşılanırken, öncelikle erişim engelleme olmak üzere bazı nedenlerden ötürü de eleştirilmektedir.

Türkiye'de uygulanan erişim engellemeler neticesinde, istatistiklerden edinilen bilgilere göre engelleme aşma yöntemlerinin de sıklıkla kullanıldığı görülmektedir. Engelleme aşma yöntemlerinin genelde çok fazla bilgi güvenliği bilinci olmayan kullanıcılar tarafından kullanılmasından dolayı çok ciddi bilgi güvenliği riskleri ortaya çıkmaktadır. Bu risklerin gerçeğe dönüşmesi durumunda da büyük maddi ve manevi zararlarla karşılaşılmaktadır.

Erişim engellemeler neticesinde ortaya çıkan zararlar ve bu zararlardan korunmak amacıyla Türkiye'de İnternet içerik düzenlemeleri ve uygulamalar konusunda yapılabilecek düzeltmeler ve her seviyede alınabilecek önlemler tezde üzerinde durulan konular olmuştur. Devletten aileye ve toplumun tüm bireylerine düşen görevler konusunda yapılabilecek değişiklikler ifade edilmiştir.

Abstract

Internet use is rapidly increasing all over the world. Hence, both the borders of communication have expanded and the speed has increased and the communication is shifted to a large extent to the web. As a result, the desire of governments to influence people that has always existed on earth has not ignored the role that Internet has acquired within the world communities. Today internet is being censored almost in every country. Moreover in some countries it is more than censorship and internet content is manipulated. Considering the specific nature of the Internet, being totally out of control would not benefit the humanity.

As it is all over the world, it is claimed that Internet is censored in Turkey too. Until 2007 in Turkey, Internet intervention examples were mostly based on the Turkish Penal Code (TCK) articles. However the principle requiring the regulations that limit the fundamental rights and freedoms to be based on specific laws according to the article number 13 of the Turkey Constitution was making the applications illegal. Also trying to regulate the Internet without special regulations which did not mention Internet and its typical nature and actors was causing debates. For this reason, the law number 5651, Regulation of Internet Publications and Combating Crimes Committed by Means of the Law on These Publications has been enacted on 2007. After the Law has been adopted, a significant increase occurred in the number of blocked web sites. Because blocking access is the method determined by the Law to fight the content that is defined as illegal by the Law. Three guiding regulations were published to guide the applications of the Law. The Law has been appreciated having sharp and clear articles and – being different from other many countries – being transparent in applications. On the other hand it has been criticized for many reasons, mostly blocking access to the Internet.

As a result of blocking access to many web sites in Turkey, according to the reports collected from statistics filter circumvention techniques are used commonly. Serious information security risks arise because of those circumvention methods and tools being used by unconscious users. In case of these risks coming true, many individuals face financial and non-pecuniary losses.

Possible improvements about Internet content regulations and applications have been subject to the dissertation in order to minimize the costs of the risks that arise from blocking Internet access and filtering the Internet content. From the authority to the family, future changes about the duties of all members of society have been expressed.

İÇİNDEKİLER

KISALTMALAR

a.g.e.	Adı geçen eser(ler)
AB	Avrupa Birliği
ABD	Amerika Birleşik Devletleri
ARPA	Advanced Research Projects Agency
ARPANET	Advanced Research Projects Agency Network
ARPANET	Advanced Research Projects Agency Network
aşa.	Aşağıda
AVM	Alış Veriş Merkezi
BTK	Bilgi Teknolojileri ve İletişim Kurumu
CGI	Common Gateway Interface
CRC	Convention on the Rights of the Child
DDoS	Distributed Denial of Service
DNS	Domain Name System
EC	European Commission
ECJ	European Court of Justice
EFT	Elektronik Fon Transferi
FSEK	Fikir ve Sanat Eserleri Kanunu
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICANN	Internet Corporation for Assigned Names and Numbers
IE	Internet Explorer
IETF	Internet Engineering Task Force
INHOPE	International Association of Internet Hotlines
IP	Internet Protocol
IP adresi	İnternet Protokol adresi
IWF	Internet Watch Foundation
İSS	İnternet Servis Sağlayıcı
MÜYAP	Bağlantılı Hak Sahibi Fonogram Yapımcıları Meslek Birliği
ONI	OpenNet Initiative
PIPA	Protect Intellectual Property Act
RFC	Request For Comments
RIM	Research In Motion
RTÜK	Radyo Televizyon Üst Kurulu
SABAM	Société d'Auteurs Belge – Belgische Auteurs Maatschappij
SOPA	Stop Online Piracy Act
TBMM	Türkiye Büyük Millet Meclisi
TCK	Türk Ceza Kanunu
TCP/IP	Transmission Control Protocol/Internet Protocol
TİB	Telekomünikasyon İletişim Başkanlığı
UN	United Nations
URL	Uniform Resource Locator (Tekil Kaynak Konumlayıcı)
vb.	ve benzeri
VoIP	Voice Over Internet Protocol
VPN	Virtual Private Network
Washington, D.C.	Washington District of Columbia
yuk.	Yukarıda

KAYNAKÇA

Akdeniz	Akdeniz, Yaman "Governance of Pornography and Child Pornography on the Global Internet: A Multi-Layered Approach," in Edwards, L and Waelde, C eds, Law and the Internet: Regulating Cyberspace, Hart Publishing, 1997, s. 223-241.
Akdeniz/Altıparmak	Yaman Akdeniz / Kerem Altıparmak, İnternet: Girilmesi Tehlikeli ve Yasaktır Türkiye'de İnternet İçerik Düzenlemesi ve Sansüre İlişkin Eleştirel Bir Değerlendirme, 2008
Alkan	Necati Alkan, Terör Örgütlerinin İnternet Ortamında Yürüttüğü Faaliyetler, http://www.caginpolisi.com.tr/20/41-43.htm#_ftn5
Aru	Çağdaş Aru, OpenNet İnisiyatifi 2011'deki İnternet Sansürlerinin Haritasını Çıkarttı, Türkiye 'Seçici' Olarak Sınıflandırıldı, http://turk.internet.com/portal/yazigoster.php?yaziid=36864, 25 Nisan 2012
Aru-2	Çağdaş Aru, ABD Yönetiminden Gözdağı: Ülkeye Yönelik Hack Saldırıları Askeri Bir Harekatla Sonuçlanabilir, http://www.turk.internet.com/portal/yazigoster.php?yaziid=32472, 20 Mayıs 2011
Avşar/Öngören	Zakir Avşar/Gürsel Öngören, Bilişim Hukuku, İstanbul 2010
Bayamlıoğlu	İbrahim Emre Bayamlıoğlu, Fikir ve Sanat Eserleri Hukukunda Teknolojik Koruma, İstanbul 2008
Berber/Kaya	Leyla Keser Berber/Mehmet Bedii Kaya, 5651 Sayılı Kanunun Teknik Ve Hukuki Açıdan Değerlendirilmesi, İstanbul Bilgi Üniversitesi Bilişim Ve Teknoloji Hukuku Enstitüsü, http://www.turk.internet.com/portal/yazigoster.php?yaziid=28665
Berne Convention	Berne Conventionfor the Protection of Literary and Artistic Works, September 9 1886, http://www.wipo.int/treaties/en/ip/berne/trtdocs_wo001.html
Brown	Brown, I. (2008). Internet censorship: be careful what you ask for
Convention on Cybercrime	Convention on Cybercrime, Budapest, 23 November 2001, http://conventions.coe.int/treaty/en/treaties/html/185.htm
Deibert/Palfrey/Rohozinski/ Zittrain	Ronald Deibert/John Palfrey/Rafal Ronozinski/Jonathan Zittrain, Access Denied: The Practice and Policy of Global Internet Filtering, Massachusetts 2008
Deibert/Villenueve	Deibert, R. & Villeneuve, N. (2005). Firewalls and Power: An Overview of Global State Censorship of the Internet. In M. Klang & A. Murray (Eds.), Human Rights in the Digital Age (s.111—124). London: GlassHouse.
Dhamija/Tygar/Hearst	Rachna Dhamija/J. D. Tygar/Marti Hearst, Why phishing works, Proceedings of the SIGCHI conference on Human Factors in computing systems, April 22-27, 2006, Montréal, Québec, Canada
Dinçer	Ergün Dinçer, İngiliz Hükümeti, İsyancılara Ortam Sağlanmaması Konusunda Facebook, Twitter ve RIM ile Toplantı Yapıyor, http://www.turk.internet.com/portal/yazigoster.php?yaziid=33436, 11 Ağustos 2011
Dokurer	Semih Dokurer, Bilişim Suçları Laboratuvarlarında Çocuk Pornografisi İncelemeleri, Adli Tıp Kurumu, http://www.dokurer.net/files/documents/ChildpornExamining.pdf
Durnagöl	Yasemin Durnagöl, 5651 Sayılı Kanun Kapsamında İnternet Aktörlerine Getirilen Yükümlülükler İle İdari Ve Cezai Yaptırımlar, TAAD, Cilt:2, Yıl:2, Sayı:4, 20 Ocak 2011 (s.375 - 416)
Goldsmith/Wu	Jack L. Goldsmith/Tim Wu, Who Controls the Internet? Illusions of a Borderless World, North Carolina 2006
Jeftovic	Mark Jeftovic, How SOPA Will Destroy The Internet, 22.12.2011, http://blog2.easydns.org/2011/12/22/how-sopa-will-destroy-the-internet/
Kaya	Mehmet Bedii Kaya, Teknik ve Hukuki Boyutlarıyla İnternete Erişimin Engellenmesi, 5651 Sayılı Kanun ve Dünya Uygulamaları, 1. Baskı, İstanbul

	2010
McCoy/Bauer/Grunwald/Kohno/Sicker	Damon McCoy/Kevin Bauer/Dirk Grunwald/Tadayoshi Kohno/Douglas Sicker, Shining Light in Dark Places: Understanding the Tor Network
McMillan	Robert McMillan, DNS attack could signal Phishing 2.0, December 2007, http://www.computerworld.com/s/article/9052198/DNS_attack_could_signal_Phishing_2.0
Munns	Roger Munns, First-computer controversy finally nearing a conclusion, http://www.scl.ameslab.gov/ABC/Articles/First-computer.html
Nebil-1	Füsun Sarp Nebil, Müyap Kapatmalarındaki Kötü Alışkanlık, 5651 Dışı Site Erişim Kapatmalarında Kural Haline Dönüşmüş – 1, http://www.turk.internet.com/portal/yazigoster.php?yaziid=20882, 6 Mayıs 2008
Nebil-2	Füsun Sarp Nebil, Türkiye'de Site Erişime Kapatmalarının Tarihçesi – 2, http://www.turk.internet.com/portal/yazigoster.php?yaziid=20909, 8 Mayıs 2008
ONI China Filtering	OpenNet Initiative, Internet Filtering in China, 15 June 2009, http://opennet.net/research/profiles/china
OpenNet Initiative Bulletin	China's Green Dam, The Implications of Government Control Encroaching on the Home PC, OpenNet Initiative Bulletin
RFC 791	RFC: 791, Internet Protocol, Darpa Internet Program Protocol Specification, Eylül 1981, http://tools.ietf.org/pdf/rfc791.pdf
Richard Clayton	Richard Clayton, Anonymity and traceability in cyberspace, Technical report, University of Cambridge Computer Laboratory, Number 653, November 2005, http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-653.pdf
Roberts / Zuckerman/York /Faris/Palfrey	Hal Roberts/Ethan Zuckerman/Jillian York/Robert Faris/John Palfrey, 2011 Circumvention Tool Usage Report, The Berkman Center for Internet & Society, October 2010, http://cyber.law.harvard.edu/publications/2011/2011_Circumvention_Tool_Evaluation
Roberts/Larochelle	Hal Roberts/David Larochelle, Mapping Local Internet Control, Berkman Center for Internet & Society Harvard University, http://cyber.law.harvard.edu/netmaps/country_detail.php/?cc=CN
Roberts/Zuckerman/Faris/ York/Palfrey Evolving Landscape	Hal Roberts/Ethan Zuckerman/Robert Faris/Jillian York/John Palfrey, The Evolving Landscape of Internet Control, A Summary of Our Recent Research and Recommendations, The Berkman Center for Internet & Society, August 2011, http://cyber.law.harvard.edu/publications/2011/Evolving_Landscape_Internet_Control
Roberts/Zuckerman/Palfrey	Hal Roberts/Ethan Zuckerman/John Palfrey, 2007 Circumvention Landscape Report: Methods, Uses, and Tools, The Berkman Center for Internet & Society at Harvard University, March 2009, http://cyber.law.harvard.edu/publications/2009/2007_Circumvention_Landscape_Report
Spring	Tom Spring, Spam Slayer: Slaying Spam-Spewing Zombie PCs, PC World, 2005-06-20
Uzunay/Koçak	Yusuf Uzunay/Mustafa Koçak, İnternet Üzerinden Çocuk Pornografisi Ve Mücadelede Yaşanan Sıkıntılar, Turkish Journal of Police Studies, Vol: 7 Issue:1, pp.97-116, 2005
Yeşil/Alkan	Sezen Yeşil/Mustafa Alkan, İnternet Yönetişimi Ve İçerik Düzenlemeleri, XII. "Türkiye'de İnternet" Konferansı 8-10 Kasım 2007 (s.128 - 135), Ankara
Zittrain/Edelman	Jonathan Zittrain/Benjamin Edelman, Internet Filtering In China, Research Report, Berkman Center for Internet & Society, Harvard Law School Research Paper No. 62, IEEE Internet Computing (March/April 2003)

ELEKTRONİK AĞ ADRESLERİ*

2011 Circumvention Tool Usage Report,
http://cyber.law.harvard.edu/publications/2011/2011_Circumvention_Tool_Evaluation

5651 Sayılı Kanunun Teknik ve Hukuki Açıdan Değerlendirilmesi – 1,
http://www.turk.internet.com/portal/yazigoster.php?yaziid=28665

ABD Yönetiminden Gözdağı: Ülkeye Yönelik Hack Saldırıları Askeri Bir Harekatla Sonuçlanabilir,
http://www.turk.internet.com/portal/yazigoster.php?yaziid=32472

ABD'de TOR Yazılımını Kullanarak Takipten Kurtulmaya Çalışan Uyuşturucu Çetesi Çökertildi,
http://turk.internet.com/portal/yazigoster.php?yaziid=36752

About Inhope, http://www.inhope.org/gns/about-us/about-inhope.aspx

About IWF, http://www.iwf.org.uk/about-iwf

Anonymity and traceability in cyberspace, http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-653.pdf

Berne Conventionfor the Protection of Literary and Artistic Works,
http://www.wipo.int/treaties/en/ip/berne/trtdocs_wo001.html

Bilişim Suçları Laboratuvarlarında Çocuk Pornografisi İncelemeleri,
http://www.dokurer.net/files/documents/ChildpornExamining.pdf

Birth of the Internet, http://library.thinkquest.org/27887/gather/history/internet.shtml

China, http://opennet.net/research/profiles/china

China's online population hit 513 mln, http://www.isc.org.cn/english/Focus/listinfo-18509.html

Cleanfeed (content blocking system), http://en.wikipedia.org/wiki/Cleanfeed_(content_blocking_system)

Convention on Cybercrime, http://conventions.coe.int/treaty/en/treaties/html/185.htm

Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse,
http://conventions.coe.int/Treaty/EN/treaties/Html/201.htm

DNS attack could signal Phishing 2.0,
http://www.computerworld.com/s/article/9052198/DNS_attack_could_signal_Phishing_2.0

Dünyada Internet'in gelişimi, http://www.internetarsivi.metu.edu.tr/tarihce.php

En Çok Ziyaret Edilen Site Sıralamasında Facebook, 2010 Yılında Google'u Geçti,
http://www.sosyalmedyapazarlama.com/2011/01/en-cok-ziyaret-edilen-site-siralamasinda-facebook-2010-yilinda-googleu-gecti/
Fiberoptik, http://tr.wikipedia.org/wiki/Fiberoptik

* Bu bölümdeki URL'ler 1 Haziran 2012 tarihinde tekrar erişilerek güncellikleri ve erişilebilirlikleri teyit edilmiştir.

First-computer controversy finally nearing a conclusion, http://www.scl.ameslab.gov/ABC/Articles/First-computer.html

Global Internet Filtering Map, http://map.opennet.net/filtering-pol.html

How SOPA Will Destroy The Internet, http://blog2.easydns.org/2011/12/22/how-sopa-will-destroy-the-internet/

Human Rights and Rule of Law - News and Analysis, http://cecc.gov/pages/virtualAcad/index.phpd?showsingle=24396

International Strategy For CyberSpace, http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

İngiliz Hükümeti, İsyancılara Ortam Sağlanmaması Konusunda Facebook, Twitter ve RIM ile Toplantı Yapıyor, http://www.turk.internet.com/portal/yazigoster.php?yaziid=33436

Judgment of the Court (Third Chamber) of 24 November 2011. Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)., http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62010CJ0070:EN:NOT
Mapping Local Internet Control, Berkman Center for Internet & Society Harvard University, http://cyber.law.harvard.edu/netmaps/country_detail.php/?cc=CN

Morse Code & the Telegraph, http://www.history.com/topics/telegraph

Müyap Kapatmalarındaki Kötü Alışkanlık, 5651 Dışı Site Erişim Kapatmalarında Kural Haline Dönüşmüş – 1, http://www.turk.internet.com/portal/yazigoster.php?yaziid=20882

OpenNet İnisiyatifi 2011'deki İnternet Sansürlerinin Haritasını Çıkarttı, Türkiye 'Seçici' Olarak Sınıflandırıldı, http://turk.internet.com/portal/yazigoster.php?yaziid=36864

OpenNet Map, http://map.opennet.net/

Protection of Children Act 1978, http://www.legislation.gov.uk/ukpga/1978/37

RFC 791, http://tools.ietf.org/pdf/rfc791.pdf

Robert McMillan, DNS attack could signal Phishing 2.0, December 2007, http://www.computerworld.com/s/article/9052198/DNS_attack_could_signal_Phishing_2.0

Statement from Chairman Smith on Senate Delay of Vote on PROTECT IP Act, http://judiciary.house.gov/issues/issues_RogueWebsites.html

Terör Örgütlerinin İnternet Ortamında Yürüttüğü Faaliyetler, http://www.caginpolisi.com.tr/20/41-43.htm#_ftn5

The Evolving Landscape of Internet Control, A Summary of Our Recent Research and Recommendations, http://cyber.law.harvard.edu/publications/2011/Evolving_Landscape_Internet_Control

The Telephone, http://web.mit.edu/invent/iow/graham_bell.html

Tor: Overview, https://www.torproject.org/about/overview.html.en

Türkiye 2010 Yılı DDoS Raporu, http://blog.lifeoverip.net/2011/02/20/turkiye-2010-yili-ddos-raporu/

United States and Canada, http://opennet.net/research/regions/namerica

Youtube yasağı ülkemizde Ekim 2010'da kaldırılmıştır. http://www.leylakeser.org/search/label/Youtube

§1. GİRİŞ

İnternet, Kaliforniya Üniversitesi'ndeki ARPANET[1] projesi ile hayatımıza girdiği 1969[2] yılından beri büyümekte, içeriğinin denetimi güçleşmekte ve hatta imkânsızlaşmaktadır. İnternetin denetiminin üzerinde çok duruluyor olması ve bu konuya önem verilmesi, yayımlanan içeriğin dünyanın her yerine saniyeler içinde ulaşılabiliyor olması ve bu içeriğe İnternete bağlı her bilgisayardan erişilebiliyor olması nedeniyledir. Öyle ki, konunun temel insan hak ve özgürlüklerine zarar vermeden nasıl çözüleceği devletler bazında tartışılmaktadır. Bazı ülkelerde otorite, çözüm için çok fazla kaynak ve zaman harcamadan sorunu İnternet erişimine sansür uygulayarak çözebileceğini düşünmektedir. Ancak İnternet, özellikle 2000'li yılların başlarından itibaren tüm dünyada sosyal, ekonomik ve kültürel amaçlarla daha yaygın şekilde kullanılmaya başlamıştır[3]. Dolayısıyla sansür sonucu zarar görecek hak ve hürriyetlerin kapsamı da genişlemiştir.

Ülkemizdeki hukuk altyapısı göz önünde bulundurulduğunda, İnternete erişimin kısıtlanması Anayasa'nın 17. maddesindeki maddi ve manevi varlığı koruma ve geliştirme hakkı, 24. maddesindeki din ve vicdan hürriyeti, 25. maddesindeki düşünce ve kanaat hürriyeti, 26. maddesindeki düşünceyi açıklama ve yayma hürriyeti, 27. maddesindeki bilim ve sanat hürriyeti ve 28. maddesindeki basın hürriyeti gibi birçok hak ve hürriyeti sınırlama riski bulunmaktadır. Aslında bu liste teknolojinin gelişmesi ve İnternetin kullanım alanlarının genişlemesiyle hızla büyümektedir.

Bu çalışma dünyanın en önemli sorunlarından bir tanesi olmaya aday olan İnternet erişiminin engellenmesi ve İnternete uygulanan sansür konusunda dünya ülkelerinde ortaya konan farklı yaklaşımlarla ülkemizdeki hukuki altyapıyı ve uygulamaları karşılaştırmaktadır. İnternet modern hayatı sarmaladıkça ortaya yeni sorunlar çıkmaktadır. Çalışmada bu sorunların, toplum hayatının olmazsa olmazı haline gelmiş bir olgusu olan kitle iletişim araçlarının ve esasında İnternetin erişim engelleme yoluyla kontrol edilmesi sorgulanmaktadır. Temel hak ve özgürlüklere zarar vermeden ve bahsettiğimiz "kontrol"ün teknik olarak toplumu etkileyen yan etkilerinin, günümüz teknolojisinin sunduğu imkânlar da kullanılarak, en aza indirilmesi için öneriler getirilmektedir. Dünya ülkelerinde ve ülkemizde uygulanmakta olan farklı erişim engelleme teknikleri ve bu tekniklere karşı geliştirilmiş popüler engelleme aşma yöntemleri detaylarıyla incelenerek, otoriteler bakımından uygulanan engelleme tekniklerinin ne ölçüde etkili olduğunun analizi - istatistiksel verilerin de yardımıyla – yapılmaktadır. Ayrıca ülkemizde sıklıkla kullanılan engelleme aşma yöntemleri ve engelleme aşma araçları saptanıp bu yöntem ve araçların ortaya çıkardığı bilgi güvenliği riskleri ve bu risklerin gerçek olması durumunda yaşanması muhtemel veya yaşanmakta olan maddi – manevi kayıplara dikkat çekilmektedir. Çalışma, temel insan hak ve özgürlüklerini minimal düzeyde kısıtlayan, daha olgun bir İnternet toplumunun oluşması için gerekli düzenleme ve uygulamalar için bir takım çözüm önerileri ile son bulmaktadır.

---

[1] ARPANET ile ilgili ayrıntılı bilgi için bkz. İnternetin Ortaya Çıkışı (sf. 3).
[2] Birth of the Internet, http://library.thinkquest.org/27887/gather/history/internet.shtml.
[3] Mehmet Bedii Kaya, Teknik ve Hukuki Boyutlarıyla İnternete Erişimin Engellenmesi, 5651 Sayılı Kanun ve Dünya Uygulamaları, 1. Baskı, İstanbul 2010, a.g.e. s.16.

§2. İNTERNET

I. İnternet Nedir?

Bilginin bir yerden bir yere taşınması problemine telefon ve telgrafın icadından önce fiziksel transfer yoluyla çözüm getirilmekteydi. Telgraf sistemlerinin bilgi transfer etmek amacıyla kullandığı Morse alfabesi bilgisayarlar gibi ikilik sayma sistemine dayanır; uzun ve kısa sinyallerden oluşan ileti dizisi konuşma diline çevrilerek bilgi iletilmiş olur. 1844 yılında Washington, D.C. ile Baltimore, Maryland arasına ilk telgraf hattının çekilmesi[4] ve sonrasında 1876 yılında[5] telefonun icadıyla bilgi dolaşımı yer ve zamandan bağımsız bir hâl almıştır. Telefonun kullanılmaya başlanması ile bilgi artık ses formatında da taşınmaya başlamıştır. İlk bilgisayarın 1942 yılında[6] yapılması ve bilgisayarda veri saklama ve veri işleme teknolojilerinin hızla gelişim göstermesiyle kütüphaneler dolusu bilgiyi tek bir bilgisayarda saklamak mümkün hâle gelmiştir. Bilgisayarların zaman içinde büyük boyutlarda veri saklama kabiliyeti kazanacağı ve saklanan bilginin bir bilgisayardan diğerine aktarılmasının bir ihtiyaç haline geleceği aşikârdı. Bilgisayar ağlarının ortaya çıkması ve nihayetinde gelişmesiyle tüm dünyayı saran devasa bir bilgisayar ağı oluşturulmuş oldu. Bilgisayar ağları vasıtasıyla bilginin iletimi zamandan ve mekândan bağımsız hale gelince "sanal bir bilgi düzlemi"[7] ortaya çıkmıştır. İnternet, sanal bilgi düzlemi olgusunun somutlaşmış halidir.

Fiberoptik[8] kablo sistemlerinin ülkelerin İnternet altyapılarında kullanımının yaygınlaşmasıyla gigabyte'larca veri saniyeler içinde dünyanın bir ucundan diğer ucuna iletilebilmektedir. Bu gelişmeler sonucunda bilgi bugün İnternet üzerinden yazılı, sesli ve görüntülü olarak rahatlıkla iletilebilmektedir. Ayrıca holografik görüntüler[9] de İnternet üzerinden çok hızlı şekilde iletilebilmektedir. Tüm bunların ötesine de geçilerek elektronik ortamda kokunun iletimine yönelik çalışmalar yapılmakta ve bu kısmen başarılmaktadır. Bu çalışmalar olgunlaştığında, belki de insanlara telefonda sevgililerinin onlar için beğendiği parfümü test etme imkânı doğacaktır. Teknoloji dünyası beş duyuyu iletebilmek yönünde ciddi adımlar atmaktadır. İçinde ekran bulunduran gözlüklerle ve vücuda bağlanan bazı aparatlarla televizyon seyrederken dokunma duyusu da kısmen iletilebilmektedir.[10] Belki de bir gün, büyük boyutlarda bilgi 1'ler ve 0'lar formatında saniyeler içinde dünyanın herhangi

---

[4] Morse Code & the Telegraph, http://www.history.com/topics/telegraph

[5] The Telephone, http://web.mit.edu/invent/iow/graham_bell.html.

[6] Roger Munns, First-computer controversy finally nearing a conclusion, http://www.scl.ameslab.gov/ABC/Articles/First-computer.html.

[7] İbrahim Emre Bayamlıoğlu, Fikir ve Sanat Eserleri Hukukunda Teknolojik Koruma, İstanbul 2008, a.g.e., s.38.

[8] Fiberoptik kablolar, kendi boyunca ışığın yönlendirilebildiği plastik veya cam liflerden oluşmuş kablolardır. Bu kablolar diğer iletişim malzemelerine oranla çok daha hızlı veri iletimine imkân sağlamaktadırlar. (Bkz. http://tr.wikipedia.org/wiki/Fiberoptik).

[9] Lazer ışınlarını kullanarak üç boyutlu görüntü işlemeye holografi denir. Bu teknikle bir cismin uzaydaki konumu, şekli, görüntüsü vb. bilgiler lazer ışınlarıyla elde edilip depolanır ve bu bilgiler uzaktaki bir lokasyona kayıpsız iletilerek cismin üç boyutlu görüntüsü elde edilmiş olur.

[10] Zakir Avşar/Gürsel Öngören, Bilişim Hukuku, İstanbul 2010, a.g.e., s.17.

bir yerine iletilebileceği gibi nesneler, hatta insanlar da fiziksel olarak istenilen yere saniyeler içinde ışınlanabilecek ve belki bunun için de İnternet kullanılıyor olacaktır.

İnternetin ortaya çıktığı dönemdeki ve günümüzdeki teknolojik konjonktür nazara alınarak gelişiminden bahsedildikten ve mevcut gelişmeler ve bilimsel çalışmalar ışığında gelecek tahmini yapıldıktan sonra İnternetin kullanım amaçları konusuna değinilecektir. İnternetin ayrıntılı tarihçesi ve teknik altyapısı ile ilgili yeterli bilimsel çalışmalar ve eserler bulunmakta olduğundan bu konuya kısaca değinilecektir.

II. İnternetin Ortaya Çıkışı

İnternetin ortaya çıkışı Amerika Birleşik Devletleri (ABD) tarafından geliştirilen bir askeri projeye dayanır. 1957 yılında ABD, dünyanın çeşitli yerlerine yerleştirilmiş savaş sistemlerini bir bilgisayar ağı üzerinden kontrol edebilmek için birbirinden bağımsız bilgisayarları birbirine bağlayarak bir ağ oluşturmuştur. Projeyi yürütmek için ABD Savunma Bakanlığı'na bağlı ARPA (Advanced Research Projects Agency) adında bir birim oluşturulmuş ve oluşturulan bilgisayar ağına da ARPANET (Advanced Research Projects Agency Network) adı verilmiştir. Bu ağ üzerinden ilk bilgi transferi 1969 yılında gerçekleştirilmiştir. Bu ağdaki bilgisayarların aynı dili konuşması, yani birbirlerine gönderdikleri verilerin alıcı taraflarda anlamlandırılabilmesi için de TCP/IP adı verilen bir protokol[11] tasarlanmış ve yazılımı geliştirilmiştir[12]. Nihayetinde bu ağa bağlanan bilgisayar sayısı arttıkça ABD ordusu bu ağdan ayrılarak kendi ağını oluşturmuş ve bu ağın sivilleşmesini sağlamıştır. Sonuç olarak TCP/IP protokolüne dayanan ve hızla büyüyen bir bilgisayar ağı oluşmuş ve "İnternet" olarak adlandırılmıştır.

III. İnternetin Kullanım Alanları

20. ve 21. yüzyıla damgasını vuran bir buluş olan İnternet günümüzün en etkili iletişim araçlarından biri olmuştur. Birer kişisel iletişim aracı olan cep telefonları bile bugün İnternet ortamına entegre olmuştur. İnternet erişimi cep telefonu operatörlerinin sunmuş olduğu en temel hizmetlerinden biri olmuştur. Sosyal paylaşım sitelerinin ortaya çıkması ve yaygınlaşmasıyla iletişim kavramı farklı bir boyuta taşınmıştır. Sosyal paylaşım siteleri, günlük sayfaları (bloggerlar) ve kullanıcılarına daha etkileşimli arayüzler sunan web siteleri sayesinde kullanıcıların daha aktif rol aldıkları "Web 2.0" kavramı ortaya çıkmıştır. Yani yayıncılığın televizyon ve gazetelerden ibaret olduğu dönemlerdeki gibi kullanıcıların sadece kendilerine sunulanı aldığı ve yayımlanan içerik üzerinde hiçbir ekleme ve değişiklik yapamadığı dönem sona ermiştir. Artık İnternet kullanıcıları tarafından okunan gazetelerin

[11] Bir bilgisayar bilimleri kavramı olarak protokol, elektronik aygıtlar arasında iletişimin sağlanabilmesi için uyulması gereken kurallar dizisidir.
[12] Avşar/Öngören, a.g.e., s.30.

web sitelerinde yayımlanan haberlere yorumlar yazılabilmekte, bloglarda (online günlüklerde) yayımlanan yazılar gazetelerin web sayfalarında yayımlatılabilmektedir. Böylece İnternet milyonlarca kullanıcının içeriğinin oluşumuna katkı sağladığı bir sanal ortam haline gelmiştir. Google'ın ortaya çıkmasıyla bilgi paylaşımında bir devrim yaşanmıştır. Bilgi paylaşımının eskiye oranla çok hızlanmış olması sayesinde paylaşılan ve üretilen bilgi miktarı da eksponansiyel bir artış göstermiştir. İnternetin son 10 yılda göstermiş olduğu tüm gelişmeler İnterneti vazgeçilmez ve bir o kadar da kontrol edilmesi hayati önem taşıyan bir ortam haline getirmiştir.

A. İnternetin Olumlu ve Kamu Yararına Faaliyetlerde Kullanımı

İnternet teknik bir arıza ya da aksaklık olmadığı sürece 7 gün 24 saat kullanımımıza açık bir ortamdır. İnternet kullanılarak uzaktaki insanlara eposta gönderilebilmekte, anlık mesajlaşılabilmektedir. Ayrıca uzaktaki bilgisayarlara dosya transferi de yapılabilmektedir. İnternet her türlü bilginin kaynağı haline gelmiştir. Doğru ve güvenilir bilgi kaynakları kullanılarak her türlü bilgiye hızlı ve kolayca erişmek mümkündür. Aranılan her türlü yazılıma ücretli ya da ücretsiz olarak erişmek mümkün olup İnternetten her türlü ihtiyacımıza cevap verecek şekilde alış veriş yapılabilmektedir. İnternet ayrıca her türlü eğitim faaliyeti için de kullanılabilmektedir. Zira uzaktan eğitim kavramı gittikçe popülerleşmektedir. İnsanlar evlerinde bilgisayar karşısında İnternetten gerçek zamanlı yayımlanan ve aktif katılım imkânı sunan dersleri takip ederek lisans, yüksek lisans ve doktora eğitimlerini tamamlayabilmektedirler. Ayrıca İnternet üzerinden havale, EFT ve benzeri işlemler yoluyla kilometrelerce uzaktaki lokasyonlara para göndermek mümkün hale gelmiş olduğundan hem alış verişler çok kolaylaşmış olup, hem de - paranın fiziksel olarak taşınması ihtiyacının ortadan kalkması ile – insanların zaman ve paradan tasarruf etmeleri neticesinde hayat standartları yükselmiştir. İnternetin kullanım amaçlarına her geçen gün yenileri eklenmektedir. Bu yüzden bu konuyu daha fazla detaylandırmadan İnternetin art niyetli kullanım amaçlarına değinmek yerinde olacaktır.

B. İnternetin Olumsuz ve Kamuya Zarar Veren Faaliyetlerde Kullanımı

İnternet, sanal ve kimlik gizlemenin kolay olduğu bir ortam olduğundan dolayı, en başta terör örgütleri olmak üzere art niyetli insanların yoğun bir şekilde suça alet ettikleri bir ortamdır. Bu yüzden İnternetin denetimi ihtiyacı ortaya çıkmaktadır. Nasıl ki fiziksel ortamda kolluk kuvvetleri güvenliği sağlıyorsa, İnternetin de kolluk kuvvetleri olması sanal ortamın güvenliği için gerekli görülebilir. Ama bu denetimin ölçüsü tartışmalıdır. Dünya genelinde henüz sınırları çizilememiştir. Teknolojik gelişmelerin hızına bakıldığında bu sınırlar her gün daha karışık bir hâl almaktadır.

1. Terör Örgütlerinin İnternetteki Faaliyetleri

Terör örgütleri hayatiyetlerini propaganda ile sürdürürler. Propaganda örgütlerin hem amacı, hem aracıdır. İnternet propagandanın en ucuz ve kolay yoludur. Zira örgütler İnternet vasıtasıyla seslerini dünyanın her noktasına kolayca ulaştırabilmektedirler. Terör örgütleri İnternet üzerinden yayımladıkları bazı materyallerle de üyelerini ve sempatizanlarını eğitmektedirler. Bomba yapımından silah kullanımına ve polis takibinden nasıl kurtulabileceklerine kadar birçok konuda bilgiyi İnternet üzerinden üyelerine ve sempatizanlarına ulaştırmaktadırlar.[13]

İnternetin terör örgütlerine sunduğu önemli avantajlardan biri de hızlı ve etkin haberleşme imkânıdır. Teknolojiyi yakından takip eden terör örgütleri eylemlerini İnternet üzerinden organize ederek polis takibini zorlaştırmaktadır. Ayrıca iletilerini kendi içlerinde geliştirdikleri kripto algoritmalarıyla şifreleyerek birbirlerine gönderdikleri mesajların güvenlik güçleri tarafından çözülmesini de zorlaştırmaktadırlar. Örgüt elemanlarının haberleşmesi bu kadar hızlı olunca güvenliğin sağlanması da hızlı ve sürekli takibi gerektirmektedir.

Terör örgütleri İnternetten saldırı hedefleriyle ilgili bilgileri çok kısa zamanlarda ve ucuz yöntemlerle elde edebilmektedirler. Ayrıca günümüzde örgütlerin hedefinde sadece fiziksel hedefler bulunmamaktadır. Teröristler örgütsel ya da kişisel olarak, zarar vermek istedikleri hedeflerine sanal ortamda da zarar vermeye çalışmakta, özellikle devletlerin İnternet ortamındaki kritik seviyedeki bilgi sistemlerine saldırarak bu bilgileri dışarıya sızdırmaktadırlar.

Terör örgütleri düşman olarak belirledikleri ülkelere sıklıkla siber saldırılar gerçekleştirmektedirler. Bu ülkelerden bir tanesi de ABD'dir. Zira El Kaide terör örgütüyle başı belada olan ABD, Mayıs 2011'de Uluslararası Siberalan Stratejisi (International Strategy For Cyberspace)[14] adıyla yayımladığı politikasında ülkeye yönelik siber ortamda gerçekleştirilecek her türlü saldırganlığa karşı gereken cevabın verileceğini ve bu tür davranışlara müsamaha gösterilmeyeceğini belirtmiştir. Verilecek cevaplar arasında askerî harekâtın da bir seçenek olduğu vurgulanmaktadır[15].

2. Çocukların Cinsel İstismarı

Pornografi kavramı, İnternetin yaygınlaşmasıyla sıkça tartışılmaya başlanmış ve pornografik içeriğin düzenlenmesi İnterneti ilgilendiren en tartışmalı konulardan biri

---

[13] Terör Örgütlerinin İnternet Ortamında Yürüttüğü Faaliyetler, http://www.caginpolisi.com.tr/20/41-43.htm#_ftn5.

[14] Politika belgesinin tam ve orijinal metni için bkz. http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

[15] Çağdaş Aru, ABD Yönetiminden Gözdağı: Ülkeye Yönelik Hack Saldırıları Askeri Bir Harekatla Sonuçlanabilir, http://www.turk.internet.com/portal/yazigoster.php?yaziid=32472, 20 Mayıs 2011.

olmuştur[16]. Çünkü pornografinin ya da müstehcenliğin sınırlarını belirlemek oldukça zordur, hatta imkânsızdır. Ancak çocuk pornografisinde sınırlar birçok ülkeye göre çok nettir. Çünkü burada konu çocuktur ve eylemin suç olduğu dünyada birçok ülkeye göre suç olarak kabul edilmektedir. Çocuk pornografisi ulusal ve uluslar arası düzeyde çocuk haklarını ihlal eden önemli bir suçtur. İnternet kullanımının yaygınlaşmasıyla bu tür suçlar sanal ortama taşınmış ve çocuk pornografisi küresel anlamda bir sektör haline gelmiştir. Bu tür suçlarla mücadelede ulusal ve uluslararası çalışmalar bulunmaktadır. Çünkü suça konu olan çocuklar olunca bu suçlarla mücadele ayrı bir ehemmiyet kazanmaktadır. Zira bu tür suçlara maruz kalan çocuklar psikolojik, ruhsal ve fiziksel bozukluklar yaşamaktadırlar ve bu açıkça çocukların haklarının ihlali anlamına gelmektedir.[17]

Çocukların cinsel istismarı ile mücadelede uluslar arası işbirliği kaçınılmaz olduğundan, Birleşmiş Milletler Çocuk Hakları Anlaşması (UN Convention on the Rights of the Child (CRC)) Ek Protokolünde (UN, 1989) çocuk pornografisinin uluslararası tanımı yapılmıştır. Çocuk pornografisi *"Ne sebeple olursa olsun temelinde cinsel bir niyetle, bir çocuğun cinsel uzuvlarının herhangi bir şekilde teşhiri veya çocuğu gerçekte veya öyleymiş gibi cinsel faaliyet içerisinde gösterme."* şeklinde tanımlanmaktadır. Çocuk kavramının ve hangi yaş aralıklarının çocuk kavramına dâhil olduğunun tanımları ülkelere göre değişiklik gösterdiğinden, çocuk pornosuyla uluslararası çapta mücadelede uluslararası tanım gereklidir.[18] Çocuk pornografisine bir uluslararası tanım da İnterpol Çocuklara Karşı İşlenen Suçlar Uzman Grubu tarafından yapılmıştır. Tanımda, "*Çocuk pornografisi; çocuğun kötüye kullanımı veya cinsel istismarı sonucu oluşmaktadır. Çocuğun cinsel davranışları ve uzuvlarına odaklanmış yazılı ve sesli materyallerin kullanımı da dâhil, çocuğun cinsel istismara yöneltilmesi veya betimlemesi anlamındadır.*"[19] denmektedir. Bir tanım da Avrupa Konseyi'nin Bilişim Suçları Sözleşmesi'nde (EC, 2001), "*Çocuk pornografisi, bir küçüğün cinsel olarak kullanılmasını, küçük gibi görünen bir kişinin cinsel olarak kullanılmasını, bir küçüğü temsil eden gerçekçi bir imajın cinsel olarak kullanılmasını görsel olarak içeren pornografik materyaldir."*[20] şeklinde yer almaktadır.

a) Cinsel Çocuk İstismarının Uluslararası Hukukta Yeri

İnternetin yaygınlaşmasıyla uluslararası bir hüviyete bürünen çocuk pornografisi suçuyla ancak uluslararası anlaşmalar ve kanunlarla mücadele edilebilir. Bu doğrultuda, uluslararası anlaşmalarda çocukların cinsel istismarını suç olarak kabul eden ve taraf ülkelerin

---

[16] Akdeniz, Yaman "Governance of Pornography and Child Pornography on the Global Internet: A Multi-Layered Approach," in Edwards, L and Waelde, C eds, Law and the Internet: Regulating Cyberspace, Hart Publishing, 1997, s. 223-241.

[17] Yusuf Uzunay/Mustafa Koçak, İnternet Üzerinden Çocuk Pornografisi Ve Mücadelede Yaşanan Sıkıntılar, Turkish Journal of Police Studies, Vol: 7 Issue:1, pp.97-116, 2005.

[18] Semih Dokurer, Bilişim Suçları Laboratuvarlarında Çocuk Pornografisi İncelemeleri, Adli Tıp Kurumu, http://www.dokurer.net/files/documents/ChildpornExamining.pdf.

[19] Dokurer.

[20] Convention on Cybercrime, Budapest, 23 November 2001, http://conventions.coe.int/treaty/en/treaties/html/185.htm.

bu konuda almaları gereken önlemleri vurgulayan maddeler yer almaktadır. Örneğin, CRC 34. maddede şu ifadeler yer almaktadır:

"*Taraf Devletler, çocuğu, her türlü cinsel sömürüye ve cinsel suiistimale karşı koruma güvencesi verirler. Bu amaçla Taraf Devletler özellikle:*

a) Çocuğun yasadışı bir cinsel faaliyete girişmek üzere kandırılması veya zorlanmasını;

b) Çocukların, fuhuş, ya da diğer yasadışı cinsel faaliyette bulundurularak sömürülmesini;

c) Çocukların pornografik nitelikli gösterilerde ve malzemede kullanılarak sömürülmesini, önlemek amacıyla ulusal düzeyde ve ikili ile çok taraflı ilişkilerde gerekli her türlü önlemi alırlar."

CRC 19. maddede ise: "*Bu Sözleşmeye Taraf Devletler, çocuğun anne-babasının ya da onlardan yalnızca birinin, yasal vasi veya vasilerinin ya da bakımını üstlenen herhangi bir kişinin yanında iken bedensel saldırı, şiddet veya suiistimale, ihmal ya da ihmalkâr muameleye, ırza geçme dâhil her türlü istismar ve kötü muameleye karşı korunması için; yasal, idari, toplumsal, eğitsel bütün önlemleri alırlar*." ifadesi yer almaktadır.

Ayrıca Avrupa Konseyi tarafından yayımlanan Bilişim Suçları Sözleşmesi 9. maddede Çocuk Pornografisi İle Bağlantılı Suçlar başlığıyla aşağıdaki maddelere değinmiştir:

"*Her bir Taraf devlet, bir hak olmaksızın kasıtlı*

a) bilgisayar sistemi vasıtasıyla dağıtmak amacıyla çocuk pornografisi üretmek,

b) bilgisayar sistemi vasıtasıyla çocuk pornografisini temin edilebilir hale getirmek veya göstermek,

c) bilgisayar sistemi vasıtasıyla çocuk pornografisini aktarmak veya dağıtımını yapmak,

d) kendisi veya başkası için bilgisayar sistemi vasıtasıyla çocuk pornografisi temin etmek,

e) bir bilgisayar sisteminde veya bilgisayar veri depolama ortamında çocuk pornografisine sahip olmak

Fiillerinden sorumlu tutulması için gerekli kanuni düzenlemeyi yapmalı ve ihtiyaç duyulan önlemleri almalıdır."

25/10/2007 tarihinde Lanzarote'de imzalanan ve amaçları 1. maddesinde,

"*1- Bu Sözleşmenin amaçları:*

a) Çocukların cinsel sömürüsü ve istismarım engellemek ve bunlarla mücadele etmek;

b) Cinsel sömürü ve istismara maruz çocuk mağdurların haklarını korumak;", olarak belirtilen Avrupa Konseyi Çocukların Cinsel Sömürü ve İstismara Karşı Korunması Sözleşmesi'ne[21] Türkiye'de 2011 yılında taraf olmuştur[22].

b) Cinsel Çocuk İstismarının Türk Hukuku'ndaki Yeri

Türkiye CRC'yi ek protokolleriyle birlikte imzalayarak kabul etmiştir. Dolayısıyla yukarıda üzerinde durduğumuz maddelerde yasaklanan fiiller ülkemizde de yasaklanmış olmaktadır. Ancak 2004 yılına kadar Türk Ceza Kanunu'nda (TCK) (765 Sayılı yürürlükten kaldırılan TCK) çocuk pornografisini hedef alan bir madde bulunmamaktaydı. 26.09.2004 tarihinde 5237 sayılı Yeni TCK'nın kabulü ile 103. ve 226. maddelerde cinsel çocuk istismarı – yine TCK'nın 6. maddesinin b bendine göre, Çocuk deyiminden; henüz onsekiz yaşını doldurmamış kişi anlaşılmak üzere – aşağıdaki ifadelerle suç olarak yer bulmuştur:

103. maddede; "*Çocuğu cinsel yönden istismar eden kişi, üç yıldan sekiz yıla kadar hapis cezası ile cezalandırılır. Cinsel istismar deyiminden;*

a) Onbeş yaşını tamamlamamış veya tamamlamış olmakla birlikte fiilin hukukî anlam ve sonuçlarını algılama yeteneği gelişmemiş olan çocuklara karşı gerçekleştirilen her türlü cinsel davranış,

b) Diğer çocuklara karşı sadece cebir, tehdit, hile veya iradeyi etkileyen başka bir nedene dayalı olarak gerçekleştirilen cinsel davranışlar, anlaşılır." ifadeleriyle, "müstehcenlik" başlığı altındaki 226. maddedeki; "*1. a) Bir çocuğa müstehcen görüntü, yazı veya sözleri içeren ürünleri veren ya da bunların içeriğini gösteren, okuyan, okutan veya dinleten,*

b) Bunların içeriklerini çocukların girebileceği veya görebileceği yerlerde ya da alenen gösteren, görülebilecek şekilde sergileyen, okuyan, okutan, söyleyen, söyleten,

c) Bu ürünleri, içeriğine vakıf olunabilecek şekilde satışa veya kiraya arz eden,

d) Bu ürünleri, bunların satışına mahsus alışveriş yerleri dışında, satışa arz eden, satan veya kiraya veren,

[21] Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, http://conventions.coe.int/Treaty/EN/treaties/Html/201.htm

[22] 6084 Sayılı Avrupa Konseyi Çocukların Cinsel Sömürü Ve İstismara Karşı Korunması Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun, RG., Sayı: 27781, Tarih: 10.12.2010.

e) Bu ürünleri, sair mal veya hizmet satışları yanında veya dolayısıyla bedelsiz olarak veren veya dağıtan,

f) Bu ürünlerin reklamını yapan,

Kişi, altı aydan iki yıla kadar hapis ve adlî para cezası ile cezalandırılır.

2. Müstehcen görüntü, yazı veya sözleri basın ve yayın yolu ile yayınlayan veya yayınlanmasına aracılık eden kişi altı aydan üç yıla kadar hapis ve beşbin güne kadar adlî para cezası ile cezalandırılır.

3. Müstehcen görüntü, yazı veya sözleri içeren ürünlerin üretiminde çocukları kullanan kişi, beş yıldan on yıla kadar hapis ve beşbin güne kadar adlî para cezası ile cezalandırılır. Bu ürünleri ülkeye sokan, çoğaltan, satışa arz eden, satan, nakleden, depolayan, ihraç eden, bulunduran ya da başkalarının kullanımına sunan kişi, iki yıldan beş yıla kadar hapis ve beşbin güne kadar adlî para cezası ile cezalandırılır.

4. Şiddet kullanılarak, hayvanlarla, ölmüş insan bedeni üzerinde veya doğal olmayan yoldan yapılan cinsel davranışlara ilişkin yazı, ses veya görüntüleri içeren ürünleri üreten, ülkeye sokan, satışa arz eden, satan, nakleden, depolayan, başkalarının kullanımına sunan veya bulunduran kişi, bir yıldan dört yıla kadar hapis ve beşbin güne kadar adlî para cezası ile cezalandırılır.

5. Üç ve dördüncü fıkralardaki ürünlerin içeriğini basın ve yayın yolu ile yayınlayan veya yayınlanmasına aracılık eden ya da çocukların görmesini, dinlemesini veya okumasını sağlayan kişi, altı yıldan on yıla kadar hapis ve beşbin güne kadar adlî para cezası ile cezalandırılır." ifadeleri her türlü cinsel çocuk istismarını suç saymakla birlikte 3. Fıkradaki "*Müstehcen görüntü, yazı veya sözleri içeren ürünlerin üretiminde çocukları kullanan kişi*" ifadesiyle özellikle İnternet üzerinden çocuk pornosu içeriği üretenler hedef alınmıştır. Ayrıca, 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'un 8. maddesinin 1. fıkrasında "*İnternet ortamında yapılan ve içeriği aşağıdaki suçları oluşturduğu hususunda yeterli şüphe sebebi bulunan yayınlarla ilgili olarak erişimin engellenmesine karar verilir:*" ifadesinden sonra a bendinin 2. maddesinde TCK'nın 103. maddesine atıfta bulunularak çocukların cinsel istismarı suçlarının İnternette erişim engelleme sebebi olduğu belirtilmektedir.

3. Bilgisayar Virüsleri, İstenmeyen E-postalar (SPAM), Hacking, Phishing

Bilgisayar virüsü ya da diğer bir deyişle kötücül yazılım, bir bilgisayarda ya da bilgisayar sisteminde, bilgisayar kullanıcısının ya da sistem yöneticisinin bilgisi ya da izni dışında sistemde bulunabilen, sistemde kendini izinsiz çalıştırabilen ve çoğaltabilen,

bilgisayarın çalışma şeklini değiştirebilen ya da bulunduğu bilgisayar sisteminden dışarıya bilgi sızdırabilen her türlü bilgisayar programına verilen addır. İnternet, virüslerin en hızlı ve en kolay yayılma imkânı bulduğu ortamdır. Virüsler üzerinde çalıştıkları sistemin çalışma şeklini değiştirerek (sistem bellek kullanımını ya da diğer kaynakların kullanımını artırarak ya da sistem dosyalarına zarar vererek) o sistemi işlemez hale getirebilir ve sistem üzerindeki bilgileri erişilemez durumda bırakabilirler. Virüsler için geliştirilmiş kesin bir çözüm yolu bulunmamakta ve her geçen gün yeni virüs türleri ortaya çıkmaktadır.

Geniş kitlelere İnternet üzerinden hizmet veren sistemlere DDoS[23] atağı düzenlenerek, bu sistemlerin hizmet vermesine engel olunabilmektedir. Bu tür saldırılar da saldırganların virüs bulaştırarak "zombi"leştirdikleri[24] bilgisayarlar üzerinden yapılmaktadır. Saldırganlar, virüs bulaştırdıkları yüzlerce, binlerce ve hatta bazen yüz binlerce bilgisayarı hedeflerine yönlendirip aynı anda hizmet talebinde bulundukları zaman hedefteki sistem anlık kullanıcı sayısı üst sınırına ulaştığından hizmet vermesi gereken kullanıcıların taleplerine karşılık veremeyecek hale gelmektedir. Özetle, DDoS saldırıları, bilgi güvenliği bileşenlerinden erişilebilirliği (availability) hedef almaktadır[25]. DDoS saldırıları en yaygın erişim engelleme saldırılarından biridir. Zira ülkemizde de, DDoS saldırıları istatistiklere ve bilgi güvenliği uzmanlarının görüşlerine göre virüslerle birlikte siber tehditler sıralamasında ilk 2 sırayı paylaşmaktadır[26]. Ayrıca DDoS atakları bazen devletlerin de – yasadışı olduğu aşikâr da olsa

[23] DDoS (Distributed Denial of Service), bir bilişim sisteminin erişilebilirliğini hedef alan en etkili yöntemlerden biridir. Öyle ki, bu tehditlerden korunmanın ne kesin bir yolu, ne de sistemleri bu tehditten koruyabildiğini iddia edebilen yazılımlar mevcuttur.

[24] Zombi kavramı kısaca, virüs vb. kötücül bir yazılım vasıtasıyla, internet ağında kötücül yazılımın kaynağı olan bilgisayarın emrine girmiş ve bu bilgisayarın komutlarıyla yönlendirilen bilgisayar olarak tanımlanabilir.

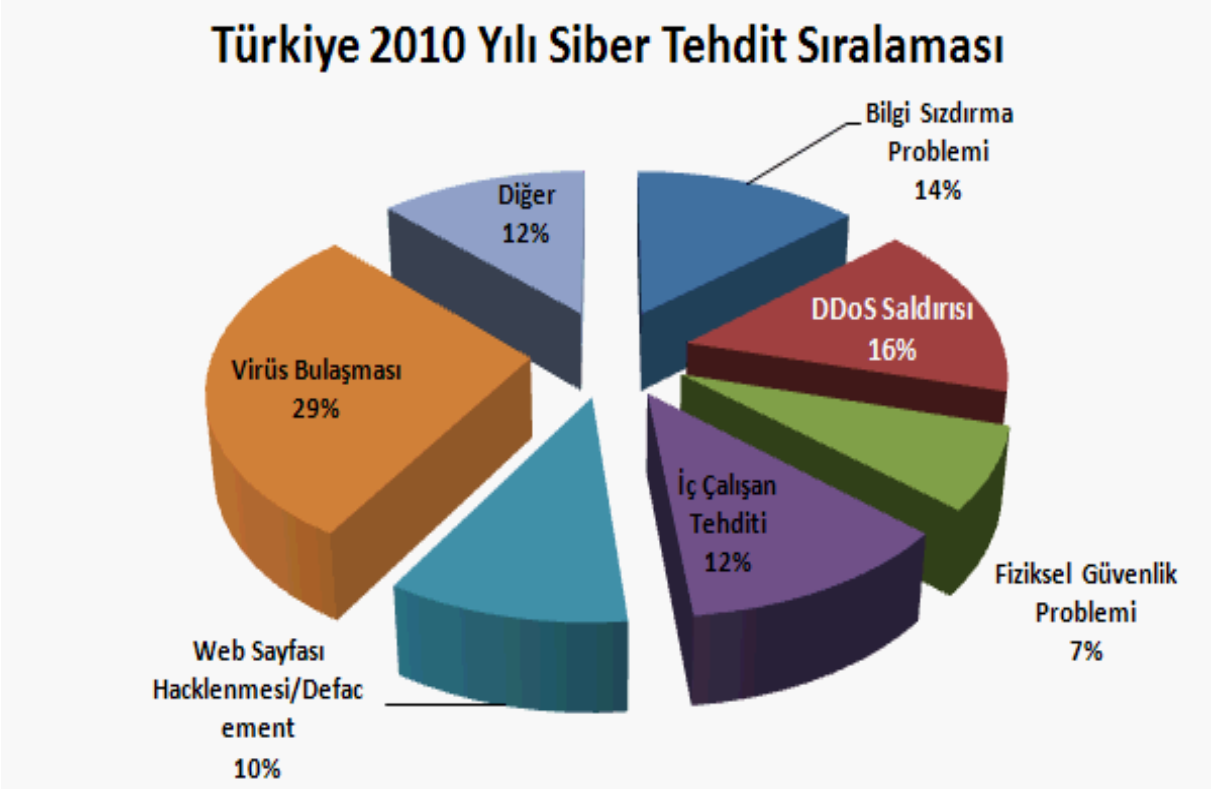
[25] Türkiye 2010 Yılı DDoS Raporu, http://blog.lifeoverip.net/2011/02/20/turkiye-2010-yili-ddos-raporu/.

[26] Bilgi Güvenliği Akademisi (BGA) tarafından 2010 yılında yapılmış olan ve 600 bilgi güvenliği uzmanının katılmış olduğu "2010 Yılı Türkiye Siber Tehditler Sıralaması" anketinin sonuçlarına göre aşağıdaki gibi bir siber tehdit dağılımı ortaya çıkmış olup virüslerden sonra en önemli tehdidin DDoS saldırıları olduğu görülmektedir. (Kaynak: www.bga.com.tr)

– başvurduğu bir erişim engelleme yöntemidir. Örneğin, Kırgızistan'daki Şubat 2005 genel seçimleri süresince devlet tarafından tüm muhalif partilerin İnternet siteleri DDoS atağına maruz bırakılmıştır. Bu yöntemle devlet muhalif partilerin seçim süreci boyunca propaganda yapmalarını engellemiştir.[27]

Siber tehditler genellikle birbiriyle sıkı sıkıya ilişkilidir. Bir tehdidin ortaya çıkmasına neden olan güvenlik zafiyeti çoğu zaman beraberinde başka tehditleri de getirir. Mesela SPAM[28] olarak bilinen istenmeyen epostaların gönderilmesinde zombi bilgisayarların önemli katkısı söz konusudur. Zombiler 2005 yılında dünya üzerinde gönderilen tüm SPAM'lerin %50 - %80 kadarının gönderilmesi amacıyla kullanılmışlardır[29]. Yani her hangi bir bilgisayar kullanıcısının bilgisayarına bulaşmış bir virüs aracılığıyla ya da o bilgisayardaki güvenlik açıklıkları vasıtasıyla, farkında olmadan o kullanıcı bir DDoS saldırısına katkıda bulunmuş olabilir. Belki de, virüs bulaşmış o bilgisayar birçok insanı rahatsız eden SPAM'lerin gönderilmesinde kullanılmış olabilir.

SPAM tehdidi beraberinde birçok farklı tehdidi getirmektedir. Eposta kutusuna gelen bir SPAM, İnternet kullanıcısını Phishing sitesi diye adlandırılan sitelere yönlendirebilir. Phishing basit bir ifadeyle, İnternet kullanıcılarının dolandırıcılık sitelerine yönlendirilmesi tekniğidir[30]. En basit örneğiyle, eposta kutunuza gelmiş, sayfa tasarımı itibariyle müşterisi olduğunuz bankanın İnternet şubesinin tasarımıyla birebir aynı içerikte bir epostayı kimden



[27] Ronald Deibert/John Palfrey/Rafal Ronozinski/Jonathan Zittrain, Access Denied: The Practice and Policy of Global Internet Filtering, Massachusetts 2008, a.g.e., s.41.
[28] SPAM, çoğunlukla reklam içerikli olan, çok sayıda alıcıya ulaştırılan istenmeyen eposta olarak tanımlanabilir.
[29] Tom Spring, Spam Slayer: Slaying Spam-Spewing Zombie PCs, PC World, 2005-06-20.
[30] Rachna Dhamija/J. D. Tygar/Marti Hearst, Why phishing works, Proceedings of the SIGCHI conference on Human Factors in computing systems, April 22-27, 2006, Montréal, Québec, Canada.

geldiğine çok dikkat etmeden okuyup değerlendirmeniz halinde phishing tuzağına düşmüş olursunuz. En popüler haliyle, bu eposta size bazı güvenlik bilgilerinizi güncellemeniz gerektiğini bildirecek ve müşteri numaranızı, parolanızı, vs. girmenizi isteyecek ve eposta içeriğindeki butona tıkladığınızda sizi kendi sayfasına yönlendirecek ya da nihayetinde bu epostayı size gönderenin ulaşmak istediği bilgiler olan güvenlik bilgilerinizi bir form aracılığıyla kendi veritabanına ya da eposta adresine kolaylıkla yönlendirecektir.

İnternet kullanıcıları için en büyük tehlikelerden biri de, Türkçeye sanal korsanlık olarak geçmiş olan hacking kavramıdır. Aslında yukarıda saymış olduğumuz tehlikelerin tamamı birer hacking eylemidir. Ancak özellikle bir kullanıcının eposta adresine ait parolayı, İnternet banka şubesine girişte kullandığı özel bilgilerini ele geçirmek ya da bir bilgisayar sistemine sızmak için özel yöntemler geliştiren kişiler hacker (bilgisayar korsanı) diye adlandırılmaktadır. Mesela bir hacker seçtiği kurbanına keylogger adı verilen bir programcık göndererek, kurbanının bilgisayarında klavyesine yapmış olduğu her dokunuşu takip edebilir ve bu yolla kurbanının kullanıcı adı, parola, vb. bilgilerini elde edebilir. Bilinen çok sayıda hacking yöntemi olup her geçen gün yeni yöntemler geliştirilmektedir.

4. Müstehcenlik, Kumar, Fuhuş

İnternetin dünya genelinde denetimi fiziksel ortamın denetimi kadar kolay olmadığından her türlü suç ve zararlı faaliyet bu ortamda yaygın bir şekilde yürütülmektedir. İnternetin yaygınlaşmasıyla çok sayıda yasadışı kumar siteleri türemiştir. Ayrıca sanal ortamın fuhuş için teknik bir araç olarak kullanımı yaygınlaşmış hatta sosyal paylaşım siteleri bile bu işe alet edilmeye başlamıştır. Ancak zaman içerisinde güvenlik güçlerinin sanal ortam denetimini daha iyi yapabilmek amacıyla gerekli donanım ve bilgi seviyesine erişmesiyle İnternet suçluları da yakalanabilir olmuştur. Adı geçen suçlar, çalışmamıza konu olan 5651 sayılı kanunun 8. maddesinde erişim engelleme nedenlerinden bazıları olarak zikredilmiştir.

5. Fikri Hakların İhlali

Fikri hakların ihlali İnternet kullanımının yaygınlaşmasıyla çok daha kolaylaşmaktadır. Ancak Fikir ve Sanat Eserleri Hukuku İnternetin ortaya çıkmasından önce de dünya ülkeleri için önemli bir konuydu. Özellikle gelişmiş ülkeler 19. yüzyıl sonlarına doğru ulusal çapta eser koruması sağlamak amacıyla düzenlemeler yapmışlardır. Bu çalışmaların akabinde eserlerin uluslar arası çapta da korunması maksatlı olarak ülkeler birçok ikili anlaşma yapmışlardır. Bir süre sonra ikili anlaşmaların çokluğu ve birbiriyle uyumsuzluğu nedeniyle ülkeler ikili anlaşmaları ortadan kaldırarak 1886 yılında ortak bir konvansiyon imzalamışlardır. Bu konvansiyon Bern Konvansiyonu olarak bilinmektedir[31].

[31] Berne Conventionfor the Protection of Literary and Artistic Works, September 9 1886, http://www.wipo.int/treaties/en/ip/berne/trtdocs_wo001.html.

Ancak Bern Konvansiyonu, sonrasında imzalanmış pek çok uluslar arası anlaşma gibi hukuki bir eser koruması getirmemektedir. Sadece anlaşmalara taraf ülkelerin kendi iç hukuklarında uygulamaları gereken asgari bir koruma rejimi öngörmektedir[32].

Türk Hukukunda fikri haklar 5846 sayılı Fikir ve Sanat Eserleri Kanunu (FSEK) ile koruma altına alınmıştır. Bundan dolayıdır ki 5651 sayılı Kanunda fikri hakların ihlali ayrıca bir erişim engelleme sebebi olarak zikredilmemiştir. 5846 sayılı FSEK'e 2001 yılında getirilen ve 2004 yılında da değişikliğe uğrayan Ek 4. maddede, "*dijital iletim de dâhil olmak üzere işaret, ses ve/veya görüntü nakline yarayan araçlarla servis ve bilgi içerik sağlayıcılar tarafından eser sahipleri ile bağlantılı hak sahiplerinin bu Kanunda tanınmış haklarının ihlâli halinde, hak sahiplerinin başvuruları üzerine ihlâle konu eserler içerikten çıkarılır. Bunun için hakları haleldar olan gerçek veya tüzel kişi öncelikle bilgi içerik sağlayıcısına başvurarak üç gün içinde ihlâlin durdurulmasını ister. İhlâlin devamı halinde bu defa, Cumhuriyet savcısına yapılan başvuru üzerine, üç gün içinde servis sağlayıcıdan ihlâle devam eden bilgi içerik sağlayıcısına verilen hizmetin durdurulması istenir. İhlâlin durdurulması halinde bilgi içerik sağlayıcısına yeniden servis sağlanır."* denmektedir. Ayrıca, *"servis sağlayıcılar, bilgi içerik sağlayıcılarının isimlerini gösterir listeyi her ayın ilk iş günü Bakanlığa bildirir. Servis sağlayıcılar ile bilgi içerik sağlayıcıları, Bakanlıkça istendiği takdirde her türlü bilgi ve belgeyi vermekle yükümlüdür"*, ifadeleriyle servis sağlayıcılar için 5651 sayılı Kanundakine benzer bir yükümlülüğü Kültür ve Turizm Bakanlığı'na karşı getirmektedir.

§3. İNTERNETE ERİŞİMİ ENGELLEME

Son yıllarda İnternet erişimini sınırlayan ülkelerin sayısı hızla artmıştır ve artmaya devam etmektedir. Öne sürülen gerekçelerse genellikle fikri hakları koruma, çocukları cinsel ve psikolojik istismardan koruma, ulusal güvenliğin sağlanması, manevi değerlerin ve ailenin korunması ve benzeri şeklinde olmaktadır. Bazı ülkeler söz konusu hukuka aykırılıkların önüne geçebilmek için İnternet erişimine geniş çapta engellemeler koyarken, bazılarıysa teknolojik gelişmeleri yakından takip ederek daha etkin çözümler geliştirmeye çalışmaktadır. Otoriter rejimlerle yönetilen bazı ülkelerdeyse İnternet erişiminin kısıtlanması, yukarıda bahsedilen sebeplerin arkasına sığınılarak yapılmakta ve toplumun temel hak ve hürriyetlerine müdahalede bulunulmaktadır[33]. İnternet içeriğine ve erişimine hiç müdahale etmeyip, kullanıcılarını kendi yasal sorumluluklarıyla baş başa bırakan ülkeler de bulunmaktadır. Ülkelerdeki farklı uygulamalar ilerleyen bölümlerde dikkat çekici örnekleriyle incelenmektedir.

[32] Bayamlıoğlu, a.g.e., s.131.
[33] Örnek için bkz. yuk. §2. III. B. 3.

I. Türkiye'de İnternet İçeriğinin Düzenlenmesi

12 Nisan 1993 tarihinde[34] 64 kbit/saniye kapasiteli kiralık hat (leased line) ile Washington NSFNET (İnternet omurga ağı) üzerinden ilk İnternet bağlantısı gerçekleştirilerek Türkiye uluslar arası İnternet ağına bağlanmıştır. Bu tarihten 2001 yılına kadar Türkiye'de İnterneti düzenleyen özel bir kanun yapılmamış olup hükümet de müdahaleci olmayan bir tutum sergilemiştir. İfade suçlarıyla ilgili eski Türk Ceza Kanunu'nun[35] 159. maddesinin 1. fikrasındaki; "*Türklüğü, Cumhuriyeti, Büyük Millet Meclisini, Hükümetin manevi şahsiyetini, Bakanlıkları, Devletin askeri veya emniyet muhafaza kuvvetlerini veya Adliyenin manevi şahsiyetini alenen tahkir ve tezyif edenler altı aydan üç seneye kadar hapis cezası ile cezalandırılırlar.*" şeklindeki ifade İnternet üzerinden işlenen ifade suçlarını da kapsamaktaydı. Zira bu tarihe kadar açılmış davaların hepsi bu fikraya dayanmaktadır[36].

Türkiye'de kayıtlara suç olarak geçen ilk olay 1998 Haziran'ında 18 yaşındaki Emre Ersöz hakkında açılan davadır[37]. Ersöz polisin şiddet kullanmasını protesto etmek amacıyla İnternetteki bir forumda polis aleyhine yazı yazmış ve hakkında açılan dava sonucu 10 ay hapse mahkûm edilmiştir. Söz konusu forumda Ankara'da açık bırakılan yol çukurlarını protesto eden görme özürlü vatandaşların zabıta tarafından dövülmesini polis tarafından dövülmüş olarak algılamış ve forumda bunu protesto amaçlı bir mesaj yazan Ersöz "devletin emniyet kuvvetlerini alenen tahkir"den[38] dolayı 10 ay hapse mahkûm edilmiştir. Ersöz savunmasında yazdıklarının sadece İnternet ortamında yayımlanmış olduğunu ve İnternetin aleni değil sadece İnternet kullanıcılarına açık bir alan olduğunu ifade ederek beraatini talep etmiştir. Ancak cezası iyi halinden dolayı beş yıl ertelenmekle birlikte, bu süre içinde benzer bir ceza almaması koşuluyla mahkeme tarafından onaylanmıştır.

A. Türkiye'de Genel İçerik Düzenlemeleri

Yayıncılığın doğuşu ile devletler yayıncılık faaliyetinin kitleleri etkileme gücünü kontrol altında tutmaya çalışmışlardır[39]. Teknolojik gelişmeler kontrol yöntemlerini değiştirse ve bu kontrolü zorlaştırsa da otoritelerin denetim çabaları devam etmektedir. İnternetin doğuşuna kadar yayıncılık faaliyetinin sosyal etki gücü –teknolojik gelişmelere paralel olarak- gittikçe artan eksponansiyel bir grafik sergilemiştir. İnternetin doğuşundan önce en etkili yayın araçları radyo ve televizyondu. Radyo ve televizyonun etki alanı belirli fiziksel alanlar ile frekans aralıkları olduğundan, yayınların denetim ve kontrolü rahatlıkla yapılabilmekteydi. Mevcut düzenlemeler yayımlanan içeriği kontrol etmeye yeterliydi.

---

[34] Dünyada Internet'in gelişimi, http://www.internetarsivi.metu.edu.tr/tarihce.php.
[35] 765 Sayılı Türk Ceza Kanunu, RG., Sayı: 320, Tarih: 13.03.1926.
[36] Yaman Akdeniz / Kerem Altıparmak, İnternet: Girilmesi Tehlikeli ve Yasaktır Türkiye'de İnternet İçerik Düzenlemesi ve Sansüre İlişkin Eleştirel Bir Değerlendirme, 2008, adı geçen eser, s.4.
[37] Akdeniz/Altıparmak, a.g.e., s.5.
[38] Akdeniz/Altıparmak, a.g.e., s.5.
[39] Sezen Yeşil/Mustafa Alkan, İnternet Yönetişimi Ve İçerik Düzenlemeleri, XII. "Türkiye'de İnternet" Konferansı 8-10 Kasım 2007 (s.128 - 135), Ankara.

1.Radyo Televizyon Üst Kurulu (RTÜK) Kanunu

RTÜK 3984 sayılı Radyo ve Televizyonların Kuruluş ve Yayınları Hakkında Kanun[40]'a göre 1994 yılında radyo ve televizyonların faaliyetlerini denetlemek amacıyla kurulmuş özerk bir kurumdur.

Radyo ve televizyon yayınlarının İnternetten de yapılmaya başlaması ve İnternetteki içeriğin denetimine imkân sağlayan herhangi bir kanun olmaması nedeniyle RTÜK Kanunu'nun 31. maddesinde 2002 yılında değişiklik yapılmıştır. 31. maddedeki "*Her türlü teknoloji ile ve her tür iletişim ortamında yapılacak yayın ve hizmetlerin usul ve esasları, Haberleşme Yüksek Kurulunun belirleyeceği strateji çerçevesinde Üst Kurulca tespit edilip, Haberleşme Yüksek Kurulunun onayına sunulur. Bu yayın ve hizmetlerin mevzuata uygunluğu Üst Kurulca denetlenir.*" ibaresi nedeniyle RTÜK'e İnternetin denetimi yetkisi de verileceği endişesi İnternet yayıncıları, sektör çalışanları, sivil toplum örgütleri ve İnternet kullanıcıları arasında yayılmıştır. Ancak zaman içerisinde RTÜK'ün yaklaşımı göstermiştir ki, Kurul sadece radyo ve televizyon yayınlarını denetleyip, bu yayınların İnternet üzerinden yapılanlarını da izlemektedir. Dolayısıyla RTÜK, yukarıda bahsi geçen 31. maddedeki ibareden kendisine görev çıkarmamış, tamamen kendi kuruluş amacı ve kapsamına sadık kalmıştır. Zira RTÜK Kanunu'nun 1. maddesinde "*Bu Kanunun amacı, radyo ve televizyon ile tüm medya araçlarından yapılan yayınların düzenlenmesine ve özerkliği ve tarafsızlığı Anayasada hükme bağlanan Türkiye Radyo-Televizyon Kurumunun kuruluş, görev, yetki ve sorumluluklarına ilişkin esas ve usulleri belirlemektir.*" ve 2. maddesinde de "*Bu Kanun, her türlü teknik, usul ve araçlarla ve her ne isim altında olursa olsun elektromanyetik dalga yoluyla yurt içine ve yurt dışına yapılan radyodifüzyon ve televizyon yayınları ile ilgili hususları kapsar.*" şeklinde Kurul'un kuruluş amaç ve kapsamı belirtilmiştir.

2. Basın Kanunu

9 Haziran 2004 tarihinde kabul edilen 5187 sayılı Basın Kanunu[41], basılı süreli ya da süresiz tüm yayınları düzenlemektedir. Yani her tür kitap, dergi, gazete, vb. içeriği bu kanun ile düzenlenmektedir. Basın Kanunu 1. maddede belirtilen "*Bu Kanun basılmış eserlerin basımı ve yayımını kapsar.*" Şeklindeki kapsamı dolayısıyla sadece basılı yayınları düzenlemektedir. Ancak gazete, dergi ve kitap gibi yayınların tamamına yakını İnternette de faaliyet göstermekte olduğundan ya kanun kapsamının İnternette yayımlanan gazete, dergi, gibi yayınları da kapsayacak şekilde genişletilmesi ya da İnternette yayımlanan gazete, dergi ve benzeri yayınların ve İnternette yapılan tüm yayınların düzenlenmesini sağlayacak yeni bir kanun çıkarılması ihtiyacı ortaya çıkmıştır. Bu ihtiyaç 5651 Sayılı Kanun[42]'a zemin hazırlayan faktörlerden biridir. Zira sonraki bölümlerde ele alacağımız 5651 sayılı Kanun,

[40] 3984 Sayılı Kanun, R.G., Sayı: 21911, Tarih: 20.04.1994.
[41] 5187 Sayılı Kanun, R.G., Sayı: 25504, Tarih: 26.06.2004.
[42] 5651 Sayılı Kanun, R.G., Sayı: 26030, Tarih: 23.05.2007.

5187 sayılı Basın Kanunu ile benzerlik gösteren maddeler içermektedir. Mesela 5187 sayılı kanundaki "*Cinsel saldırı, cinayet ve intihar olayları hakkında, haber vermenin sınırlarını aşan ve okuyucuyu bu tür fiillere özendirebilecek nitelikte olan yazı ve resim yayımlayanlar birmilyar liradan yirmimilyar liraya kadar ağır para cezasıyla cezalandırılır. Bu ceza bölgesel süreli yayınlarda ikimilyar liradan, yaygın süreli yayınlarda onmilyar liradan az olamaz."* şeklindeki 20. maddeye konu edilen intihara yönlendirme ve cinsel istismar suçları 5651 sayılı kanunun 8. maddesine de konu edilmektedir.

B. 5651 Sayılı Kanun Öncesi İnternet Erişimi Engellemeleri

Geleneksel yayıncılık yöntemlerini kullanarak yayıncılık faaliyetlerinde bulunmak isteyenlerin otorite kuruluş tarafından lisans alması gerekmektedir. Zira lisanssız yayın yapanlar tespit edilebilmekte ve yayın yapmaları engellenebilmektedir. Ancak İnternet üzerinden yapılan yayıncılık ve sunulan içerik geleneksel yöntemlerle denetlenememektedir[43]. Dünya İnternet yayıncılığının denetiminin ne kadar gerekli olduğunu ya da denetlenmesi gerektiği düşünülse bile denetimin ne kadar zor olduğunu tartışırken "Web 2.0" kavramı ortaya çıkmıştır. İnternet artık yayıncılar ve sade İnternet kullanıcıları olarak katı çizgilerle birbirinden ayrılan iki aktör tipinden oluşmamakta, kullanıcılarına da içerik sunma imkânı sağlayan interaktif web sitelerinin çoğalmasıyla sade kullanıcılar diye nitelenen kullanıcılar da birer içerik sağlayıcı olmuşlardır. Bu durumda İnternette içerik kontrolü çok daha karmaşık bir hal almıştır.

Ülkemizde İnternet denetimi 4 Mayıs 2007 tarihinde 5651 Sayılı Kanun'un kabul edilmesinden önce bazı muhtelif kanun maddelerine dayanarak yapılmaktaydı. Ülkemizde bu tarihten önce erişim engellemenin pek fazla yapılmadığı sanılmakta olmasına rağmen henüz 2000 yılında bile erişime kapatılan web siteleri olduğu yapılan araştırmalarca ortaya konulmuştur[44]. Her ne kadar bunlar münferit bazı örnekler[45] olsa da 2005 yılının Haziran ayında MÜYAP'ın (Bağlantılı Hak Sahibi Fonogram Yapımcıları Meslek Birliği) temsil etmekte olduğu Türk sanatçılarına ait korsan müzik ve video içerikleri barındıran web sitelerinin erişime kapatılmasına yönelik açtığı peş peşe davalar neticesinde Türkiye'de erişime kapatılan web sitelerinin sayısında ciddi bir artış meydana gelmiştir. Yapılan bir araştırmaya göre ülkemizde MÜYAP tarafından açılan davalar sonucu, 2005 yılında 153, 2006 yılında 886 ve 2007 yılında da 549 web sitesi erişime kapatılmıştır[46].

---

[43] Yeşil/Alkan.

[44] Akdeniz/Altıparmak, a.g.e., s.6.

[45]" Subay.net", "ideapolitika.com", "akparti.gen.tr", "cunta.org" gibi birçok web sitesinin, çoğu itibariyle TCK 159. maddeye dayanılarak 2000-2004 yılları arasında erişime kapatılmasıyla ilgili bkz. "Akdeniz/Altıparmak, a.g.e., s.6".

[46] Füsun Sarp Nebil, Müyap Kapatmalarındaki Kötü Alışkanlık, 5651 Dışı Site Erişim Kapatmalarında Kural Haline Dönüşmüş – 1, http://www.turk.internet.com/portal/yazigoster.php?yaziid=20882, 6 Mayıs 2008,
Füsun Sarp Nebil, Türkiye'de Site Erişime Kapatmalarının Tarihçesi – 2, http://www.turk.internet.com/portal/yazigoster.php?yaziid=20909, 8 Mayıs 2008.

Ülkemizde İnternet içeriğinin denetlenmesine yönelik bir düzenlemenin eksikliği, Youtube'un erişime kapatılmasına da neden olan Mustafa Kemal Atatürk ve Türk Bayrağı hakkında hakaret içeren videoların yayımlanması ile kamuoyunda daha ciddi şekilde hissedilmeye başlamıştır. Söz konusu video içerikleri 5816 sayılı Atatürk Aleyhine İşlenen Suçlar Hakkında Kanun ve yeni TCK 300. maddeyi ihlal ettikleri gerekçesiyle ve erişim engelleme içerik bazlı değil, alan adı üzerinden yapıldığından Youtube 2007 yılının Mart ayında Türkiye'de erişime kapatılmıştır[47].

C. 5651 Sayılı Kanun'un Hukuki Analizi

2006 yılında İnternet üzerinden yayılan çocuk pornografisine yönelik polis operasyonları ve 2007 yılındaki Youtube'un kapatılması olayları[48] neticesinde İnternet içeriğinin denetlenmesi ve bu denetimin dayandırılacağı düzenleme ihtiyacı kamuoyunda yoğun olarak tartışılmaya başlamıştır. Tüm bu toplumsal ihtiyaçlar ve bu yönde yasal bir boşluğa dikkat çeken kamuoyu etkisi ile Ulaştırma Bakanlığı tarafından hazırlanan "Elektronik Ortamda İşlenen Suçların Önlenmesi ile 2559 ve 2937 sayılı Kanunlarda Değişiklik Yapılmasına Dair Kanun Tasarısı" ve İstanbul Milletvekili Gülseren TOPUZ tarafından TBMM'ye sunulan "Bilişim Sistemi Üzerinden Suç Teşkil Eden Zararlı Yayınlarla Mücadele Hakkında Kanun Teklifi" TBMM'de görüşülerek 4 Mayıs 2007 tarihinde 5651 sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun" adıyla kanunlaşmıştır[49]. 23 Mayıs 2007 tarihinde de Resmi Gazete'de yayımlanmıştır. Kanun'un uygulama yetkisi Bilgi Teknolojileri ve İletişim Kurumu'na (BTK) verilmiştir ve yürütme Kurum bünyesinde bulunan Telekomünikasyon İletişim Başkanlığı'na (TİB) bağlı İnternet Daire Başkanlığı tarafından başlatılmıştır[50].

5651 sayılı Kanun'un amacının İnternet ortamında hukuka aykırı içerik ve belirli suçlarla mücadele olduğu 1. maddede "*Bu Kanunun amaç ve kapsamı; içerik sağlayıcı, yer sağlayıcı, erişim sağlayıcı ve toplu kullanım sağlayıcıların yükümlülük ve sorumlulukları ile internet ortamında işlenen belirli suçlarla içerik, yer ve erişim sağlayıcıları üzerinden mücadeleye ilişkin esas ve usûlleri düzenlemektir."* ifadesiyle belirtilmiştir. Ayrıca bu Kanun'un 2. maddesi ile ülkemizde ilk defa İnternet aktörlerinin tanımı yapılmaktadır. 2. maddenin "e" ve "f" fıkralarında sırasıyla "erişim sağlayıcı" tanımında "Kullanıcılarına internet ortamına erişim olanağı sağlayan her türlü gerçek veya tüzel kişileri" ifadesiyle bildiğimiz anlamda internet servis sağlayıcılar (İSS) işaret edilmekte, "içerik sağlayıcı" tanımında "İnternet ortamı üzerinden kullanıcılara sunulan her türlü bilgi veya veriyi üreten, değiştiren ve sağlayan gerçek veya tüzel kişileri" ifadesiyle - internet ortamına Web 2.0 kavramının hâkim olmasıyla – internet ortamında içerik sağlayan herkes yani diğer bir ifade ile günümüzdeki tüm internet

[47] Akdeniz/Altıparmak, a.g.e., s.10.
[48] Bkz. yuk. § 3. I. B.
[49] Yasemin Durnagöl, 5651 Sayılı Kanun Kapsamında İnternet Aktörlerine Getirilen Yükümlülükler İle İdari Ve Cezai Yaptırımlar, TAAD, Cilt:2, Yıl:2, Sayı:4, 20 Ocak 2011 (s.375 - 416).
[50] Durnagöl.

kullanıcıları işaret edilmektedir. Ayrıca aynı maddenin "i"fıkrasında "Toplu kullanım sağlayıcı" tanımında "Kişilere belli bir yerde ve belli bir süre internet ortamı kullanım olanağı sağlayanı" ifadesiyle günümüz konjonktüründe en bilinen örnekleriyle internet kafeler, kütüphaneler, AVM'ler, oteller gibi halka açık internet hizmeti sunan özel ve tüzel kişiler işaret edilmektedir. Yine aynı maddenin "m" fıkrasında "Yer sağlayıcı" tanımında da "Hizmet ve içerikleri barındıran sistemleri sağlayan veya işleten gerçek veya tüzel kişileri" ifadesiyle en bilindik örneğiyle hosting şirketleri, cloud computing hizmeti veren şirketler ya da kullanıcılarına içerik sunma imkânı tanıyan web siteleri işaret edilmektedir. 5651 sayılı Kanun'un uygulaması ile ilgili dikkat çeken en önemli temel hususlardan bir tanesi, Ulaştırma Bakanlığınca hazırlanan "Elektronik Ortamda İşlenen Suçların Önlenmesi ile 2559 ve 2937 Sayılı Kanunlarda Değişiklik Yapılmasına Dair Kanun Tasarısı"nın genel gerekçesinde yer alan "*…söz konusu kanunda yer alan bazı suçların, elektronik ortamda işlenmesinin içerik, yer ve erişim sağlayıcıları üzerinden önlenmesine ilişkin esas ve usûller belirlenmektedir.*" ifadesi ile İnternet ortamında suç teşkil eden içerik ve davranışlarla Kanun'un 2. maddesinde tanımlanmış olan İnternet aktörleri vasıtasıyla mücadele edilecek olmasının belirtilmiş olmasıdır. Zira Avrupa Birliği (AB) ve üye ülkeleri de İSS'leri ve bilişim şirketlerini politikalarını uygulamak için kullanmakta ve baskı altında tutmaktadırlar. Bu vasıtayla birlik ve üye devletler doğrudan engelleme yapmayıp İSS'ler ve bilişim şirketlerine uygulattıkları politikaları nedeniyle alacakları tepkileri azaltmaya çalışmaktadırlar[51].

5651 sayılı Kanun, uygulama bakımından adil olmadığı ve kamu yararının gözetilmediği yönünde eleştiriler alsa da ülkemizin İnternet içerik politikasını şeffaf bir şekilde ortaya koymaktadır[52]. Özellikle haklarında dünya kamuoyunda, düşünce hürriyetine duyulan saygıdan ötürü erişim engelleme yapmadıkları yanlış algısı bulunan AB üyesi devletlerin yukarıda da anlatılan İnternet içerik politikalarındaki "ulusal güvenlik", "kamu yararı" gibi keyfi uygulamalara açık kapı bırakan muğlâk ifadeler göz önüne alındığında, 5651 sayılı Kanun'da engellemeye sebep teşkil edecek maddelerin tamamının TCK 5237 sayılı ve 5816 sayılı özel kanunlarda suç olarak belirlenen maddeler olduğu görülmektedir[53]. Zira Anayasa'mızın 13. maddesinde "*Temel hak ve hürriyetler, özlerine dokunulmaksızın yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabilir. Bu sınırlamalar, Anayasanın sözüne ve ruhuna, demokratik toplum düzeninin ve lâik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamaz.*" şeklinde belirtilen temel hak ve hürriyetleri sınırlayıcı düzenlemelerin ancak kanunla yapılması gerektiği ilkesine sadık kalınmıştır. Yani engellemenin çerçevesi net ve şeffaf bir şekilde çizilmiştir.

[51] Leyla Keser Berber/Mehmet Bedii Kaya, 5651 Sayılı Kanunun Teknik Ve Hukuki Açıdan Değerlendirilmesi, İstanbul Bilgi Üniversitesi Bilişim Ve Teknoloji Hukuku Enstitüsü, http://www.turk.internet.com/portal/yazigoster.php?yaziid=28665, adı geçen eser, s.6.
[52] Berber/Kaya, a.g.e., s.17.
[53] Berber/Kaya, a.g.e., s.17.

D. 5651 Sayılı Kanun'un Çizdiği Çerçeve

5651 sayılı Kanun'a göre erişimin engellenmesi cezasını gerektirecek suçlar 8. maddenin 1. fıkrasında aşağıdaki gibi listelenmiştir:

"*a) 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanununda yer alan;*

1) İntihara yönlendirme (madde 84),

2) Çocukların cinsel istismarı (madde 103, birinci fıkra),

3) Uyuşturucu veya uyarıcı madde kullanılmasını kolaylaştırma (madde 190),

4) Sağlık için tehlikeli madde temini (madde 194),

5) Müstehcenlik (madde 226),

6) Fuhuş (madde 227),

7) Kumar oynanması için yer ve imkân sağlama (madde 228),

suçları.

b) 25/7/1951 tarihli ve 5816 sayılı Atatürk Aleyhine İşlenen Suçlar Hakkında Kanunda yer alan suçlar."

8. maddenin 1. fıkrasında listelenen suçlar uygulamada "katalog suçlar" olarak isimlendirilmekte olup, bu suçların tamamı yukarıdaki listede de belirtildiği üzere daha önceden hukukumuzda yeri olan suçlardır. 1. fıkranın "a" bendinde listelenen suçlar 5237 sayılı Türk Ceza Kanunu'nda[54] yer almaktadır.

8. maddenin 2. Fıkrasına göre erişimin engellenmesi kararı soruşturma evresinde hâkim, kovuşturma evresinde ise mahkeme tarafından verilecek ve karar TİB tarafından uygulanacaktır. Ancak Kanun'a göre suç teşkil eden içeriğin, içerik ya da yer sağlayıcısının yurt dışında olması durumunda erişim engelleme kararı TİB tarafından re'sen verilebilecektir[55]. Ayrıca içeriği, yukarıda listelenen suçlardan "*çocukların cinsel istismarı*" ve "*müstehcenlik*" olan yayınlar için de, içerik ve yer sağlayıcısı yurt içinde olsa bile TİB re'sen erişim engelleme kararı verebilecektir[56].

Kanun'un 3. maddesinde içerik, yer ve erişim sağlayıcılar için kendilerini tanıtıcı bilgilerin, kendilerine ait İnternet ortamında bulundurulması zorunluluğu getirilmektedir. Bu sayede herhangi bir içerikten rahatsız ya da mağdur olan İnternet kullanıcıları içerik, yer veya erişim sağlayıcılara bizzat başvurarak içeriğin yayından kaldırılmasını talep edebileceklerdir. Ayrıca adli makamlar da kendilerine başvurulduğunda gerekli tebligatı bu bilgiler üzerinden yapabileceklerdir.

4. madde içerik sağlayıcıyı yayımladığı her türlü içerikten dolayı sorumlu tutmaktadır. Yani sıradan bir İnternet kullanıcısı da günümüz İnternet koşulları düşünüldüğünde içerik sağlayıcı olduğundan, bu maddede bütün İnternet kullanıcıları muhatap alınmaktadır. 5. maddede ise yer sağlayıcıların, kullanıcılarının ya da müşterilerinin sundukları içeriklerin

[54] 5237 Sayılı Kanun, R.G., Sayı: 25611, Tarih: 12.10.2004.
[55] Yeşil/Alkan.
[56] Yeşil/Alkan.

hukuka uygunluğunu denetlemek zorunda olmadıkları "*Yer sağlayıcı, yer sağladığı içeriği kontrol etmek veya hukuka aykırı bir faaliyetin söz konusu olup olmadığını araştırmakla yükümlü değildir.*" ifadesiyle belirtilmektedir. Zira böyle bir sorumluluk yer sağlayıcı açısından altından kalkılamaz bir iş yükü olacaktır. Yer sağlayıcının terabaytlarca[57], hatta petabaytlarca[58] verinin hukuka uygunluğunu araştırması makul bir sürede bitirilebilecek bir iş değildir. Ancak yer sağlayıcı için, haberdar edildiği takdirde, hukuka aykırı içeriği yayından kaldırma yükümlülüğü getirilmiştir.

5651 sayılı Kanun 6. maddedeki "*Herhangi bir kullanıcısının yayınladığı hukuka aykırı içerikten, bu Kanun hükümlerine uygun olarak haberdar edilmesi halinde ve teknik olarak engelleme imkânı bulunduğu ölçüde erişimi engellemekle*" ifadesiyle erişim sağlayıcıya – diğer bir deyişle İSS'ye – hukuka aykırı içeriğe erişimi engelleme görevi ve yetkisini vermektedir. Bu yaklaşım, dünyada birçok ülkede görülen bir yaklaşım olup web sitelerinin erişime kapatılması neticesinde oluşacak tepkinin ilgili hükümet organları üzerine toplanmamasını amaçlamaktadır. Ayrıca bu maddeyle erişim sağlayıcılara trafik bilgisi (teknik ifadesiyle, log) tutmaları yükümlülüğü getirilmektedir.

Kanun'un 7. maddesiyle; İnternet kafe, kütüphane, otel gibi toplu kullanım sağlayıcılarla ilgili yükümlülükler tanımlanmaktadır. "*Ticarî amaçla olup olmadığına bakılmaksızın bütün toplu kullanım sağlayıcılar, konusu suç oluşturan içeriklere erişimi önleyici tedbirleri almakla yükümlüdür.*" ifadesiyle toplu kullanım sağlayıcıların, kullanıcıları hukuka aykırı içeriklere erişmelerini engellemek için gerekli önlemleri almaları gerektiği üzerinde durulmaktadır. Bu maddeden toplu kullanım sağlayıcıların, İnternet kullanıcılarının hukuka aykırı içeriklere erişmelerini engelleyecek şekilde yapılandırılmış filtre, güvenlik duvarı gibi yazılımları kullanmaları gerektiği anlaşılmaktadır.

E. 5651 Sayılı Kanun'un Teknik Analizi

5651 sayılı Kanun'un 8. maddesinde "*İnternet ortamında yapılan ve içeriği aşağıdaki suçları oluşturduğu hususunda yeterli şüphe sebebi bulunan yayınlarla ilgili olarak erişimin engellenmesine karar verilir*" denilerek, aynı maddede söz konusu olan suçların işlenmesi durumunda Kanun'un amaçlarından olan "*internet ortamında işlenen belirli suçlarla içerik, yer ve erişim sağlayıcıları üzerinden mücadele*" için erişim engelleme yöntemi benimsenmektedir. Ancak bu yöntem engelleme kararı verilen çoğu web sitesi için ölçülülük ilkesine aykırı olmaktadır[59]. Zira Anayasa'nın 13. maddesine göre temel hak ve hürriyetlerin sınırlandırılmasında ölçülülük ilkesine sadık kalınması gerekmektedir. Anayasa Mahkemesi'ne göre ölçülülük ilkesi, yasal düzenlemede sınırlama aracının, sınırlama amacına elverişli olması, sınırlama aracıyla amacı arasındaki oranın ölçüsüz olmaması anlamını ifade

[57] Terabayt, 1 Gigabayt'lık veri depolama ölçüsü biriminin 1024 katı olan veri depolama ölçüsü birimidir.
[58] Petabayt, 1 Terabayt'lık veri depolama ölçüsü biriminin 1024 katı olan veri depolama ölçüsü birimidir.
[59] Berber/Kaya, a.g.e., s.17.

etmektedir[60]. Ayrıca erişim engelleme yöntemi uygulanacaksa bile, öncelikle hukuka aykırı içeriğin yayından kaldırılması için gerekli uyarı yapılmalı, uyarı dikkate alınmıyorsa engelleme işlemi uygulanmalıdır. Bu şekilde muhatabın kendini savunma hakkı elinden alınmamış olacaktır[61].

5651 sayılı Kanun'da adı geçen erişim engelleme uygulamaları tedbir niteliğinde olup, ceza ya da yaptırım değildir[62]. Temel hak ve hürriyetlere sınırlama getirilmesi uygulamaları hukuk devletlerinin temel ilkeleri bakımından adli makamların işidir. Ancak Kanun'un 8. maddesinin 4. fıkrasında yer alan "*İçeriği birinci fıkrada belirtilen suçları oluşturan yayınların içerik veya yer sağlayıcısının yurt dışında bulunması halinde veya içerik veya yer sağlayıcısı yurt içinde bulunsa bile, içeriği birinci fıkranın (a) bendinin (2) ve (5) numaralı alt bentlerinde yazılı suçları oluşturan yayınlara ilişkin olarak erişimin engellenmesi kararı re'sen Başkanlık tarafından verilir. Bu karar, erişim sağlayıcısına bildirilerek gereğinin yerine getirilmesi istenir."* ifadesiyle 8. maddenin 1. fıkrasında belirtilen suçları oluşturan yayınların içerik veya yer sağlayıcıları yurt dışında ise TİB'e re'sen erişim engelleme yetkisi verilmektedir. Ayrıca çocukların cinsel istismarı ve müstehcenlik suçlarını oluşturan içerik barındıran web sitelerinin içerik veya yer sağlayıcıları yurt içinde bulunsa bile bu web siteleri için de TİB'e erişim engelleme yetkisi verilmektedir. Yani idari bir makama erişim engelleme yetkisi tedbir için kullanılmak üzere de olsa verilmektedir ve bu yetki kötüye kullanıma açıktır. Bu anlamda TİB'in alacağı erişim engelleme kararlarında çok hassas davranması hukuk devleti ilkesinin temelleri dışına çıkılmaması açısından büyük önem arz etmektedir.

5651 sayılı Kanun'un uygulamasını düzenleyen yönetmeliklerden İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul Ve Esaslar Hakkında Yönetmelik'in[63] 15. maddesinde "*Koruma tedbiri olarak verilen erişimin engellenmesi kararında alan adı veya IP adresi olarak erişim engelleme yöntemi belirtilir.*" ifadesiyle erişim engelleme yöntemi olarak IP engelleme[64] ya da DNS engelleme[65] yöntemlerinden birinin kullanılacağı belirtilmektedir. Ancak her iki yöntemde de erişime kapatılan web sitesi tamamıyla erişilemez olmaktadır. Ayrıca DNS engelleme yönteminde web sitesinin alan adı altındaki bütün hizmetler devre dışı kalmaktadır. IP engelleme yönteminde ise web sitesini barındıran web sunucusunun IP adresine erişim engelleme uygulandığından dolayı söz konusu sunucudan yayın yapan bütün web sitelerinin erişimi engellenmiş olmaktadır. Yani hukuka aykırı içerik barındırmayan web siteleri de zarar görmektedir. Bu durumda ceza sorumluluğunun şahsiliği ilkesine aykırı hareket edilmiş olmaktadır. TCK[66] 20. maddede "*Ceza sorumluluğu şahsîdir. Kimse başkasının fiilinden dolayı sorumlu tutulamaz.*" denilmektedir. Bu maddeye muhalif uygulamalar yaşanmaması için – eğer engelleme zorunluysa – URL engelleme tekniği[67] kullanılarak sadece hukuka aykırı olduğu yargısına varılan içeriğe erişmek için kullanılan URL engellenerek, hukuka aykırı içerik barındırmayan web sayfalarının da engellenmesinin

[60] Anayasa Mahkemesi, Esas Sayısı: 2001/309, Karar Sayısı: 2002/91, Tarih: 15.10.2002.
[61] Berber/Kaya, a.g.e., s.18.
[62] Berber/Kaya, a.g.e., s.18.
[63] R.G., Sayı: 26716, Tarih: 30.11.2007.
[64] Bkz. aşa. § 4 I A.
[65] Bkz. aşa. § 4 I C.
[66] 5237 Sayılı Kanun, R.G., Sayı: 25611, Tarih: 12.10.2004.
[67] Bkz. aşa. § 4 I D.

önüne geçilmelidir. Ayrıca bu şekilde kamu yararı da gözetilerek her türlü hak ve hürriyetlerin gereksiz yere kısıtlanmasının da önüne geçilecektir[68]. Bu konuya dair ülkemizde yaşanan en önemli örneklerden bir tanesi blog hizmeti veren blogspot.com, blogger.com gibi web sitelerinin 2007 yılında kapatılmasıdır. Söz konusu web sitelerinin kullanıcılarından birkaç tanesinin hukuka aykırı içerik paylaşması neticesinde web siteleri tamamen erişime kapatılarak, kullanıcı sayıları milyonlarla ifade edilen dünyaca ünlü web sitelerinin ülkemizdeki kullanıcıları da, web sitelerinin sahibi şirketler de mağdur olmuştur.

5651 sayılı Kanun'un uygulamalarına dair bir diğer sıkıntı da kamuoyunun engellemeler konusunda yeterince bilgilendirilmemesidir. TİB, erişimi engellenen web sitelerini ve bu sitelerle ilgili ayrıntılı istatistikleri yayımlamamaktadır. Ayrıca erişime kapatılan web sitelerinin bir kısmına erişilmeye çalışıldığında "Ulaşmaya çalıştığınız İnternet sitesi Mahkeme/Savcılık kararı ile erişime engellenmiştir" cümlesinden ibaret bir uyarı yazısı ile karşılaşılmaktadır (Şekil 5). Ancak bazılarında bu mesajın altında, kararı veren adli makam ve karar numarası bilgisi Türkçe ve İngilizce olarak yer almaktadır[69]. Bu bilgilerin erişime kapatılan bütün web sitelerinde yer alması gerekmektedir. Ayrıca bu bilgilerin altında da engelleme sebebi, tedbirin süresi ve tedbirin kaldırılması için izlenmesi gereken itiraz süreci de yer almalıdır[70].

5651 sayılı Kanun'la ilgili uygulamada yaşanan önemli bir problem de katalog suçların tamamının açıkça tanımlanmamış olmasıdır. Suçta ve cezada kanunîlik ilkesine uygunluk açısından katalog suçların çerçevesinin net bir şekilde çizilmesi gerekmektedir[71]. Zira 5651 sayılı Kanun'da 8. maddede "müstehcenlik" olarak ifade edilen müstehcenliğin ölçüsünün ne olduğu açık olmamakla birlikte neyin müstehcen olduğu sübjektiftir. 8. maddenin içeriğinin dayandırıldığı 5237 sayılı TCK'nın 226. maddesi müstehcen içeriğe ilişkin eylemleri detaylı olarak anlatmışsa da, bu maddede müstehcenliğin tanımı bulunmamaktadır[72].

F. Ampirik Veriler Işığında 5651 Uygulamaları ve Değerlendirme

Ülkemizde 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'un 2007 yılında yürürlüğe girmesinden bu yana geçen 5 yılın sonunda ülkemiz, OpenNet Initiative ("ONI") tarafından hazırlanan raporlarda, politik sansür, sosyal sansür ve araçların sansürü

---

[68] Örneğin, Youtube gibi bir web sitesinin erişime kapatılması akla gelebilecek hemen her konuda türlü türlü eğitici içerik barındıran bir bilgi kaynağından istifade edilmesine de engel olmaktadır. Bu da kamu yararına zarar vermektedir.

[69] Araştırmamıza göre bazı örneklerde sadece "Ulaşmaya çalıştığınız internet sitesi Mahkeme/Savcılık kararı ile erişime engellenmiştir" iletisi bulunmaktadır. Örneğin http://bilgiat.com/, http://www.sharebus.com/. Bazılarında ise yukarıda belirtilen ayrıntılı bilgilere rastlanmıştır. Örneğin http://delicast.com/, http://imcomininpeacesometimes.blogspot.com/. (Örnekler http://engelliweb.com/ adresinden tamamen rastgele seçilmiştir.)

[70] Berber/Kaya, a.g.e., s.23.

[71] Berber/Kaya, a.g.e., s.23.

[72] Kaya, a.g.e., s. 105.

kategorilerinde "seçici" olarak sınıflandırılarak sansür bakımından dünya ülkeleri arasında orta sıralarda yer almıştır[73](Bkz. Şekil1, Şekil2, Şekil3, Şekil4). Her ne kadar 5651 sayılı Kanun yürürlüğe girdikten sonra erişim engellemelerin sayısı ciddi miktarda arttıysa da, bütün engelleme kararları 5651'e dayanmamaktadır. Mesela, Ekim 2008'de tüm dünyada yaygın bir şekilde kullanılan blogger.com ve blogspot.com blog sitelerinin erişime kapatılması kararları 5846 Fikir ve Sanat Eserleri Kanunu[74] hükümlerine dayandırılmaktadır[75]. Karar, blog kullanıcılarından bazılarının blog sayfaları üzerinden Lig TV abonesi olunmadan futbol maçlarının izlenebilmesi konusunda bilgi paylaşmaları sonucunda Digitürk'ün başvurusuyla alınmıştır.

Kasım 2007'den 1 Ekim 2008 tarihine kadar geçen 5651 sayılı Kanun'un uygulanması sürecinde TİB verilerine göre, Kanun hükümlerine dayandırılarak 1115 web sitesi erişime kapatılmıştır. Bu 1115 web sitesinin 252 tanesi (%23'ü) mahkeme kararıyla engellenmiş, 863 tanesi de (%77'si) TİB tarafından re'sen verilen idari kararlarla erişime kapatılmıştır[76]. Mahkeme kararıyla kapatılan web sitelerinden 38 tanesi müstehcenlik, 4 tanesi çocukların cinsel istismarı, 17 tanesi kumar, 2 tanesi de bahis suçları gerekçe gösterilerek erişime kapatılmıştır. Ayrıca bu web sitelerinden 49 tanesi Atatürk aleyhine işlenen suçlarla ilgili kanun (5846 sayılı Kanun) gerekçe gösterilerek erişime kapatılmıştır[77]. Mahkeme tarafından engellenenlerden başka, TİB tarafından erişime kapatılan web sitelerinin çoğunluğunu 411 web sitesi ile (%77) çocukların cinsel istismarı gerekçesiyle kapatılan web siteleri oluşturmaktadır. Geri kalan idari engelleme kararlarından 352'si (%40) müstehcenlik, 64 tanesi (%7) kumar, 23 tanesi bahis, 10 tanesi fuhuş, 2 tanesi Atatürk aleyhine işlenen suçlar ve bir tanesi de intiharı teşvik suçları gerekçe gösterilerek verilmiştir[78]. 1 Ekim 2008 tarihi sonrasındaki verilere TİB ayrıntılı rapor yayımlamadığından dolayı gayrı resmi raporlar üzerinden ulaşılabilmektedir[79].

1. 5651 Sonrası Erişim Engelleme Uygulamaları ve Etkileri

http://engelliweb.com/istatistikler/ web adresinden elde edilen güncel[80] bilgilere göre bugüne kadar ülkemizde 18640 erişim engelleme kararı verilmiştir. Bu engelleme kararlarının 15599 tanesi (%83,9) TİB tarafından, 934 tanesi (%5) mahkeme tarafından ve 801 tanesi de (%4,3) savcılık tarafından verilmiştir. Ayrıca erişime kapatılan 1248 (%6,7) web sitesinin de kapatılma nedeni belirtilmemiştir.

---

[73] "Seçici" kategorisi, diğer bütün sınıflandırma kategorileri ve dünya ülkelerinin belirlenen sansür kategorilerindeki sınıflandırılma bilgileri için bkz. http://map.opennet.net/.
[74] 5846 Sayılı Kanun, R.G., Sayı: 7981, Tarih: 13.12.1951.
[75] Akdeniz/Altıparmak, a.g.e., s.26.
[76] Akdeniz/Altıparmak, a.g.e., s.27.
[77] Akdeniz/Altıparmak, a.g.e., s.28.
[78] Akdeniz/Altıparmak, a.g.e., s.29.
[79] Örneğin, bu çalışma kapsamında engelliweb.com sitesinde yer alan rapor ve istatistikler sıklıkla kullanılmıştır.
[80] http://engelliweb.com/istatistikler/ adresinden 15.05.2012 tarihinde elde edilen bilgilerdir. Ancak web sitesinde verilen istatistikler sadece ulaşılabilen bilgilerdir. Erişime kapatılan web sitelerinin sayısının gerçekte daha fazla olduğu tahmin edilmektedir.

Ülkemizde uygulanmakta olan erişim engelleme yöntemi çoğunlukla DNS engelleme yöntemidir[81]. Bu yöntemin erişim engelleme konusunda yetersiz kaldığı yapılan araştırmalar ve Youtube engellemesi neticesinde ortaya çıkmıştır. Zira Youtube erişiminin ilk defa engellendiği Mart 2007'den erişim yasağının tamamen kaldırıldığı Ekim 2010'a kadar ülkemizde genellikle en çok ziyaret edilen web siteleri arasında olmuştur. 2010 yılında, henüz erişime açılmamışken Youtube ülkemizde en çok ziyaret edilen beşinci web sitesi olmuştur[82]. Ayrıca İnternet trafiği ve ülkelere göre en çok ziyaret edilen web sitelerinin istatistiklerini veren www.alexa.com'dan elde edilen güncel verilere[83] göre, ülkemizde en çok ziyaret edilen web siteleri sıralamasında ilk 400 web sitesi içinde 17 tanesinin erişime kapatılmış ve çoğu yurt dışından yayın yapan[84] web siteleri olduğu ortaya çıkmıştır. İlk 400'deki web siteleri içinde iki tanesi de, 109. Sıradaki www.ktunnel.com ve 323. sıradaki www.vtunnel.com web proxy siteleridir. Bu bilgi de göstermektedir ki, ülkemizde erişim engelleme teknikleri oldukça yaygın bir şekilde kullanılmaktadır.

Yukarıda bahsedilen ülkemizle ilgili engelleme aşma girişimlerinin yaygınlığına dair veriler ışığında engellenen web sitelerinin çok sıkı bir şekilde takip edilmezse erişiminin mümkün olduğunu ve erişim engellemelerin artmasıyla toplumda engelleme aşma yöntemlerine yönelimin artacağını söylemek mümkündür. Bu trend neticesinde de çok sayıda güvenlik zafiyeti ortaya çıkmakta ve İnternet kullanıcıları başta olmak üzere, İnternet kullanıcılarının bilinçsiz şekilde engelleme aşma yöntemlerini kullanmalarıyla kurumsal ağlar da güvenlik risklerinden nasibini almaktadır. Bu bilgilere dayanarak, ülkemizde uygulanan erişim engelleme yönteminin çok etkili olmadığını ve dolaylı olarak bilgi güvenliği açıklıklarına neden olduğunu söylemek mümkündür.

2. 5651 Sonrası Ülkemizdeki Google Aramaları ve Değişen Trendler

Ülkemizde engelleme aşma yöntemlerinin sıklıkla kullanıldığı yukarıda bahsedilen istatistikî verilerden anlaşılacağı gibi google.com'da arama yapılan arama terimler incelenerek de anlaşılabilmektedir. Google tarafından sağlanan Google Trends[85] hizmeti sayesinde dünyanın herhangi bir yerinde, herhangi bir zaman aralığında, hangi konuda, ne

---

[81] Bu konuda resmi bir bilgi ya da belgeye ulaşılamamıştır. Ancak deneysel çalışmalar ve kullanılan engelleme aşma yöntemlerinin verdiği sonuçlar genellikle bu yöntemi işaret etmektedir. Ayrıca ağ hatası diye tabir edilen yöntemin nadiren de olsa uygulandığı yaptığımız araştırmalar neticesinde gözlemlenmiştir. Örneğin, http://www.livejasmin.com/ adresine ülkemiz sınırları dâhilinde erişilmeye çalışıldığında "Web sitesine bağlanılamadı." şeklinde bir uyarı yazısı ile karşılaşılmakta olup, sitenin erişime engellendiğine dair bir bilgiye rastlanılmamaktadır. Ancak web sitesine proxy üzerinden erişilmeye çalışıldığında web sitesi erişilebilir olmakta olduğundan bu web sitesi için erişim engelleme uygulandığını söylemek mümkündür.

[82] Ergün Dinçer, En Çok Ziyaret Edilen Site Sıralamasında Facebook, 2010 Yılında Google'u Geçti, 3 Ocak 2011, http://www.sosyalmedyapazarlama.com/2011/01/en-cok-ziyaret-edilen-site-siralamasinda-facebook-2010-yilinda-googleu-gecti/

[83] 8 Mayıs 2012 tarihinde yapmış olduğumuz araştırma neticesinde elde ettiğimiz verilerdir.

[84] Bu web sitelerinden dört tanesi Hong Kong'dan, dört tanesi ABD'den ve geri kalan sekiz tanesi de farklı ülkelerden yayın yapmakta olup, bir tanesi de yurt içinden yayın yapmaktadır. Söz konusu web sitelerinin nerelerden yayın yaptıkları hakkındaki bilgi için www.whois.com adlı web sitesinden faydalanılmıştır.

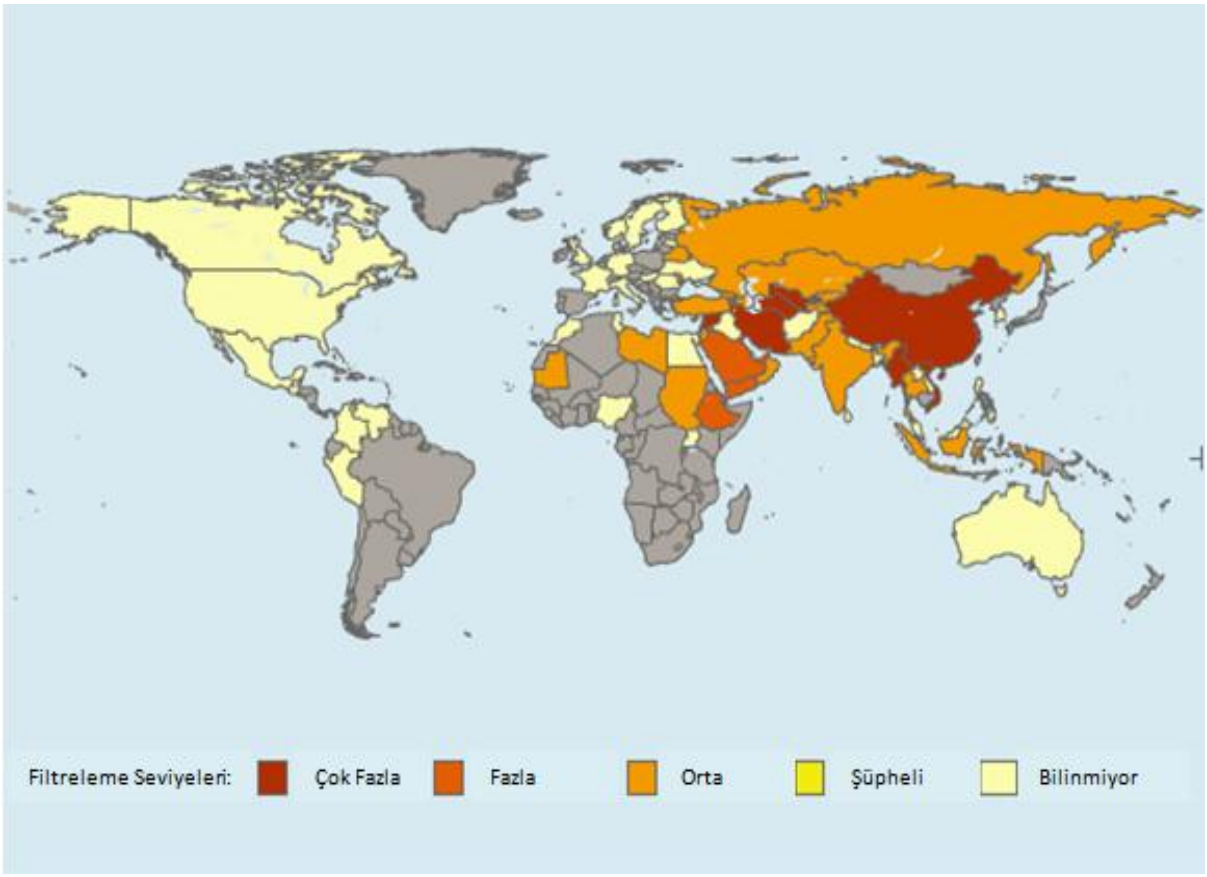
[85] About Google Trends, http://www.google.com.tr/intl/en/trends/about.html.

sıklıkla arama yapıldığını ya da en çok neyin arandığını öğrenmek mümkündür. Ülkemizde de Google'da yapılan aramalar üzerine yaptığımız araştırma neticesinde "*youtube*" sözcüğünün, Youtube'un ülkemizden erişime kapalı olduğu Mart 2007 – Ocak 2008, Ocak 2008 – Ocak 2009, Ocak 2009 – Ocak 2010 ve Ocak 2010 – Ekim 2010 tarih aralıklarında sırasıyla birinci, dördüncü, sekizinci ve sekizinci en çok aranan terim olduğu ortaya çıkmıştır. Bu sonuç göstermektedir ki, 5651 Sayılı Kanun'un hukuka aykırı olarak belirlediği içeriğe müdahale etmek için getirmiş olduğu erişime kapatma yöntemi etkisiz kalmaktadır. Ayrıca yapılan araştırmaya göre ülkemizde engelleme aşma yöntemlerini aramak için çoktan aza doğru en çok "*youtube giriş*", "*ktunnel*", "*tunnel*", "*proxy*", "*ultrasurf*", "*dns değiştirme*", "*ip değiştirme*", vb. arama terimleri kullanılmaktadır[86].

II. Dünyada İnternet İçeriğinin Düzenlenmesi

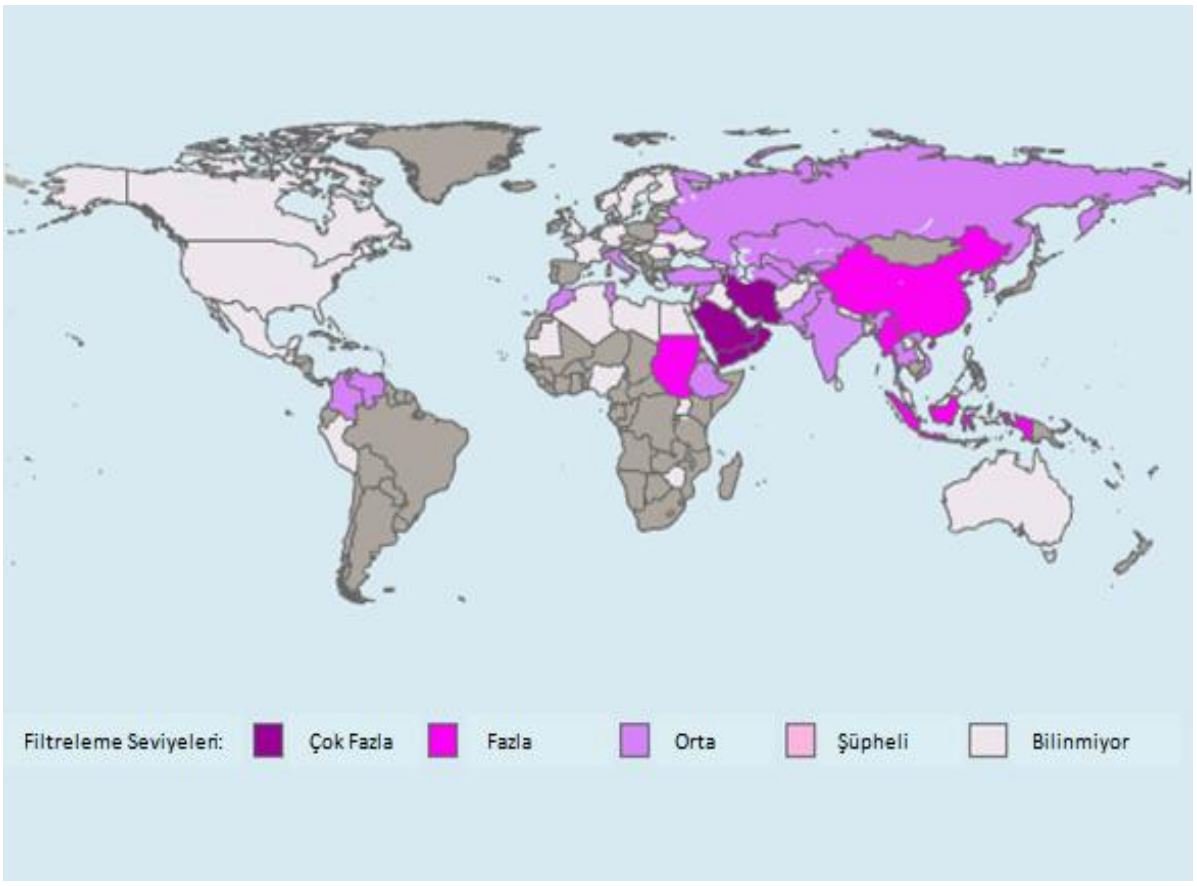
İnternet erişiminin engellenmesi ve içeriğinin filtrelenmesi politikaları dünya üzerinde filtrelenen içeriğe ve kullanılan filtreleme teknolojisine göre değişkenlik gösterir. Kuzey Kore benzeri baskıcılıkla eleştirilen rejimlerde politik ve muhalif içerik sıkı sıkıya engellenirken, Suudi Arabistan ve İran'da da sosyal içeriğe yoğun bir sınırlama getirilmektedir[87]. Öte yandan Avrupa ülkeleri de genel olarak çocuk pornografisi ve ırkçılık ihtiva eden İnternet içeriğini sınırlamaktadır[88]. İncelenmek üzere seçilen ülkeler işlenmeden önce, dünya genelinde ONI[89] tarafından hazırlanan, İnternet filtreleme politikalarının özetlendiği dünya haritaları aşağıdaki şekillerde gösterilmektedir[90].

[86] Araştırma, Ocak 2007 – Nisan 2012 tarih aralığını kapsamaktadır.
[87] Brown, I. (2008). Internet censorship: be careful what you ask for.
[88] Deibert, R. & Villeneuve, N. (2005). Firewalls and Power: An Overview of Global State Censorship of the Internet. In M. Klang & A. Murray (Eds.), Human Rights in the Digital Age (s.111—124). London: GlassHouse.
[89] Global Internet Filtering Map, http://map.opennet.net/filtering-pol.html.
[90] Haritalarda "Bilinmiyor" ile gösterilen ülkelerde "Bilinmiyor" ifadesi, bu ülkelerde filtreleme olduğu ya da olmadığı anlamına gelmemektedir.



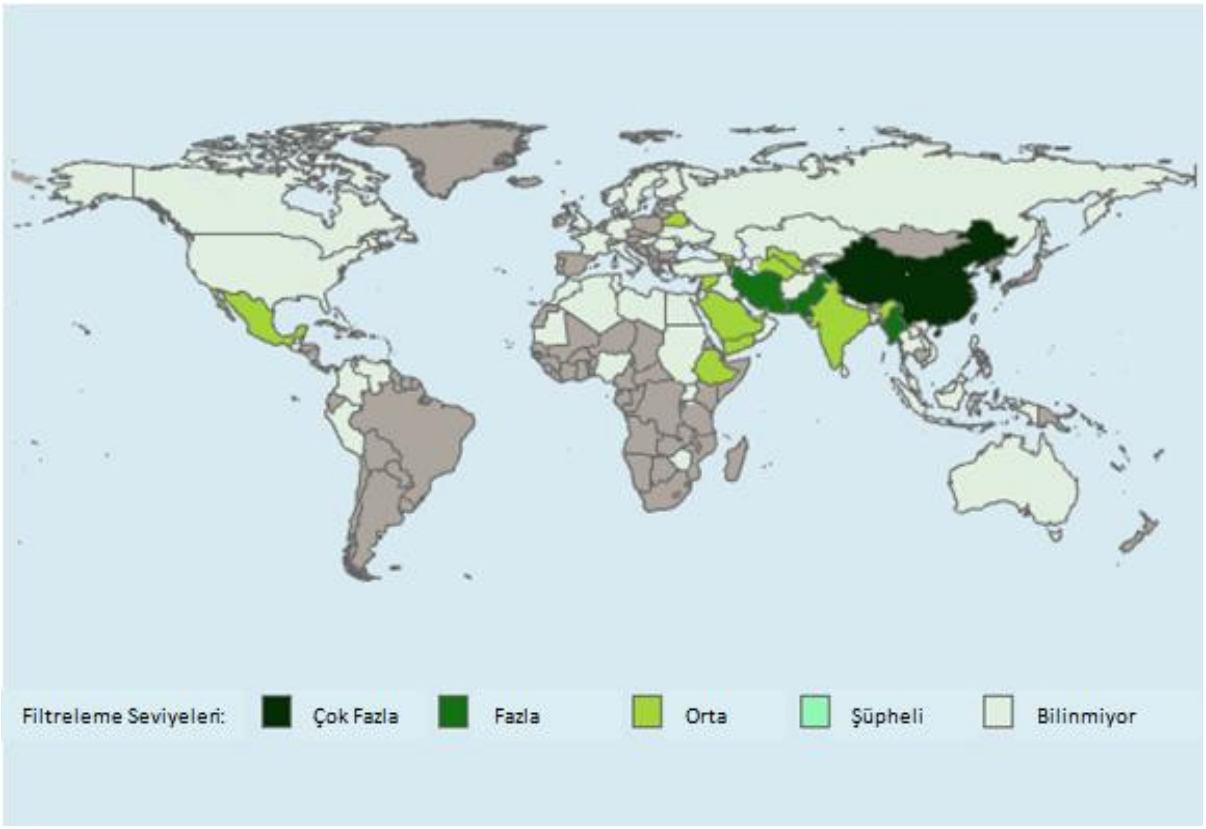
Şekil 1 Politik İçerik: Mevcut rejimlere muhalif fikirler içeren, insan haklarıyla, ifade özgürlüğüyle, azınlık haklarıyla ya da dini hareketlerle ilişkili içeriklere yapılan engellemelerin haritası

Şekil 1'de mevcut rejimlere muhalif fikirler içeren, insan haklarıyla, ifade özgürlüğüyle, azınlık haklarıyla ya da dinî hareketlerle ilişkili içeriklere yapılan engellemelerin dünya üzerindeki dağılımı gösterilmektedir. Bu haritada en çok dikkat çeken ülkeler Çin, Orta Asya ülkeleri ve birçok Arap ülkesidir.



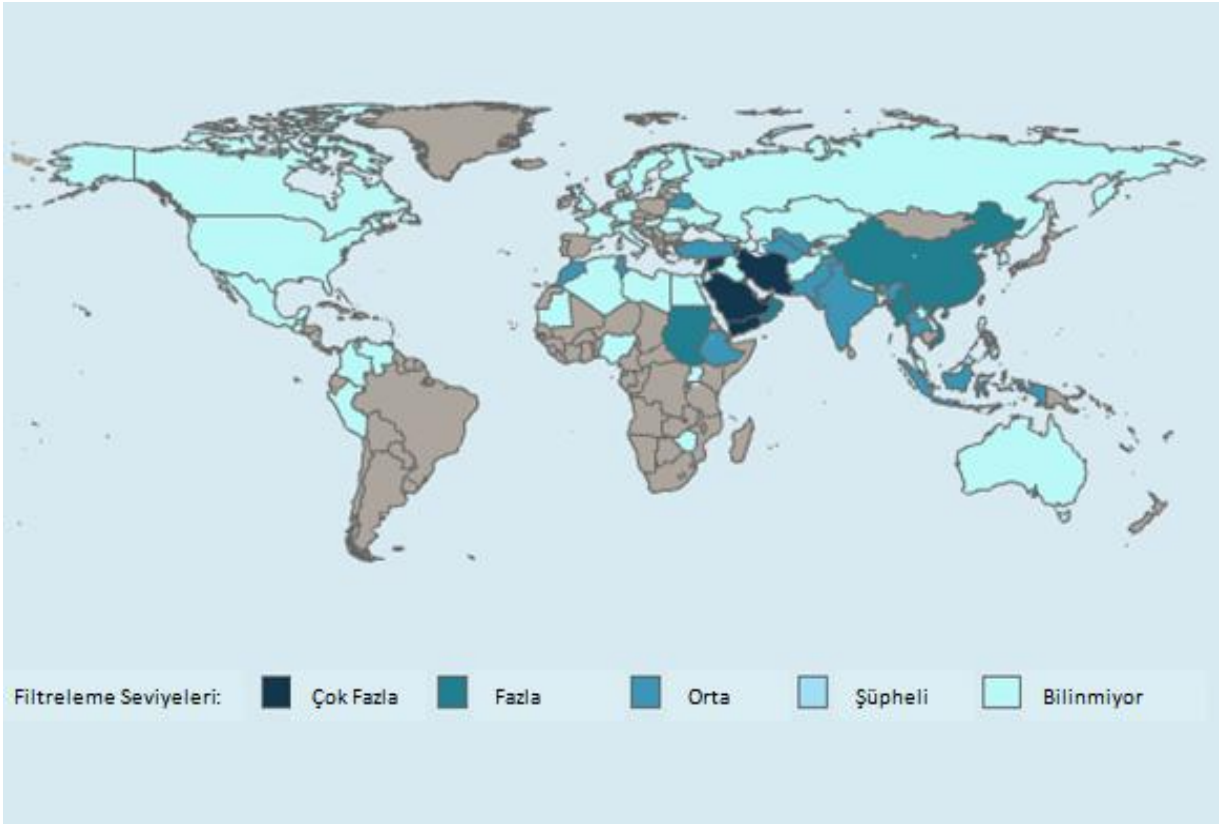
Şekil 2 Sosyal İçerik: Cinsellik, kumar, yasa dışı ilaçlar, alkol ile ilişkili ya da sosyal olarak hassas algılanan içeriklere yapılan engellemelerin haritası

Şekil 2'de cinsellik, kumar, yasa dışı ilaçlar, alkol ile ilişkili ya da sosyal olarak hassas algılanan içeriklere yapılan engellemelerin dünya üzerindeki dağılımı gösterilmektedir. Bu haritada da İran ve Suudi Arabistan dikkat çeken ülkelerdir.



Şekil 3 Güvenlik: Silahlı karışıklıklar, sınır ihtilafları, ayrılıkçı hareketler ve terörist faaliyetlerle ilgili içeriklere yapılan engellemelerin haritası

Şekil 3'te silahlı karışıklıklar, sınır ihtilafları, ayrılıkçı hareketler ve terörist faaliyetlerle ilgili içeriklere yapılan engellemelerin dünya üzerindeki dağılımı gösterilmektedir. Bu haritada Çin ve İran gibi otoriter rejimler dikkat çekmektedir.



Şekil 4 İnternet Araçları: Eposta, içerik sunucu, arama, çeviri, VoIP ve telefon hizmetleri sunan web siteleri ve engelleme atlatma yöntemlerini içeren web sitelerine yapılan engellemelerin haritası

Şekil 4'te eposta, içerik sunucu, arama, çeviri, VoIP ve telefon hizmetleri sunan web siteleri ve engelleme atlatma yöntemlerini içeren web sitelerine yapılan engellemelerin dünya üzerindeki dağılımı gösterilmektedir. Bu haritada da İran, Suudi Arabistan ve Çin dikkat çekmektedir.

A. ABD

Amerika Birleşik Devletleri İnternetin ortaya çıktığı ülke olması ve 347 milyonu aşkın[91] İnternet kullanıcısının olduğu bir ülke olması nedeniyle, İnternet yönetimi konusunda diğer ülkeler için bir model teşkil edebilecek öneme sahiptir. Bu yüzden ABD'de İnternetle ilgili gelişmeler dünya kamuoyu tarafından sürekli dikkatle takip edilmektedir.

ABD'de İnternet yasalarla çok sıkı bir şekilde denetlenmekte olup güçlü bir yasal düzenleme sistemi bulunmaktadır. ABD'deki ilk İnternet düzenlemeleri 1990'larda müstehcen içeriğin fazlalaşmasıyla yapılmaya başlamıştır[92]. Ancak üzerinden 20 yıla yakın bir zaman geçmiş olmasına rağmen İnternet üzerinden kumar oynatan siteler, siber güvenlik ve sosyal medyanın çocuklar için arz ettiği tehlike hâlâ tartışılmaktadır. Yapılan düzenlemeler çoğunlukla İnternet üzerinden kumar oynama imkânı sağlayan siteleri, müstehcen içeriği,

[91] http://www.internetworldstats.com/stats.htm adresinden alınan 2011 yılına ait değerdir.
[92] United States and Canada, http://opennet.net/research/regions/namerica.

İnternet üzerinden hakaret ve kişisel haklara saldırı ifade eden içeriği ve fikri mülkiyet ihlallerini hedef almaktadır. ABD'de teknik filtreleme – görünürde – çok olmasa da İnternet düzenlemelerle sıkı bir şekilde kontrol edilmektedir. Ayrıca ABD, teknik takibin de en sıkı olduğu ülkelerden bir tanesidir[93].

Bu günlerde[94] sanal dünya -öncelikle ABD kökenli siteler olmak üzere- 24 Ocak'ta[95] Temsilciler Meclisi'nde oylanacak olan 'Çevrimiçi Korsanlığı Önleme Yasası' (SOPA-Stop Online Piracy Act) ve Senato'ya sunulmuş olan 'Entelektüel Mülkiyetin Korunması Yasası'ndan (PIPA-Protect Intellectual Property Act) dolayı İnternet dünyasının en geniş katılımlı eylemlerinden birine tanıklık etmektedir. 18 Ocak 2012 Çarşamba günü gerçekleşen eyleme Google, Huffington Post, Pandora.com, Wikipedia, Facebook, Amazon, Reddit.com ve Github.com gibi siteler destek vermektedir. Ayrıca İnternet kullanıcılarını da tepkilerini göstermeye davet eden çok sayıda kampanyalar ve anketler düzenlenmektedir. Zira SOPA yasa tasarısına göre, ABD yetkili organları tarafından İSS'ler telif ya da ticari marka yasalarını ihlâl ettiğinden şüphelenilen ve kullanıcılarının faaliyetlerini yeterince takip etmeyen siteleri engellemeye zorlanabilecektir. Özetle, ABD bu tasarıyla öncelikle İnternetteki dosya paylaşım sitelerinin önünü kapatmayı hedeflemektedir.

Tüm sansür girişimlerine ek olarak ABD'de dosya paylaşım sitelerinin de geleceği, ünlü dosya paylaşım sitesi megaupload[96]'un erişime kapatılmasıyla tehlikeye girmiştir. Zira erişim engelleme kararının akabinde üç büyük dosya paylaşım sitesi faaliyetlerinde radikal değişiklikler gerçekleştirmiştir. FileSonic tüm dosya paylaşım özelliklerini kapatarak sadece kişisel dosya depolama hizmetine dönüşmüştür. Fileserve telif haklarını ihlal eden tüm hesapları kapatmıştır. Uploaded.to adlı dosya paylaşım sitesi de ABD'deki hizmetlerini durdurmuştur.

İnternetin ortaya çıktığı ülke olan ABD'deki gelişmeler İnternetin özgür doğasının geleceğinin hiç de parlak olmadığını göstermektedir. Zaten ABD'yi dünya ülkeleri arasında ilk olarak ele almış olmamız bu nedenledir.

B. ÇİN

2 milyara yakın nüfusu ile zaten her türlü istatistikî çalışmaya özne olan Çin Halk Cumhuriyeti 513 milyonun üzerindeki[97] İnternet kullanıcısı sayısıyla da İnternet politikaları incelemelerinde de öncelikli rol almayı hak etmektedir.

---

[93] ONI Ülke analizleri.
[94] 18 Ocak 2012.
[95] Tasarının oylanmasının gelen tepkiler üzerine süresiz olarak ertelenmesi haberi için bkz. "Statements from Chairman Smith on Senate Delay of Vote on PROTECT IP Act". http://judiciary.house.gov/issues/issues_RogueWebsites.html.
[96] www.megaupload.com.
[97] http://www.isc.org.cn/english/Focus/listinfo-18509.html adresinden alınan 2011 yılı sonuna ait değerdir.

Çin, dünyanın en gelişmiş İnternet filtreleme sistemlerine sahip olmak için olağanüstü kaynaklar harcamış ve harcamakta olan bir ülkedir[98]. Komünist Parti tekelinde tek partili politik bir düzene sahip olan Çin Halk Cumhuriyeti, hükümetin baskıcı uygulamaları sonucunda kapalı bir toplum olmaktan kurtulamamıştır. Hükümetin baskıcı politikalarının şüphesiz en önemli ayağı İnternete uygulanan sansürdür. Bugün İnternet sayesinde dünyada neler yaşandığı anında her yere ulaşmaktadır. Bunlar göz önüne alındığında Çin hükümeti devlet kontrolünü ve sosyal istikrarı sağlayabilmek için İnternet erişimine katı bir sansür uygulamakta olup medyayı da sıkı kontrol altında tutmaktadır. Her ne kadar resmiyette ve teorik olarak Çin anayasası ifade özgürlüğünü ve temel insan hak ve özgürlüklerini teminat altına alıyor olsa da, yapılan düzenlemeler İnternetin sansüre tabi olduğunu ve olacağını hem resmiyette hem de pratikte göstermektedir[99]. Çin müdahale edeceği içeriğin çerçevesini – muğlâk ifadelerle de olsa – Devlet Konseyi Bilgilendirme Ofisi (State Council Information Office) ve Sanayi ve Bilgi Teknolojileri Bakanlığı'nın (Ministry of Industry and Information Technology) 25 Eylül 2005 tarihinde yayımladığı İnternet Haber ve Bilgi Hizmetleri Yönetimine İlişkin Hükümler (Provisions on the Administration of İnternet News Information Services) adlı düzenleme ile kamuoyuna duyurmuştur[100]. Düzenlemenin 19. maddesine göre,

1. anayasadaki temel ilkeleri ihlal eden,

2. ulusal güvenliği tehlikeye atan, devlet sırlarını ifşa eden, rejimi ya da ulusun birliğini tehlikeye sokan,

3. ulus onuruna ve değerlerine zarar veren,

4. insanlar arasında kin ve ırkçılığı teşvik eden, birlik ve beraberliği bozan,

5. dinle ilgili ulusal politikaları ihlal eden ve batıl inançları yayan,

6. toplumsal düzen ve dengeyi bozucu söylentiler yayan,

7. müstehcenliği, pornografiyi, kumarı, şiddet ve terörü yayan veya suça teşvik eden,

8. üçüncü şahıslara hakaret edip aşağılayan, üçüncü şahısların yasal hak ve menfaatlerini ihlal eden,

9. kamusal düzeni bozan yasadışı oluşumları, toplulukları, toplantı ve gösterileri teşvik eden,

10. yasalar ya da kurallarla yasaklanan, her türlü içeriğin engelleneceği ifade edilmiştir. Düzenlemedeki ucu açık ifadeler, düzenlemenin keyfi uygulamalara kılıf olarak kullanılabileceğini göstermektedir.

---

[98] OpenNet Initiative, Internet Filtering in China, 15 June 2009, http://opennet.net/research/profiles/china.
[99] ONI China Filtering.
[100] Düzenlemenin Çince orijinal metni için bkz. http://www.isc.org.cn/20020417/ca315779.htm. Düzenlemenin gayrı resmi İngilizce çevirisi için bkz. http://cecc.gov/pages/virtualAcad/index.phpd?showsingle=24396.

Çin, düzenlemelerdeki insan hakları ve anayasayı koruyan ifadeleri pratikte uygulamak bir yana, bu ifadeleri gerekçe göstererek açıkça insan hak ve özgürlüklerine müdahale etmektedir. Çin dünyanın en büyük İnternet duvarına sahiptir. Öyle ki, bu duvar için Çin Seddi benzetmesi yapılmaktadır[101]. Çin bu duvarın geliştirilmesi için CISCO şirketiyle anlaşmıştır. Çin, Google, Microsoft, Yahoo gibi büyük şirketlerle işbirliği yaparak vatandaşların İnternetteki faaliyetlerini takip edebilmektedir. Bu şirketlere, Çin'deki faaliyetlerine devam edebilmeleri için ülkenin İnternet politikalarına uyum sağlamaları gerektiği zorunlu kılınmıştır[102]. Bu şirketlerden alınan bilgiler sayesinde hükümet vatandaşlarının İnternette nasıl faaliyetler içerisinde olduğunu takip edebilmektedir. Ancak bu şirketlerin Çin hükümetine sağladığı bilgiler, bu şirketlerin kendi kurumsal ilkeleri de olan, iletişimin ve kişisel verilerin gizliliği ilkelerini ihlâl etmektedir.

Çin hükümetinin uyguladığı en etkin engelleme yöntemlerinden bir tanesi de Google gibi arama motorlarında aranan kelimelerin filtrelenmesidir. Jonathan Zittrain ve Benjamin Edelman'ın ortak hazırladıkları bir araştırma[103] raporunda yayımladıkları grafik Çin'de bölgelere göre Google aramalarında filtrelenen kelimelerin oranlarını gözler önüne sermektedir. Sonuçlar oldukça çarpıcıdır. Çünkü filtrelemeye takılan kelimeler çoğunluğu itibariyle, doğrudan temel insan hak ve özgürlükleriyle ilişkili terimler ve Çin baskısından bunalmış toplumların adlarıdır. "*eşitlik*", "*demokrasi*", "*özgürlük*", "*muhalif*", "*devrim*", "*bağımsızlık*", "*adalet*", "*Tibet*", "*Tayvan*" gibi kelimeler Google aramalarında en çok filtrelenen terimler olarak göze çarpmaktadır.

Çin'deki baskı ve korku rejiminin etkileri İnternet ortamında da kendini göstermektedir. Devlet sosyal engelleme yöntemlerini de yaygın olarak kullanmaktadır[104]. Çinli kullanıcılar hukuk dışı içeriklere eriştiklerinde karşılarına İnternetteki tüm faaliyetlerin kaydedildiği ve İnternette hukuka aykırı işler yapanların ihbar edilmesi gerektiğini ifade eden bir uyarı çıkmaktadır. Ayıca İnternetteki sohbet odalarında propaganda yapmaları için devlet ajanlarını görevlendirmektedir.

Çin'de ayrıca Green Dam Youth Escort adıyla bilinen "Yeşil Duvar" yazılımının da devletin görünürde iyi niyetle aile ve çocukları koruma amaçlı teşvik ettiği bir yazılım olduğu ifade edilmektedir. Hükümet bu yazılımı bilgisayar üreticilerinden, bilgisayarı müşteriye bu yazılımla sunmalarını istemektedir. Aralarında Lenovo ve Dell'in de bulunduğu büyük firmaların herhangi bir yaptırımı olmayan bu talebi geri çevirmediği dikkat çekmektedir.

---

[101] Jack L. Goldsmith/Tim Wu, Who Controls the Internet? Illusions of a Borderless World, North Carolina 2006, a.g.e., s. 92.

[102] Kaya a.g.e., s. 63.

[103] Jonathan Zittrain ve Benjamin Edelman yaptıkları araştırmanın yöntemini de şu şekilde anlatmaktadırlar: "Testimiz iki farklı veri toplama yöntemine dayanmaktaydı: modemler ve açık proxy sunucular. 20 Mart 2002 tarihinden 6 Mayıs 2002 tarihine kadar çevirmeli bağlantı yoluyla Çinli internet servis sağlayıcılar (İSS) üzerinden bağlantı sağladık. Ancak modemlerimiz 6 Mayıs'tan sonra Çinli İSS'lerle bağlantı kuramadı. Sonrasında 14 Ağustos'tan 12 Kasım 2002'ye kadar Çin'deki açık proxy sunuculara bağlandık. Bu sunucuların yerlerini araştırma raporumuzda kullanmak amacıyla APNIC (www.apnic.net) tarafından sağlanan WHOIS (WHOIS sorgusu bir alan adının hangi özel ya da tüzel kişi adına kayıtlı olduğu bilgisini sağlayan hizmettir) hizmeti yoluyla belirledik. Test süresince ABD'den erişilebilen ancak Çin'den erişilemeyen web sitelerini ve hangi terimleri içeren aramaların ne oranda erişilemediğini tespit ettik."

[104] Kaya, a.g.e., s. 65.

Green Dam Youth Escort, Windows işletim sistemi üzerinde çalışan bir istemci programıdır. Öncelikli olarak İnternet Explorer (IE) ve diğer İnternet tarayıcılarının ve hatta Notepad gibi bazı diğer Windows uygulamalarının görüntülediği içeriği filtreler[105]. ONI (OpenNet Initiative) tarafından test edilen uygulamanın bloke ettiği içeriğin, uygulamanın yapılandırma ara yüzünde sunulan kategorilerle uyuşmadığı saptanmıştır. Yapılan testlere ve araştırmalara bakıldığında, Çin hükümetinin bu uygulamayı çocuk ve ailenin korunmasından ziyade iletişim ve kişisel bilgilerin gizliliği ilkesini ihlal edecek düzeyde bir istihbarat toplama ve İnternet içeriğini filtreleme aracı olarak kullandığı anlaşılmaktadır[106].

Çin hükümetinin tüm filtreleme uygulamalarının yanı sıra hukuka aykırı bulduğu web sitelerini engellemek için kullandığı yöntemler de oldukça kapsayıcıdır. Mesela erişim engelleme yöntemi olarak kullanılan web sunucusu IP adresi engelleme yöntemiyle[107], engellenmek istenen web sitesini barındıran sunucuya erişim engellenerek bu sunucuda barındırılan ve içeriği hukuka aykırı olmayan diğer web siteleri de erişime engellenmektedir[108]. Benzer şekilde DNS (Alan Adı Sunucusu) sunucularının da IP adresleri engellenmektedir[109]. Aynı mağduriyet engellenen DNS'te alan adı tutulan ve hukuka aykırı içerik taşımayan web siteleri için de yaşanmaktadır. Çin hükümetinin uyguladığı teknik engelleme yöntemlerinden bir tanesi de DNS yanlış yönlendirmedir (DNS redirecting). Bu yöntemle engellenmek istenen web sitesine erişmek isteyen kullanıcılar adresini girdikleri sitenin adresinin DNS tarafından farklı bir IP adresiyle eşleştirilmesiyle bambaşka bir web sitesine erişmektedirler. Ayrıca URL keyword filtering (Web adresi içeriği filtreleme) olarak bilinen filtreleme yöntemi de uygulanan teknik yöntemlerden biridir. Bu uygulamada da kullanıcıların tarayıcının adres satırına yazdıkları web adresi içerdiği kelimeler açısından sakınca arz ediyorsa, erişilmek istenen web sitesi engellenmektedir.

C. AVRUPA BİRLİĞİ

360 milyona yakın İnternet kullanıcısıyla, bir İnternet politika yapıcısı olarak Avrupa Birliği hem önemli bir İnternet aktörü hem de ürettiği politikalarla tüm dünyaya örnek olabilecek uygulamalara imza atan bir yapıdır[110].

Avrupa Birliği, İnternet erişimini engelleme ya da içerik filtreleme ve düzenleme konusunda müdahaleci olmayan ancak hangi içeriklerin hukuka aykırı ve kamuya zararlı olabileceği sınırlarını belirleyen bir politika gütmektedir. Buna neden olarak, İnternetin kendine özgü ve gelişmekte olan bir yapı olduğundan engelleme ve filtreleme yapmak için net yöntemler olmaması sebebiyle yapılacak müdahalelerin kesin sonuç vermeyeceği

[105] China's Green Dam, The Implications of Government Control Encroaching on the Home PC, OpenNet Initiative Bulletin.
[106] Jonathan Zittrain/Benjamin Edelman, Internet Filtering In China, Research Report, Berkman Center for Internet & Society, Harvard Law School Research Paper No. 62, IEEE Internet Computing (March/April 2003).
[107] Bkz. aşa. § 4 I A.
[108] Zittrain/Edelman.
[109] Bkz. aşa. § 4 I C.
[110] http://www.internetworldstats.com/stats9.htm adresinden alınan 2011 yılı sonuna ait değerdir.

düşünülmektedir. Ayrıca ifade hürriyeti ve iletişim özgürlüğü gibi temel insan hak ve özgürlüklerinin zarar görmesi istenmemektedir. Ayrıca İnternet Avrupa Bilgi Toplumu kapsamında değerlendirilmektedir. Bilgi paylaşımı, iletişim ve ticari ilişkileri geliştirmesi beklenen ve planlanan İnternetin kamusal yararının göz ardı edilemez olduğu düşünülmektedir. Yasal düzenlemelerinse ancak kesin engelleme yöntemleri elde edildikten sonra yapılabileceği görüşü hâkimdir[111]. Bu görüş, engellemeler neticesinde kapatılan web sitelerinin hızla yeniden ortaya çıkıyor olması gerekçesiyle desteklenmektedir. Öte yandan sadece web sitelerinin filtrelenmesine yönelik tasarlanan filtreleme sistemlerinin aşılabildiği de Avrupa Komisyonu tarafından benimsenmiş bir görüştür. 1998 yılında Komisyon tarafından yayımlanan eylem planında filtrelenmek istenen içeriğin P2P[112] vb. ağlarda erişime açık olduğu vurgulanmıştır.

Avrupa Birliği tarafından İnternet ve İnternetteki zararlı içerik hakkında ilk defa 1994 tarihli Avrupa Komisyonu Eylem Planında ilkeler tanımlanmıştır. Ancak bir yaptırımdan bahsedilmemiştir. Avrupa Konseyi'nin Avrupa Komisyonu'na bir düzenleme ihtiyacı hissedildiğini bildirmesiyle Avrupa Komisyonu'nun 1996'da çıkarmış olduğu İnternet'teki Hukuka aykırı ve Zararlı İçerik Tebliğinde zararlı içerikle ilgili ilk düzenlemeler yapılmıştır. Avrupa Komisyonu'nun düzenlemelerinin temelini çocuk pornografisi ve ırkçılık içeren İnternet içerikleridir. Bu iki husus üye ülkelerin çoğunun iç hukukunda zaten suç kabul edilmektedir.

Günümüzde Avrupa Birliği ülkelerinde filtreleme genellikle şu 3 şekilde yapılmaktadır:

1. Ülke sınırları içerisinde faaliyet göstermekte olan ve yasadışı içerik barındıran web sitelerinin devlet eliyle kapatılması,

2. ülke dışında faaliyet göstermekte olan ve yasadışı içerik barındıran web sitelerinin engellenmesi,

3. yasadışı içerik barındıran web sitelerinin arama motorlarınca filtrelenmesi.

Devlet eliyle gerçekleşen uygulamaların ötesinde İSS'ler, içerik sağlayıcılar ve arama motorları seviyesinde yapılan içerik filtreleme Avrupa Birliği ülkelerini diğer ülkelerden pozitif anlamda ayıran en önemli faktörlerden biridir. İSS'ler, içerik sağlayıcılar ve arama motorları sundukları içeriği daha sıkı yasal düzenleme ve devlet eliyle müdahale olmaması amacıyla filtrelemektedirler[113].

Avrupa Komisyonu tarafından hazırlanan ve 25 Ocak 1999'da kabul edilen İnternetin Güvenli Kullanımını Destekleme Eylem Planı 2002 yılına kadar yürürlükte kalmış ve aşağıdaki maddelerin uygulanmasını tavsiye etmiştir:

---

[111] Kaya a.g.e., s. 55.
[112] P2P (Peer-to-Peer), iki veya daha fazla internet kullanıcısı arasında, herhangi bir sunucu olmadan, veri paylaşmak için tanımlanmış bir ağ protokolüdür. Peer, İngilizcede eş, denk demektir.
[113] Deibert/Palfrey/Rohozinski/Zittrain a.g.e., s. 186.

1. Kendini düzenleyebilen İnternetin (self-regulating) geliştirilmesi amacıyla zararlı ve yasadışı olarak nitelenen içeriğin halk tarafından ihbar edilmesini sağlayacak hatlar kurulması,

2. çocukların İnternet erişimini düzenleyebilmesi ve kontrol altında tutabilmesi için ebeveyn ve öğretmenlere filtreleme araçları sağlanması,

3. sektör tarafından sunulan hizmetler hakkında kullanıcılar arasında farkındalığı artırarak İnternetten daha çok yarar sağlamalarına yardımcı olunması,

4. İnternetin daha güvenli kullanılmasının yasal sonuçlarının araştırılması,

5. düzenleme yapma konusunda uluslar arası işbirliğinin teşvik edilmesi[114].

Avrupa Birliği ülkeleri münferit olarak müstehcen içerikle devlet müdahalesi olmadan İSS seviyesinde yapılacak filtreleme ile mücadele etme yolunda çalışmalar yapmaktadır. Bu çalışmaların ilki ve en geniş kapsamlısı İngiltere'de, İngiltere'nin en büyük servis sağlayıcısı BT (British Telecom) tarafından Haziran 2004'te devreye sokulan Cleanfeed[115] projesidir. Proje kapsamında BT, 1978'de İngiltere Parlamentosu tarafından çıkarılan Protection of Children Act (Çocukları Koruma Yasası)[116] ile sınırları belirlenen çocuk istismarı sayılan görsel içerik barındıran web sitelerini filtrelemektedir. Filtrelenen web sitelerinin listesini de IWF (Internet Watch Foundation)[117] sağlamaktadır. IWF (İnterneti İzleme Örgütü) İnternetin kendini düzenleyen bir yapı haline gelmesi amacıyla 1996 yılında kurulmuş, kâr amacı gütmeyen bir sivil toplum örgütüdür. Sektörden, halktan, polis ve devletten gelen ihbarlar neticesinde bir kara liste oluşturup bu listenin filtrelenmesini sağlamaktadır. Kara liste İngiltere sınırları içinde yasalara aykırı derecede müstehcen içerik ile tüm dünyada çocuk pornografisi içeren web sitelerinden oluşmaktadır. IWF oluşturduğu kara listeyi İSS'leri, GSM operatörlerini, içerik sağlayıcıları ve çeşitli arama motorlarını da içeren üyeleriyle paylaşmaktadır. Kara listedeki web sitelere erişim sağlanmaya çalışıldığında bu sitelerin engellendiği açıkça belirtilmemekte, genellikle sayfanın bağlantı vb. problemlerden dolayı erişilemediği mesajı kullanıcılara iletilmektedir. Bu uygulama kanaatimizce ülkelerin özgürlükçü imajının korunması ama bir yandan da filtreleme ve engellemelerin sürdürülmesi amacıyla özellikle Avrupa Birliği ülkeleri arasında popüler bir uygulamadır. Ayrıca IWF'e devlet tarafından nasıl bir kara liste sunulduğu da açık değildir. Yani bu uygulama devlet eliyle erişim engelleme yapmaya son derece müsaittir. Benzer uygulamalar Norveç, İsveç, Danimarka ve İtalya gibi ülkelerde de devreye sokulmuştur[118]. IWF örnekleri dünyada gittikçe artan bir örgüttür. Ayrıca bu örgütleri tek bir çatı altında toplayan başka örgütler de kurulmaktadır. Bunlardan en bilineni ve en çok üyesi olan örgüt INHOPE (International Association of Internet Hotlines)[119] örgütüdür. INHOPE; ABD, İngiltere, Almanya, Fransa, Rusya, Hollanda gibi gelişmiş ülkeler ve Türkiye'nin de bulunduğu geniş bir üye kitlesine

[114] Deibert/Palfrey/Rohozinski/Zittrain a.g.e., s. 187.
[115] Cleanfeed (content blocking system), http://en.wikipedia.org/wiki/Cleanfeed_(content_blocking_system).
[116] Protection of Children Act 1978, http://www.legislation.gov.uk/ukpga/1978/37.
[117] About IWF, http://www.iwf.org.uk/about-iwf.
[118] Deibert/Palfrey/Rohozinski/Zittrain a.g.e., s. 188.
[119] About Inhope, http://www.inhope.org/gns/about-us/about-inhope.aspx.

sahiptir. Türkiye bu birliğe BTK (Bilgi Teknolojileri ve İletişim Kurumu) tarafından kurulmuş olan yerel ihbar hattı İnternet Bilgi İhbar Merkezi "ihbarweb"[120] ile katılmıştır. İnternetin kontrolü anlamında uluslar arası bir birlik oluşturulması, İnternetin sınırları ve lokasyon kısıtı olmayan doğasıyla mücadele etmeyi kolaylaştırmaktadır.

Avrupa'daki bazı ülkeler telif hakkı ihlalleriyle mücadele bağlamında erişim engelleme ve filtreleme yapmaktadırlar. Mesela Danimarka'da, Danimarka'nın en büyük İSS'i tarafından mahkeme kararıyla yasadışı müzik paylaşımında bulunan bir web sitesi Ekim 2006'da erişime kapatılmıştır. Norveç'te de 2007 yılında çok sayıda P2P paylaşım sitesi erişime kapatılmıştır. Ayrıca Belçika ve Fransa'daki bazı mahkemeler tarafından Google Haber Hizmetleri telif hakları ihlali gerekçesiyle Google şirketini yüksek miktarlarda cezalara çarptırmışlardır. Mahkemelerin Google'ı suçlu bulduğu nokta; Fransız ve Belçikalı bazı gazetelerin arama motorunda listelenmesi değil, gazetelerdeki makalelerin gazetelerin ana sayfaları atlanarak Google aramalarında direkt olarak erişilebilir olması olmuştur[121]. Ancak Avrupa Birliği'nde filtrelemeye genel yaklaşımın – konu telif haklarını korumak dahi olsa – AB vatandaşlarının temel haklarının zarar görmemesi adına özgür İnternetin savunulması olduğu European Court of Justice (ECJ – Avrupa Adalet Divanı) kararlarına bakıldığında anlaşılmaktadır. Zira bu konuda ECJ tarafından verilmiş çok önemli bir karar bulunmaktadır. 2004 yılında Belçika Besteciler Derneği SABAM'ın (Société d'Auteurs Belge – Belgische Auteurs Maatschappij) İnternet erişim sağlayıcı şirket Scarlet Extended aleyhine, şirket abonesi kullanıcıların repertuarındaki eserleri izinsiz ve telif hakkı ödemeden indirdikleri gerekçesiyle dava açmıştır. Bir Belçika mahkemesi söz konusu eserlerin Scarlet Extended tarafından elektronik olarak gönderilip alınmasını imkânsız kılmasını istemiştir. Scarlet Extended tarafından temyize götürülen karar Avrupa Adalet Divanı tarafından bozulmuş ve bir İnternet servis sağlayıcısına fikri mülkiyet haklarını korumak amacıyla filtre sistemi oluşturma ve elektronik haberleşmeyi engelleme talimatı vermenin, AB hukukuna aykırı olduğuna hükmetmiştir[122].

Avrupa Birliği ülkeleri her ne kadar İnternet konusunda özgürlükçü, sansürleme konusunda da minimalist bir imaj çizseler de, Hal Roberts ve David Larochelle'in yapmış oldukları bir araştırmada[123] İngiltere'nin başka ülkelerle bağlantıları kontrol etmek amaçlı kontrol noktaları sayısı olarak en yüksek orana sahip ülke olduğu ifade edilmektedir. Bu bilgi, İngiltere hükümetinin ülke dışına giden ve ülkeye gelen veri trafiğini sıkı sıkıya kontrol ediyor olduğu şeklinde yorumlanabilir. Sonuç olarak da iletişimin gizliliğinin ihlal edilmekte olabileceği ihtimalinin yüksek olduğu kanısına varılabilir. Ayrıca AB üye devletlerin İnternet içerik politikaları iç hukuklarında dağınık şekilde bulunmakta olup, bu devletler içerik politikalarında şeffaf değildirler. Üye ülkeler İSS'lere uyguladıkları baskı yoluyla filtrelemenin devlet eliyle yapılmadığı imajını vermeye çalışmaktadırlar. Engellemelerin birçoğu da mahkeme kararı olmadan idari makamlar tarafından İSS'lere gönderilen gizli

[120] http://ihbarweb.org.tr/.
[121] Deibert/Palfrey/Rohozinski/Zittrain a.g.e., s. 192.
[122] Kararın tam metni için bkz. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62010CJ0070:EN:NOT
[123] Hal Roberts/David Larochelle, Mapping Local Internet Control, Berkman Center for Internet & Society Harvard University, http://cyber.law.harvard.edu/netmaps/country_detail.php/?cc=CN.

listelerle yapılmaktadır. Ayrıca hangi web sitesinin hangi sebeple engellendiği de açıkça belirtilmemektedir[124]. Ancak İnternet sansürünü sadece web sitesi kapatmak olarak görmemek gerekir. Özellikle ONI'ın yayımladığı istatistiklerde genel itibarıyla ülkelerin sansür yapma seviyeleri, web sitelerinin erişime kapatılması ya da içeriklerinin teknik yöntemlerle filtrelenmesi ile doğru orantılı olarak belirtilmektedir. Bu tür aykırı uygulamalara örneklerse ONI'ın raporlarında masum görünen ülkelerden gelmektedir[125]. 2011 yılı Ağustos ayı başında İngiltere'de Mark Duggan adlı siyahî İngiliz vatandaşının silahlı bir çatışma sonucunda polis tarafından öldürülmesi sonucunda, ülkede yaklaşık 1 hafta süren isyan olayları çıkmıştır. Olaylar süresince isyancılar sosyal ağları kullanarak organize olduklarından İngiliz hükümeti, isyancıların iletişimini engellemek amacıyla Facebook, Twitter ve RIM ile toplantılar düzenlemiştir[126].

§4. ERİŞİM ENGELLEME ve ENGELLEME AŞMA YÖNTEMLERİ

İnternet temel olarak İnternet Protokolü'ne (Internet Protocol) dayalı bir sistemdir. İnternet Protokolü (IP) RFC 791[127]'deki tanımıyla, İnternet ağı üzerinde datagram adı verilen veri bloklarının iletimini ve bu blokların iletildikleri adreste yeniden bir araya getirilerek anlamlandırılmalarına imkân sağlayan kurallar bütünüdür[128]. İnterneti oluşturan bilgisayarların da birbiriyle iletişimini sağlayan TCP/IP (Transmission Control Protocol/Internet Protocol) adındaki protokoldür. Diğer bir deyişle, İnternet üzerinde bilgisayarların ortak bir dil kullanmasını ve birbiriyle anlaşabilmesini sağlamak amacıyla tanımlanmış kurallar bütünüdür. İnternetteki temel veri birimi IP paketleridir. Çok karmaşık, anlaşılmaz zannedilen İnternet iletişiminin temeli basitçe, bir bilgisayarın başka bir bilgisayara bağlanarak iletmek istediği bilgiyi IP paketlerine bölerek göndermesi ve karşı tarafın da bu paketleri birleştirerek anlamlandırmasıdır[129].

Bilgisayarlar İnternette IP adresleriyle tanımlanmaktadır. İnternet ortamına bağlanan her bilgisayarın diğer tüm bilgisayarlarınkinden farklı bir IP numarası vardır. Web sitelerini sunan bilgisayarlara da (sunucu) IP adreslerini kullanarak erişmek mümkündür. Ancak IP adresleri 192.168.0.1 gibi dört parçalı ve akılda tutulması zor adresler olduğundan web sitelerine erişim www.example.com gibi daha anlamlı ve akılda kalıcı adresler yoluyla yapılmaktadır. Alan adı kayıt sistemi (Domain Name System - DNS), IP numaralarının alan adlarıyla ilişkilendirilmesini sağlamaktadır[130]. İnternette herhangi bir bilgisayara (web

---

[124] Berber/Kaya, a.g.e., s.8.
[125] Çağdaş Aru, OpenNet İnisiyatifi 2011'deki İnternet Sansürlerinin Haritasını Çıkarttı, Türkiye 'Seçici' Olarak Sınıflandırıldı, http://turk.internet.com/portal/yazigoster.php?yaziid=36864, 25 Nisan 2012.
[126] Dinçer.
[127] Verilen tanım RFC 791 adıyla Internet Engineering Task Force (IETF-www.ietf.org) tarafından yayımlanmış bir dokümandaki tanımdır. IETF, internet ile ilgili olarak yeni ihtiyaçlar ve kavramlar ortaya çıktıkça bu kavram ve ihtiyaçlara standardize yaklaşımlar getiren herkese açık bir topluluktur.
[128] RFC: 791, Internet Protocol, Darpa Internet Program Protocol Specification, Eylül 1981, http://tools.ietf.org/pdf/rfc791.pdf.
[129] Deibert/Palfrey/Rohozinski/Zittrain a.g.e., s. 57.
[130] Deibert/Palfrey/Rohozinski/Zittrain a.g.e., s. 57.

sitesine) bağlanmak isteyen bir başka bilgisayarın (kullanıcı) bağlantı isteği önce DNS sunucularına gönderilir. DNS sunucularında tutulan IP tablolarından bağlanılmak istenen alan adının IP numarası değeri elde edildik ten sonra router (yönlendirici) bilgisayarlar tarafından bağlanılmak istenen IP'ye sahip bilgisayar ile veri paketi alış verişi başlatılmış olur.

Erişim engelleme ya da sansür işlemleri, yukarıda bahsedilen bağlantı kurulması süreçlerinden herhangi biri ya da birkaçı bölünerek yapılabildiği gibi erişim sağlamaya çalışan ya da erişilmeye çalışılan makinelerin IP adresleri engellenerek de yapılabilmektedir. Verilen bilgiler erişim engelleme ve engelleme aşma yöntemlerinin güçlü ve zayıf yanlarını değerlendirmek ve ne türlü zararların ortaya çıkabileceğini yorumlayabilmek adına önem taşımaktadır.

I. Erişim Engelleme Yöntemleri

Dünya genelinde İnternete erişimi engelleme gerekçeleri çoğunlukla çocukların pornografiden ve cinsel istismardan korunması, telif haklarının korunması, ulusal güvenliğin korunması, dini ve kültürel değerlerin korunması ekseninde şekillenmektedir. Gerekçenin engellemeyi yapacak otorite nezdindeki ciddiyeti, kullanılan engelleme yöntemlerinin niteliğini ve engelleme için yapılacak yatırımın maliyetini belirlemektedir.

A. IP Engelleme

Her web sitesi İnternet üzerinde bir web sunucu üzerinde yayın yapmaktadır. Web sunucular genellikle birden fazla web sitesini ya da İnternet hizmetini aynı anda sunmaktadır. Web sitelerine erişim web sunucuların IP adresleri üzerinden gerçekleşmektedir. DNS sunucularına gönderilen bağlantı istekleri neticesinde DNS'ten gelen cevapta bağlanılmak istenen web sitesinin barındırıldığı sunucunun IP adresi bulunmaktadır. IP engelleme yönteminde engellenmek istenen web sitesinin barındırıldığı web sunucunun IP adresi engellenmektedir. Yani DNS'ten gelen cevapta engellenmesi gereken bir IP adresi mevcutsa, bu IP adresinden gelen IP paketleri router tarafından görmezden gelinir ve bu paketler son kullanıcıya asla ulaştırılmaz.

IP engelleme yöntemi oldukça temel bir engelleme yöntemi olup İSS'ler için hiçbir ek yatırım gerektirmemektedir. Hiçbir akıllı yazılım ve donanım sistemiyle desteklenmediği için hem engellemenin aşılması oldukça kolay ve masrafsızdır, hem de yapılan engelleme – engellenmeye çalışılan içerik her ne kadar yasadışı da olsa- adaletsiz olabilmektedir.

Engellenmeye çalışılan web sitesinin barındırıldığı sunucu üzerinde yayın yapan diğer tüm web siteleri de engellemeden nasibini almakta olduğu için bu engelleme yöntemiyle hiçbir kamu yararı gözetilmemektedir. Ayrıca bu yöntem kullanılarak yapılan engellemelerin amacına ulaşması oldukça zordur. Zira engellenmesi amaçlanan web sitesi başka bir sunucuya

taşındığında IP adresi de değişmiş olacağından bu web sitesine erişim yeniden mümkün olacaktır. Ayrıca web sitesinin barındırıldığı sunucu değiştirilmeden, sunucunun IP adresini de değiştirmek mümkündür. Bu durumda da erişime kapatılmak istenen web sitesine erişmek yeniden mümkün olacaktır.

Bütün dezavantajlarına ve aşılmasının kolaylığına rağmen yine de bu yöntem kullanılacaksa da kamu zararının azaltılması adına "port"[131] engelleme kullanılarak daha spesifik bir engelleme yapılabilir[132]. Bir web sunucusu üzerindeki farklı İnternet hizmetleri farklı portlardan yayına sunulmaktadır. Dolayısıyla, hedef sunucu üzerindeki web trafiğinin sağlandığı portun engellenmesiyle sunucu üzerinden sağlanan diğer hizmetler gereksiz yere engellenmemiş olur.

B. IP Paket Filtreleme

Bir önceki başlıkta anlatılan IP engelleme yöntemi, paketlerin sadece ulaşacakları noktaları ya da çıkış noktalarını engellemekte, bir içerik kontrolü yapmamaktadır. Yasaklı içerik sunan IP'lerin tamamını listelemek mümkün olmadığında ya da sunduğu içeriğin çok az bir kısmı yasaklı içerik olan IP'ler bulunduğunda bu yöntem çok kullanışlı olmayacaktır[133]. Ayrıca yasaklı içerik barındıran IP'ler yasaklansa dahi, sunulan içeriğin barındırıldığı IP ya da sunucu değiştirilerek yasaklı içeriği engellenmekten kurtarmak son derece kolaydır. Bu durumda daha etkili bir yöntem olan paket filtreleme kullanılabilir.

IP paket filtreleme yöntemi, paket içeriğinin okunması ve zararlı içeriğin varlığının kontrolünü gerektirdiği için yüksek performans gerektiren bir işlemler dizisidir. Bu performans router makinelerinden beklenemeyeceği için ekstra donanım ve yazılımlara ihtiyaç vardır. Denetlenen paketler içerisinde fark edilen yasaklı içeriği barındıran paketlerin iletimi engellenir ya da iletimi gerçekleştiren taraflara uyarı mesajı gönderilir. Bu tip filtrelemeyi yapan en bilinen örnekler güvenlik duvarı yazılımları ve bu işlem için özelleşmiş güvenlik duvarı donanımlarıdır.

IP paket filtreleme yönteminin yasaklı içeriği göz ardı edebileceği durumlar da mevcuttur. Mesela yasaklı içeriğe dair bir kelimenin bir kısmı bir pakette, diğer kısmı bir sonraki pakette iletiliyorsa filtreleme mekanizması bu içeriği anlamlandıramayacağı için filtrelemeye ihtiyaç duymayacaktır. Bu durumda sistemin maliyetini daha da artıracak yeni bir kabiliyete ihtiyaç duyulacaktır. İçeriği denetleyen sistem, paketleri tek tek alıp bir ortamda birleştirerek anlamlandırmalı ve filtrelemeyi ondan sonra yapmalıdır. Bu yönteme daha

---

[131] Ulaşılan bir sunucu üzerindeki programlardan ya da hizmetlerden hangisine erişilmek istendiği, daha önceden tanımlanmış soyut bağlantı noktaları belirtilerek ifade edilir. Bu soyut bağlantı noktaları, değerleri pozitif sayılardan ibaret olan **port**lardır.

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

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

kullanışlı bir alternatif olarak ilerleyen bölümlerden birinde ele alınan HTTP proxy filtreleme yöntemi kullanılabilir[134].

C. DNS Engelleme

İnternet erişiminin tamamına yakını DNS sistemi[135] üzerinden yapılmaktadır. Web sitelerinin barındırıldığı sunucuların IP adresleri (74.123.456.11 gibi) akılda kalıcı olmadığı için web sitelerine erişim için daha akılda kalıcı ve anlamlı adresler kullanılmakta ve bu adresler IP numaralarıyla DNS sunucuları üzerinde eşleştirilmektedir. Kullanıcılar erişmek istedikleri web sitesinin adını önce DNS sunucularına gönderip, DNS sunucusundan dönen IP adresine bağlanma isteği göndermektedirler. Dolayısıyla DNS sistemindeki adres çözümleme aşaması filtrelenirse, yasaklı siteler de büyük ölçüde engellenmiş olur[136]. DNS sunucularına tanımlanan yasaklı web site adresleri sayesinde DNS sunucularının yasaklı web siteleri için adres çözümlemesi yapmaması sağlanmış olmaktadır. Bu sitelere bağlanma talebi geldiğinde DNS sunucusu tarafından kullanıcıya ya bir hata mesajı iletilmekte ya da hiçbir cevap dönülmemektedir. Web sitelerinin IP adresleri de kullanıcılar tarafından çok fazla bilinmediğinden bu sitelere erişim engellenmiş olmaktadır. Bu filtreleme sistemi de hiçbir ek maliyet gerektirmemektedir.

D. URL Engelleme

URL (Uniform Resource Locator) yani tekil kaynak konumlandırıcısı, İnternette herhangi bir web sitesinde barındırılan herhangi bir kaynağa (yazı, resim, video gibi) direkt erişim imkânı sunan adrestir. URL engelleme yöntemiyle, URL'i bilinen ve engellenmek istenen herhangi bir kaynak engellenebilmektedir. Bu yöntemin en önemli avantajı kanun dışı bir içerik barındırdığından dolayı tüm web sunucusunun engellenmesi bir yana, tüm web sitesinin de engellenmesini önlemesidir[137]. Ancak bu yöntem İSS'ler seviyesinde çok kullanışlı değildir. Zira zararlı içeriğin URL'i kolaylıkla değiştirilebilmektedir. Bu yöntem ev kullanıcıları için kullanışlı bir yöntem olup, modem aygıtları çoğunlukla URL engelleme için kullanıcılarına bir ara yüz sağlamaktadır.

Özellikle İngiltere'de uygulanan CleanFeed projesi ile URL engelleme yöntemi aktif bir şekilde kullanılmaktadır. Ancak söz konusu projede URL engelleme yöntemi bilinen en basit yöntemiyle kullanılmamakta, packet inspection (paket içeriği algılama) teknolojileri kullanılarak trafik içinde gidip gelen paketler tek tek incelenmek suretiyle sakıncalı içerik

---

[134] Deibert/Palfrey/Rohozinski/Zittrain a.g.e., s. 60.
[135] Bkz. yuk. § 4.
[136] Deibert/Palfrey/Rohozinski/Zittrain a.g.e., s. 61.
[137] Kaya, a.g.e., s. 32.

tespit edilmektedir[138]. Masum ve İnternet kullanıcılarının mağduriyetini önlemek amaçlı gibi görünen bu uygulama aslında trafikteki bütün paketlerin analizini yaparak hangi adresten hangi hedefe gitmekte olduklarını belirlemektedir. Bu durumda da özel hayatın gizliliği, kişisel verilerin güvenliği tehlikeye girmektedir. Ayrıca analizi yapılan paketlerden elde edilen kullanıcılara ait bilgilerin istihbarat elde etme amaçlı kullanılma ihtimali de bulunmaktadır. Netice itibariyle İnternet içeriğini filtrelemek için kullanılan en masum görünen teknikler bile kullanıcılar açısından büyük riskler içerebilmektedir.

E. Anahtar Kelime Filtreleme / IP Paketlerini Anlamlandırarak Filtreleme

Yukarıda bahsedilen URL filtrelemedeki URL'in içerdiği sakıncalı kelimeleri filtrelemenin ötesinde bu yöntemle IP paketlerinin içeriği anlamlandırılarak filtrelenmektedir. Söz konusu yöntemin karmaşıklığı ve maliyeti, bir router makinesinden beklenen anlamlandırma kabiliyetinden anlaşılmaktadır. Zira bildiğimiz anlamda bilgisayar işlemcisine sahip routerların IP paketlerini anlamlandırarak hukuka aykırı içeriğin parçaları olduğuna karar vermesi çok yüksek hesaplama kabiliyeti gerektirir. Günümüz teknolojisinde bu yöntemin kullanımı çok etkili sonuçlar vermemekle beraber oldukça yüksek maliyetler sunmaktadır. Anahtar kelime filtreleme yöntemi IP paketlerinin şifrelenerek iletilmesiyle aşılabilmektedir[139]. Çünkü şifreli IP paketleri, varacağı hedefe varıp şifresi çözülene kadar içerdiği orijinal veri ile tamamen alakasız veriler taşımaktadır. Dolayısıyla araya girip paketleri inceleyen router makinesi ele geçirdiği paketleri anlamlandıramamaktadır. Http protokolü yerine HTTPS protokolü kullanan web siteleri anahtar kelime filtrelemeye takılmamaktadır. Buna benzer olarak hukuka aykırı görüntü dosyalarının da filtrelenmesi basit kelime filtreleme yöntemleriyle filtrelenememektedir. Görüntü dosyaları için hesaplama gücü, kelime filtreleme için gerekli olan hesaplama gücünden çok daha yüksek makinelere ve buna ek olarak güçlü görüntü işleme (image processing) yazılımlarına ihtiyaç duyulmaktadır. Bu tür yazılımlar IP paketlerini bir araya getirerek görüntü dosyalarını bütün olarak incelemektedir. Mesela bir görüntü dosyasındaki ten rengine denk gelen alanlarda müstehcen içerik olduğu sonucuna varabilmektedirler. Bu yazılımlarla maliyet daha da artmaktadır. Ancak yüksek maliyetlere ve aşılmasının kolaylığına rağmen, başta Çin olmak üzere, bu yöntemi kullanan ülkeler mevcuttur[140].

---

[138] Richard Clayton, Anonymity and traceability in cyberspace, Technical report, University of Cambridge Computer Laboratory, Number 653, November 2005, http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-653.pdf, a.g.e. s. 117.

[139] Hal Roberts/Ethan Zuckerman/John Palfrey, 2007 Circumvention Landscape Report: Methods, Uses, and Tools, The Berkman Center for Internet & Society at Harvard University, March 2009, http://cyber.law.harvard.edu/publications/2009/2007_Circumvention_Landscape_Report, a.g.e., s. 12.

[140] Roberts/Zuckerman/Palfrey, a.g.e., s. 12.

F. Proxy Engellemesi

Proxy dilimize İngilizce'den teknik bir terim olarak geçmiş, Türkçe anlamı "vekil" olan bir kelimedir. Proxy sunucular pratikte İnternet içeriği ile kullanıcılar arasında kullanılır. Proxy sunucuların çeşitli kullanım amaçları vardır. Proxy sunucu kullanılarak bir ağdaki kullanıcıların İnternet içeriğine doğrudan erişmeleri engellenir. Bu yöntemle genellikle ağ güvenliğinin sağlanması ve ağ trafiğinin hafifletilmesi amaçlanmaktadır. Çünkü proxy sunucusu gelen bağlantı talepleri sonrasında bir kullanıcının erişimine sunduğu bir web sitesinin içeriğini önbelleğinde tutar. Aynı web sitesine aynı ağdan başka bir bağlantı isteği geldiğinde proxy, bu web sitesinin barındırıldığı web sunucusuna bağlantı isteği gönderme ihtiyacı duymaz. Bu durumda önbelleğinde tuttuğu veriyi kullanıcıya sunar. Bu şekilde ağ trafiği önemli ölçüde azalmış olur. Ayrıca proxy sunucu kullanımı ile kullanıcıların ağda kullandıkları bilgisayarlar İnternet içeriği ile doğrudan temasta olmadıklarından İnternetten gelebilecek virüs ve benzeri kötücül yazılımlardan da korunmuş olurlar. Yani proxy sunucu İnternetten gelen verileri filtreleyerek kullanıma sunar. Zira proxy makinesi için İnternet içeriğini filtrelemek gayet kolaydır, çünkü zaten içerik önbelleğinde mevcuttur. Proxy kullanımının bir diğer kullanışlı yönü de, İnternet kullanıcılarının kimliklerini gizleme imkânı sunmasıdır. Proxy sunucularının filtreleme kabiliyetleri devletler tarafından da İnternet erişiminin kontrol altında tutulması amacıyla kullanılmaktadır. İSS'lerin kullanıcılarla veri arasına konumlandırdıkları proxylerle kullanıcılara ulaştırılması istenmeyen içerik filtrelenmektedir.

G. DDoS (Distributed Denial of Service) Saldırıları

DDoS[141] saldırıları bir bilgisayarın, ağın ya da daha genel bir deyişle bir bilgi sisteminin, gereksiz sorgularla sunduğu hizmeti yavaşlatmak ya da sistemi tamamen işlemez hale getirmek amacıyla yapılan bir siber saldırı türüdür. Siber güvenlik dünyasında da henüz kesin bir çözümü bulunmayan saldırı yöntemi ile hedefe alınan hemen her sisteme – eğer güvenlik personeli anında müdahale edemezse – ciddi zararlar verilebilir, işlerliği ortadan kaldırılabilir. Bu yönüyle hukuk dışı olmasına rağmen DDoS saldırıları uygulanabilecek en etkili erişim engelleme yöntemlerinden biridir. Virüs ya da değişik kötücül yazılımlar bulaştırılan yüzlerce, hatta binlerce bilgisayar, kullanıcıları farkında olmadan, saldırganın hedef gösterdiği sisteme hizmet talebinde bulunmak için bağlanmaya çalışır. Tüm bağlantı taleplerine cevap vermeye çalışan sistem nihayetinde bu talepleri karşılayamaz duruma gelerek ya verdiği hizmet süresi makul süreleri aşar ya da sistem tamamen çöker. Bu yöntemi – hukuk dışı da olsa - uygulayan otorite erişim engelleme amacına bu şekilde ulaşmış olur.

DDoS yöntemiyle erişim engelleme yoluna giden devletler genellikle kendi hukuki kontrol alanları dışında kalan ve kendi iç hukuklarına aykırı yayın yapan web sitelerini engelleyebilmek amacıyla bu yola başvururlar. Yani ülke dışında yayın yapıp, yayın yaptığı ülkenin hukuk kurallarına tabi de olsa bir web sitesi eğer başka bir ülkenin hukuk kurallarına

[141] Bkz. yuk. § 2 III B 3.

aykırı yayın yapıyorsa DDoS saldırılarına maruz kalabilmektedir. Ayrıca dünyada, bir ülkenin sınırları içerisinde hukuka aykırı yayın yapıp erişime engellendikten sonra ülke sınırları dışında faaliyetlerine devam eden pek çok web sitesi bulunmaktadır. Böyle durumlarda da DDoS yöntemi devletler tarafından sıkça tercih edilmektedir.

H. DNS' ten Alan Adı Kaydı Silme

Bir web sitesine bağlanmanın ilk aşaması yerel DNS' e erişmektir[142]. Bütün alan adlarını aynı sunucuda barındırmak mümkün olmadığından ilk erişilen DNS sunucusu cevabını bilmediği sorguyu hiyerarşik sıralamada kendinden bir üstteki sunucuya gönderir. Bu şekilde cevap dönene kadar istek hiyerarşik sistemde ilerler. Ülkelerin ulusal uzantılarını tutan ulusal DNS sisteminin en üstünde bulunan sunuculardan ".tr", ".de" gibi ulusal uzantılara sahip web sitelerinin alan adları silindiği takdirde bu web siteleri erişilemez duruma gelmektedir.

DNS'ten alan adı silme yöntemi sadece ulusal olarak uygulanabilecek bir yöntem olmayıp alan adlarının yönetimi uluslararası bir kuruluş olan ICANN tarafından yapıldığı için bu yöntemin uluslararası bir boyutu bulunmaktadır. ICANN (Internet Corporation for Assigned Names and Numbers), 1998 yılında ABD tarafından, özerk olarak çalışan ve kâr amacı gütmeyen bir kuruluş olarak uluslararası alan adları sisteminin teknik yönetimini yapmak üzere yetkilendirilmiş bir yapıdır. Normal koşullarda her gerekçeyle alan adı silme işlemini yapamayan ICANN, ABD'de Ocak 2012'de rafa kaldırılan yasa tasarısı SOPA'nın vermiş olduğu yetki ile mahkeme kararı olan her türlü alan adı silme işlemini yapmaya yetkili olabilecekti[143]. SOPA'nın en çok tartışılan yönlerinden bir tanesi de varlığı tartışmalı olan ICANN'e bu yetkileri veriyor olmasıdır.

I. Diğer Yöntemler ve Değerlendirme

Erişim engelleme yöntemlerinden sıkça kullanılan yöntemlerden olan sunuculara fiziksel müdahalede bulunma yöntemi anlatılan yöntemler arasında en az teknolojik olanı olarak dikkat çekmektedir. Hukuka aykırı içerik barındırdığı tespit edilen web sunucusunun İnternet bağlantısı kesilerek ya da söz konusu sunucuyu ya da sunucuları işleten şahıslardan sunucunun devre dışı bırakılması talep edilerek içeriklerin İnternette yayımlanması durdurulur.

Teknik erişim engelleme yöntemleri genellikle – bazıları zor da olsa – aşılabilir yöntemler olup, bugüne kadar aşılamayan bir erişim engelleme yöntemi uygulanamamıştır. Ancak başlı başına bir erişim engelleme yöntemi olmayıp, devletler açısından daha etkili

---

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

[143] Mark Jeftovic, How SOPA Will Destroy The Internet, 22.12.2011, http://blog2.easydns.org/2011/12/22/how-sopa-will-destroy-the-internet/.

sonuçlar ortaya çıkarabilecek bir yöntem de online takiptir. İnternet kullanıcılarının, İnternette gezinirken ne tür içeriklere eriştiğinin, hangi web sitelerine bağlandığının takibinin yapılması ve buna ek olarak vatandaşların mütemadiyen takip edildikleri konusunda bilgilendirilmesi oldukça etkili bir erişim engelleme yöntemi olmaktadır. Zira bu yöntemi Çin hükümeti etkili bir şekilde kullanmaktadır[144]. Aslında bu yöntem takip yapılmıyor ya da yetersiz yapılıyor olsa bile, vatandaşların takip ediliyor oldukları şeklinde sürekli uyarılıyor olmaları durumunda da İnternet kullanıcıları üzerinde psikolojik etkiler uyandırdığından, etkili olmaktadır[145].

Bir erişim engelleme yöntemi olmasa da çeşitli yöntemlerle engellenmekte olan web sitelerinin İnternet kullanıcıları tarafından erişilmeye çalışıldığında ekrana "Web sitesine erişilemiyor.", "Ağ hatası oluştu.", "Desteklenmeyen içerik" gibi hata mesajları verilmesi yöntemi özellikle kişi hak ve hürriyetlerine saygılı, demokratik ve çağdaş bir görüntü vermeye çalışan ülkeler tarafından sıklıkla kullanılabilecek bir yöntemdir. Bu yöntem AB'ye üye devletler tarafından sıklıkla kullanılan bir yöntemdir[146]. Ülkemizde ise bu konuda şeffaf bir uygulama söz konusudur (Şekil 5).

Şekil 5 Türkiye'de erişime kapatılan web sitelerine erişilmeye çalışılırken karşılaşılan ana sayfa görüntüsü.

İnternetin ortaya çıktığı ülke olan ABD'de de çoğunlukla şeffaf bir uygulamaya rastlanılmaktadır (Şekil 6).

---

[144] Bkz. yuk. § 3 II B.
[145] Deibert/Palfrey/Rohozinski/Zittrain a.g.e., s. 65.
[146] Berber/Kaya, a.g.e., s.8.

Şekil 6 Megaupload'un erişime engellenmesiyle ortaya çıkan ana sayfa görüntüsü

İnternete erişimin engellenmesi ya da erişim takibinin yapılması nihayetinde özel yaşama müdahaledir ve iletişim özgürlüğünü kısıtlayıcıdır. Bu yüzden erişim engelleme yöntemleri mümkün olduğunca yerini toplumsal oto kontrol mekanizmalarına bırakmalıdır. Mesela aile içinde çocuğun zararlı içerikten korunmasına yardımcı olabilecek bazı basit tedbirler almak mümkündür. Çocukların kullandığı bilgisayar ev içerisinde ailenin genellikle bir arada olduğu oturma odasında, ekranı odadaki herkesçe görülebilecek şekilde konumlandırılabilir[147]. Ayrıca her aile çocukları için filtreleme seviyesini ebeveynlerin de ayarlayabilecekleri İnternet filtreleri kullanabilir.

II. Engelleme Aşma Yöntemleri ve Yan Etkileri

Engelleme aşma yöntemleri ve araçları, İnternet kullanıcılarını evde, okulda, işyerinde ya da hükümet tarafından ülke genelinde erişimi engellenmiş içeriğe ulaşabilmelerini sağlayan yöntemlerdir. Engelleme aşma yöntemleri ve araçları, erişim engelleme yöntemlerine göre farklılık arz etmektedir. Ancak temelde, engelleme aşma yöntemleri ya IP

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

paketlerinin varacağı hedefin gizlenmesi, ya IP paketlerinin içerdiği verinin gizlenmesi ya da her ikisinin de gizlenmesi hedefi gözetilerek geliştirilmektedir[148].

Yapılan araştırmalar göstermektedir ki tüm dünyadaki İnternet kullanıcıları, engellenen bir web sitesine erişebilmek için çoğunlukla herkese açık HTTP proxy sitelerini kullanmaktadırlar[149]. Bu yüzden kullanıcılar en fazla güvenlik riskine de bu proxy siteleri nedeniyle maruz kalmaktadırlar. Ülkemizde de durum hemen hemen aynıdır. Zira İnternet kullanıcıları bir web sitesine erişemediklerinde çoğunlukla arama motorlarını kullanarak "proxy" diye aratmakta ve arama sonuçlarında çıkan açık proxyleri kullanmaktadırlar. Diğer engelleme aşma yöntemlerinin de yan etkileri vardır ancak en sık kullanılan yöntem proxy siteleri olduğundan ve bu siteleri genellikle sanal güvenlik konusunda bilinçsiz kullanıcılar kullandığından güvenlik açıkları çoğunlukla bu sitelere erişimden kaynaklanmaktadır.

A. Teorik Anlamda Engelleme Aşma Yöntemleri

İnternet kullanıcılarının erişimi engellenen içeriğe ulaşmak için kullandıkları pek çok engelleme aşma yöntemi bulunmaktadır. Proxy yöntemleri erişilecek sunucuyu gizlerken, şifreleme yöntemleri de erişilen içeriği gizlemektedir. Yani farklı engelleme aşma tekniklerini birbirinden ayıran en temel farklılık erişilen sunucuyu gizleme ya da erişilen içeriği gizleme farklılığıdır[150].

1. Proxy Yöntemleri

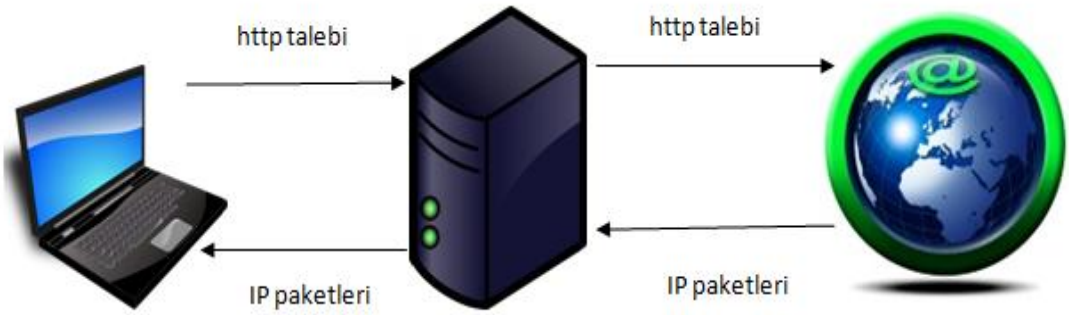
Proxy yöntemleri erişilmek istenen ancak erişimi engellenmekte olan sunuculara erişim amacıyla kullanılır. Proxy yöntemleri IP engellemeyi ve DNS engellemeyi aşmada etkilidir.

a) Http Proxy

HTTP proxy yöntemi dünyada en kolay ve en sık kullanılan engelleme aşma yöntemlerinden biridir. İnternet kullanıcıları kullandıkları İnternet tarayıcı programını proxy olarak kullanacakları sunucuya göre ayarlayarak İnternete bağlanabilmektedirler. Engelleme yapılan ülkedeki kullanıcılar başka bir ülkede bulunan proxy sunucusuna bağlanarak HTTP isteklerini normalde bağlanmak istedikleri web sitesine bağlanır gibi bu makineye göndermektedirler. Proxy sunucusu da gelen HTTP isteklerini doğrudan erişilmek istenen web sitesine bağlanarak ve erişilmek istenen içeriği paketler halinde kendi üzerinden talebi yapan kullanıcıya ileterek erişime olanak sağlamış olmaktadır (Şekil 7).

---

[148] Roberts/Zuckerman/Palfrey, a.g.e., s. 13.
[149] Roberts/Zuckerman/York/Faris/Palfrey, a.g.e., s. 2
[150] Roberts/Zuckerman/Palfrey, a.g.e., s. 13.



Şekil 7 Http Proxy yöntemi ile engelleme aşma

Kullanıcılar proxy sunucuları, genellikle İnternet üzerinde herkese açık hizmet veren proxy sunucuları listeleyen web sitelerini kullanarak bulmaktadırlar. Ancak filtreleme yapan ülkelerde genelde bu türlü siteler de engellenmektedir[151]. HTTP proxy kullanımının hem kullanıcı açısından, hem genel olarak ülke açısından ciddi yan etkileri bulunmaktadır. Proxy kullanımı, İnternet kullanıcısının erişime engellenen içeriğe ait tüm IP paketlerini aradaki proxy sunucusu üzerinden aldığı tekniktir. Bu yüzden kullanılan proxy sunucusu güvenilir bir partiye ait değilse kullanıcının anonimliği ve mahremiyeti tehlikede demektir.

Proxy sunucuların esas kullanım amacı, kurumsal ağ ya da İSS seviyesinde İnternet erişim hızını artırmak ve ağ güvenliğini tehdit eden içeriği filtrelemektir. Proxy sunucular çoğunlukla bu amaçlar doğrultusunda kullanılmaktadır.

b) CGI Proxy

CGI (Common Gateway Interface)[152] Proxy yöntemi kullanımı en kolay engelleme aşma yöntemlerinden biridir. Bu yöntemin kullanımı HTTP proxy kullanımından bile kolaydır. CGI proxy kullanımı hiçbir ekstra ayar yapmaya ya da istemci bilgisayarında herhangi bir program kurmaya lüzum bırakmamaktadır. Kullanıcılar İnternet üzerinde herkese açık hizmet sunan herhangi bir CGI proxy sitesine erişerek bu hizmetten faydalanabilmektedirler. Bu sayede istenilen engelli web sitelerine hızlı bir şekilde bağlanmak mümkün olmaktadır. Ayrıca herhangi bir program yüklemek ya da ayar yapmak gerekmediğinden okul, kütüphane ya da İnternet kafe gibi halka açık yerlerde de bu hizmetten faydalanmak mümkündür.

---

[151] Roberts/Zuckerman/Palfrey, a.g.e., s. 13.

[152] CGI, RFC 3875 dokümanında tanımlanmış bir standarttır. Web sunucusu yazılımları için web sayfalarının istemci bilgisayarlarında çalıştırılabilir programcıklara dönüştürülmesini sağlayan betikler için bir standarttır. Bu betikler CGI betikleri (CGI Scripts) olarak bilinir.

CGI proxy kavramı, web sunucusu üzerinde çalışan bir betiğin[153] web sunucusunu proxy sunucu olarak çalıştırmasından ibarettir. Engelleme aşma mekanizması HTTP proxy ile tamamen aynıdır (Şekil 7). İnternet kullanıcısı erişmek istediği engelli web sitesinin URL'sini bir HTTP talebinin veri kısmına gömerek CGI proxy sunucusuna gönderir. CGI proxy sunucusu erişilmek istenen adres bilgisini http isteği içerisinden alır ve hedefe kendi HTTP isteğini göndererek bağlanır ve gelen IP paketlerini kendi istemcisine ulaştırır[154]. CGI proxy sunucuları kullanıcılarına genellikle, normal web tarayıcısı üzerinden kendisine özgü bir arayüz sağlamaktadır. Bu arayüz çoğunlukla bağlanılmak istenen engelli web sitesinin adresinin girileceği ekstra bir adres satırı içermektedir.

CGI proxy hizmeti sunan sunucuların listesini sağlayan pek çok web sitesi mevcuttur. Ancak CGI proxy yöntemi, HTTP proxy yönteminden farklı olarak çoğunlukla erişim engelleme ve anonimliği sağlama amaçlı kullanıldığı için bu hizmeti sunan web siteleri ve bu hizmeti sunan web sitelerini listeleyen web siteleri, engelleme yapan devletler tarafından sıkı bir şekilde engellenmektedir. Bu yüzden CGI proxy hizmetine erişim HTTP proxy hizmetine erişim kadar kolay olmamaktadır.

c) IP Tunneling (IP Tünelleme)

IP tunneling teknolojisi birçok farklı uygulamada kullanılmaktadır. Bu uygulamalar genellikle ticari kullanım amaçları olan ve engelleme aşma yöntemi olmayan uygulamalardır. Ancak engelleme aşmaya da olanak sağladığı için engelli web sitelerine erişim amaçlı olarak da kullanılmaktadır.

IP tunneling teknolojisinin en çok kullanıldığı uygulamalardan biri VPN'lerdir (Virtual Private Networks). Dilimize özel sanal ağlar olarak çevirmek mümkün olan VPN kavramı kullanıcılarına eposta, anlık mesajlaşma, dosya paylaşımı gibi uygulamaların kullanımına imkân sağlayan; daha çok kurumsal amaçlarla, şirketlerin birbirinden uzakta bulunan çalışanları arasındaki etkin iletişimi sağlayan özel bir intranet uygulamasıdır. Yani VPN uygulaması ile kullanıcılar dünyanın farklı yerlerinde olsalar dahi bir VPN sunucu üzerinden hem birbirlerine, hem İnternete bağlanabilmektedirler. Bu durumda kullanıcılar bulundukları ülkede erişime engellenen herhangi bir içeriğe, VPN sunucusunun bulunduğu ülkede engelleme getirilmiyorsa, VPN sunucusu üzerinden erişebilmektedirler. VPN uygulamalarında temel olarak HTTP istek ve cevapları yerine gidip gelen IP paketleri '*tünellenmektedir'* (şifrelenmektedir). Ancak VPN'lerin tespit edilmesi çok kolaydır ve engelleme aşma amaçlı olarak kullanılıp kullanılmadığının tespiti çok zordur[155].

IP tunneling teknolojisini kullanan, daha basit bir mekanizması olan ve çoğunlukla engelleme aşma amaçlı olarak kullanılan bir diğer yöntem HTTP tunneling yöntemidir. Bu yöntem, VPN'lerden farklı olarak HTTP istek ve cevaplarını '*tüneller'* (şifreler). Bu sayede

[153] Betik kavramı yazılım terminolojisi çerçevesinde kısaca kod parçası olarak tanımlanabilir.
[154] Roberts/Zuckerman/Palfrey, a.g.e., s. 14.
[155] Roberts/Zuckerman/Palfrey, a.g.e., s. 15.

gönderilen ve alınan HTTP istek ve cevapları filtrelemeye takılmadan hedefe ulaşır. Engelleme aşma amaçlı olarak İnternette hizmet veren pek çok IP tunneling sitesi mevcuttur. Bu sitelerden hizmet almak için kullanıcıların bilgisayarlarına herhangi bir program kurmalarına ya da ayar yapmalarına gerek bulunmamaktadır. IP tunneling hizmeti veren web siteleri genellikle ana sayfalarında erişilmek istenen içeriğin URL'sinin girileceği bir adres satırı bulundurur. Proxy uygulamalarına benzer olarak istemcilerin mahremiyeti IP tunneling hizmeti veren sunucuları yöneten kişilerin inisiyatifinde bulunmaktadır.

d) Trafik Yönlendirme (Çoklu Proxy Kullanımı)

İstemci makinelerinin de –gönüllü olmaları halinde- aynı zamanda proxy işlevi görebildiği bir engelleme aşma yöntemi olan çoklu proxy kullanımı, istemcilerin makinelerine kuracakları bir program ile bağlanabildikleri bir proxy ağından ibarettir. Bu yöntem genellikle engelleme aşma yöntemi olarak kullanılmaktadır.

Çoklu proxy kullanımı yönteminde VPN proxy, CGI proxy ya da HTTP proxy yöntemlerinde olduğu gibi merkezi ve tekil bir proxy sunucusu bulunmamaktadır. Kullanıcıların erişmek istedikleri içerik hedef makineden istemciye gelene kadar proxy olmaya gönüllü birçok ağ kullanıcısının makinesi üzerinden geçer ve her uğradığı makineden tekrar şifrelenerek bir sonrakine transfer olur. Ayrıca bir proxy makineden bir diğer proxy makineye transfer olan verinin belli bir rotası da yoktur. Tüm bunlar sayesinde, engellenen içeriğe erişmek isteyen kullanıcıların güvenmek zorunda oldukları bir proxy sunucusuna ihtiyaç kalmamaktadır. Ayrıca erişim engelleme yapan otoritelerin de engelleme aşma yapıldığını tespit etmesi, erişilen içeriğin defalarca şifrelenmesi nedeniyle, çok zordur. Engelleme aşma yapıldığının tespiti halinde bile verinin transfer edildiği rotanın tespiti ve verinin içeriğinin tespiti oldukça zor ve maliyetli bir işlemler dizisi gerektirmektedir. Ayrıca proxy ağındaki kullanıcı sayısı arttıkça engelleme aşma yapıldığının tespit edilmesi ve veri trafiğinin içeriğinin belirlenmesi daha da zorlaşmaktadır.

Tüm avantajlarının yanında çoklu proxy yöntemi kullanılarak engelleme aşma yapan kullanıcılar ciddi bir performans problemi yaşamaktadırlar. Çünkü defalarca şifrelenen ve birçok farklı proxy sunucusundan geçerek hedefe ulaşan verinin hedefe ulaşma süresi normal trafiğe göre çok daha uzun olmaktadır. Tek proxy kullanımı ile çoklu proxy kullanımı arasında veri transfer hızı açısından bir kıyas yapmak da oldukça zordur. Zira çoklu proxy kullanımındaki sürenin uzunluğu, proxy ağındaki kullanıcıların sayısı ile doğru orantılı olarak artmaktadır.

2. IP Değişikliği

Proxy yöntemleri gibi geniş spektrumlu çözümler sunmayan IP değişikliği yöntemi, sadece IP engelleme yöntemiyle engellenen web sitelerini yeniden erişilebilir kılmak amaçlı

kullanılabilmektedir. Erişim engelleme yöntemleri bölümünde, IP engelleme başlığı altında anlatılan yöntem hem aşılmasının kolaylığı bakımından zayıf, hem de engellenen IP adresine sahip web sunucusu üzerinde barındırılan içeriği hukuka aykırı olmayan web sitelerini de engelleyen bir yöntemdir.

IP engelleme yöntemiyle erişime kapatılan web sitelerini işletenler, bu web sitelerini IP adresini çok zor olmayan bazı yöntemlerle değiştirerek yeniden erişilebilir hale getirebilmektedirler. Engellenen web sitelerini işletenler ayrıca web sitelerini başka sunucu makinelere taşıyarak da engellemeyi aşabilmektedirler. Ancak bu yöntem IP değişikliğine göre hem daha meşakkatli, hem de maliyetli bir yöntemdir.

3. Alan Adı Değişikliği

DDoS saldırıları, alan adı kaydı silme, DNS engellemesi gibi erişim engelleme yöntemlerini kolayca aşmaya yarayan alan adı değişikliği yöntemi, farklı bir alan adı edinmek için bir maliyet gerektirmektedir. Günümüz şartlarında bu maliyet, çoğu web sitesi sahibi tarafından rahatlıkla karşılanabilecek bir maliyettir.

Alan adı değişikliği yönteminin siteyi işleten için en zor tarafı, web sitesinin yeni adresini site tekrar erişime kapatılmadan kullanıcılarına duyurmak olmaktadır[156]. Bu sorun da genellikle web sitesinin kullanıcılarının çoğunun üye olduğu forumlarda duyurular yapılarak ya da web sitesinin yöneticisi tarafından site kullanıcılarına toplu eposta gönderilerek aşılmaktadır.

4. DNS Değişikliği

Bir web sitesini sunan web sunucusunun IP adresi bilinmiyorsa, o web sitesine erişmenin tek yolu sitenin adresini bilmektir. Sitenin adresi de erişilen DNS sunucusu tarafından çözümlenerek kullanıcı erişilmek istenen web sitesinin IP adresine yönlendirilir[157]. DNS engelleme yöntemiyle erişimi engellenen web sitesinin DNS çözümlemesi İSS'nin DNS sunucusu tarafından yapılmaz. Böylece kullanıcılar bu yöntemle engellenen web sitesine adres bilgisini kullanarak erişemezler. Ancak kullanıcı tarafında, DNS ayarları değiştirilerek alternatif DNS sunucular kullanılabilir. Böylece engelleme aşılmış olur. Ayrıca DNS engellemesi yöntemiyle erişime kapatılan web sitelerinin sahipleri, siteleri için alternatif alan adları kaydederek engellemenin etkisiz kalmasını sağlayabilmektedirler[158].

---

[156] Deibert/Palfrey/Rohozinski/Zittrain, a.g.e., s. 68.
[157] Bkz. yuk. § 4 I C.
[158] Kaya, a.g.e., s. 42.

5. URL Maskeleme

URL engellemesi, URL maskeleme yöntemi sayesinde en kolay aşılabilen erişim engelleme tekniklerinden birisidir. Zira bir web sitesinin ya da içeriğin URL'si rahatlıkla değiştirilebilmektedir. Ayrıca aynı içerik için alternatif URL'ler de bulundurulabilmekte ve erişimi engellenen içeriğe yönlendirilebilmektedir.

6. İçerik ve Alan Adı Aldatması

Web sitelerinin içerikleri ve alan adları anahtar kelime engelleme yöntemiyle filtreleniyorsa, web sitesi içeriğinde filtrelemeye takılabilecek kelimeler yerine konuyla ilgisi olmayan kelimeler kullanılarak engelleme aşılabilmektedir[159].

İçerik aldatma yöntemi tamamen insan eliyle yapılan bir şifreleme olduğundan bilgisayar programları tarafından kontrol edilen erişim engelleme sistemleri için hukuka aykırı içeriği tespit etmek imkânsız hale gelmektedir. Mesela, İran'da filtreye takılması kuvvetle muhtemel bir kelime olan 'feminizm' yerine konuyla ilgisi olmayan 'kitap' kelimesi kullanılırsa, kadın haklarını savunan web siteleri filtrelemeye takılmayacaktır. Ayrıca web siteleri alan adlarının içerdiği kelimelerden dolayı da engellenebilmektedir. Bu durumda içeriğiyle tamamen alakasız bir alan adı kullanan web siteleri engellenmekten kurtulabilmektedir[160]. Zira ülkemizde de pornografik içerikli olup alan adı itibariyle 'ödev', 'çizgi film', 'oyun' gibi çocukların ilgisini çekebilecek web sitelerinin sayısı oldukça fazladır.

7. Online Çeviri Siteleri

İnternette oldukça yaygın olan online tercüme sitelerinin birçoğu üzerinden engelli sitelere erişmek mümkündür. Tercüme siteleri genellikle web sitesi tercümesi de yapmaktadırlar. Yani kullanıcıya sundukları bir adres satırına girilen URL'deki web sitesinin dilini kullanıcının tercih edeceği dile çevirmektedirler. Örneğin http://www.worldlingo.com bir online çeviri servisi olup ABD'den hizmet vermektedir. Web sitesi çevirisi bölümünde girilecek URL'deki web sitesi ülkemizde erişime engelli olsa bile ABD'de engellenmiş değilse, çeviri servisi bu web sitesine erişmekte ve içeriğini istediğimiz dile çevirerek bize sunmaktadır. Yani bir tür proxy görevi görmektedir. Ancak bu tür bir engelleme aşma yöntemi kullanıcılar açısından oldukça tehlikelidir. Çünkü bu tür web siteleri sadece çeviri hizmeti vermek için tasarlanmış olup veri trafiğini hiçbir şifreleme işlemine tabi tutmamaktadır. Böylece bu siteleri engelleme aşma amaçlı kullananların anonimliği söz konusu değildir.

---

[159] Kaya, a.g.e., s. 43.
[160] Kaya, a.g.e., s. 43.

B. Pratikte Engelleme Aşma Yöntemleri (Engelleme Aşma Amacıyla Kullanılan Popüler Araçlar)

Bu bölümde, yukarıda anlatılan engelleme aşma tekniklerini kullanan, ücretsiz kullanılabilen ve İnternet dünyasında en çok kullanılan bazı araçlar anlatılmaktadır. Buradaki amaç engelleme aşma araçlarının kullanımını teşvik etmek değil, tam aksine bu araçları kullanmanın kullanıcılar açısından ne tür maliyetler doğuracağına dikkat çekmektir. Diğer yandan, erişim engellemelerin kapsamını belirleyen yetkililere konunun hassasiyeti hakkında fikir vermek amaçlanmaktadır.[161] Aşağıda incelenen araçların en bilinen üç tanesi Tor, Ultrasurf ve FreeGate'tir[162].

Yapılan bir araştırmaya göre[163] engelleme aşma yazılımlarının tamamının, ülkemizin de içinde bulunduğu, İnternet filtrelemenin yapılmakta olduğu ülkelerde kullanıldığı varsayılacak olsa bile; aşağıda incelenen engelleme aşma araçlarının kullanım oranı %3'ü geçmemektedir. Bu oranın içinde erişim engelleme uygulayan şirket çalışanlarının engelleme aşma amaçlı bu araçları kullanımı ve aynı şekilde engelleme uygulanan okullarda öğrenciler tarafından kullanımı da hesaba katılacak olursa, filtreleme uygulanan ülkelerde bu araçların kullanım oranı en fazla %1 olmaktadır[164]. Aslında engelleme aşma yöntemlerinin nispeten en güvenli olanları aşağıda adı geçen araçlar olarak bilinmektedir. Bu durumda geri kalan %99'luk İnternet kullanıcısı oranının güvensiz yöntemler kullanarak engelli sitelere erişme ihtimali bulunmaktadır ki, bu oran İnternet korsanları için oldukça iştah kabartıcı bir hedeftir.

1. DynaWeb FreeGate

DynaWeb FreeGate özellikle Çin'de engelleme aşma amaçlı olarak yazılmış bir HTTP proxy[165] aracıdır. Zamanla popülaritesi Çin sınırlarını aşmıştır. İnternette ücretsiz olarak İngilizce ve Çince versiyonlarını bulmak mümkündür. Şu an dünya üzerinde birçok ülkede kullanıcıları olan bir yazılımdır. DynaWeb FreeGate projesinin yürütücülerinin, Çin hükümeti tarafından sürekli olarak engellemeye tabi tutulmaya çalışılan kendilerine ait proxy sunucuları bulunmaktadır[166].

---

[161] Olumlu yönlerinden bahsedilen araçlar hakkında kesinlikle tavsiye ediliyor olduğu anlaşılmamalıdır. Zira bu tür araçları kullanan internet kullanıcıları, bu araçlar vasıtasıyla bağlanmış oldukları ağların yöneticilerini güvenilir varsaymaktadırlar ya da onlara güvenmektedirler. Bu ağların gizli servislerce yönetildiği ya da desteklendiği ihtimali her zaman ve her araç için bulunmaktadır.

[162] Hal Roberts/Ethan Zuckerman/Robert Faris/Jillian York/John Palfrey, The Evolving Landscape of Internet Control, A Summary of Our Recent Research and Recommendations, The Berkman Center for Internet & Society, August 2011, http://cyber.law.harvard.edu/publications/2011/Evolving_Landscape_Internet_Control, a.g.e., s. 3.

[163] Roberts/Zuckerman/Faris/York/Palfrey Evolving Landscape, a.g.e., s. 4.

[164] Roberts/Zuckerman/Faris/York/Palfrey Evolving Landscape, a.g.e., s. 4.

[165] Bkz. yuk. § 4 II A 1. a.

[166] Roberts/Zuckerman/Palfrey, a.g.e., s. 15.

DynaWeb FreeGate yazılımı hemen her türlü filtrelemeyi aşabilmektedir. Ancak -Çin kökenli olmasından olsa gerek- DynaWeb FreeGate yazılımı, bu yazılımın geliştiricileri hakkında, özellikle Çin hükümeti tarafından yapılan olumsuz ve saldırganca içerikleri filtrelemektedir. Yazılımın göze çarpan en önemli eksikliği, şifrelemedeki yetersizliğidir[167]. Zira bazı verileri şifreleyemeyen mekanizması sayesinde zaman zaman anahtar kelime filtrelemeye takılabilmektedir. Bu nedenle yasaklı içeriğe erişmeye çalışan kullanıcılar da tespit edilme tehlikesiyle karşı karşıya kalmaktadır.

2. Ultrasurf

Diğer birçok engelleme aşma aracının olduğu gibi Ultrasurf'ün de çıkış yeri Çin'dir. Çin'de İnternete uygulanan sıkı filtreleme neticesinde ortaya çıkmış ve tüm dünyada ücretsiz kullanılan bir araç olmuştur. Ultrasurf de, DynaWeb FreeGate gibi HTTP proxy yöntemiyle engelleme aşma yapmaktadır.

Yapılan deney çalışmaları sonuçlarına göre[168] Ultrasurf, engelleme aşma araçlarının en iyi performans gösteren aracı olmuştur. Ultrasurf uçtan uca şifreleme yaparak kullanıcılarının anonimliğini sağlamaya çalışmaktadır. DynaWeb FreeGate gibi Ultrasurf de, projenin geliştiricilerine karşı saldırgan olarak yorumladığı İnternet içeriğini filtrelemektedir[169].

3. Circumventor

Circumventor bir CGI proxy[170] aracıdır. Circumventor yazılımı ABD'de bir okuldaki öğrenciler tarafından İnternet filtresini aşmak amacıyla geliştirilmiş olup daha sonra dünya çapında ücretsiz kullanılan bir program olmuştur[171].

Circumventor aracılığıyla engellenen sitelere erişim diğer yöntemlerle erişimden biraz farklılık arz etmektedir. Çünkü bu program, engelli sitelere erişmek için kullanılan bilgisayara değil; başka bir bilgisayara kurulur ve engelli sitelere programın kurulu olduğu bilgisayar üzerinden erişilir. Örneğin iş yerindeki engelleme aşılmak isteniyorsa, çalışan programı filtrelemeye maruz kalmayan evindeki bilgisayarına kurar ve bir URL elde eder. Elde edilen URL ile iş yerinden engelli sitelere erişim mümkün olur. Ya da ülke çapında engellenen bir web sitesine erişilmek istendiğinde, dünya çapında Circumventor programını kullanarak bilgisayarını gönüllü proxy sunucusu yapan kullanıcılar üzerinden erişim mümkün olmaktadır.

---

[167] Roberts/Zuckerman/Palfrey, a.g.e., s. 15.
[168] Roberts/Zuckerman/Palfrey, a.g.e., s. 43.
[169] Roberts/Zuckerman/Palfrey, a.g.e., s. 43.
[170] Bkz. yuk. § 4 II A 1. b.
[171] Roberts/Zuckerman/Palfrey, a.g.e., s. 48.

Circumventor programı veri transfer hızı anlamında yukarıda bahsedilen araçlara göre daha yavaş bir araçtır. Ayrıca transfer edilen içeriğin tamamını şifreleyememektedir. Bu yüzden kullanıcıların anonimliği tehlikededir. Ayrıca gönüllü proxy olarak hizmet veren Circumventor kullanıcılarının kendi bilgisayarları üzerinden geçen HTTP trafiğini kötüye kullanmadıklarının garantisi de yoktur. Bu açıdan hassas verilerin bu bağlantı üzerinden aktarılması ciddi bilgi güvenliği risklerini beraberinde getirmektedir. Bu yüzden – tam koruma sağlamasa da – HTTPS protokolünün kullanılması daha sağlıklı olacaktır.

4. Psiphon

Psiphon, CGI proxy yöntemi ile engelleme aşmaya yarayan ücretsiz bir araçtır. Merkezi Kanada'da bulunan ve University of Toronto'ya bağlı olarak filtreleme aşma yöntemleri geliştiren[172] bir kuruluş olan Psiphon kâr amaçlı çıkardığı ürünlerin yanında filtrelemeye maruz kalan toplumlar için de kar amaçlı olmayan sosyal yöntemler sunmaktadır.

Psiphon projesinin filtrelemeye maruz kalan İnternet kullanıcıları için sunduğu temel özellik, filtreleme yapılmayan ülkelerdeki gönüllü İnternet kullanıcılarının bilgisayarlarını CGI proxy makinesi olarak kullandırıp, filtreleme yapılan ülkelerdeki belirli sayılardaki kullanıcı gruplarına engelleme aşma hizmeti sunmalarını sağlamaktır[173]. İstemci tarafında herhangi bir program kurulumu gerektirmeyen araç için sunucu tarafında kolay kullanımlı bir yazılım kurulumu gerekmektedir.

Psiphon kullanışlı bir araç olmasına rağmen, tüm HTTP isteklerini şifrelemekte yetersiz kalmakta olduğundan kullanıcılarının anonimliğini tam olarak koruyamamaktadır. Ayrıca üzerinden İnternete bağlanılan CGI proxy sunucuyu işletenlerin güvenilir kişiler olması gerekmektedir. Performans olarak yetersiz kalsa da, her türlü filtrelemeye karşı etkili bir çözüm sunmaktadır.

5. Tor

Tor, trafik yönlendirme (çoklu proxy)[174] yöntemi kullanan ve öncelikli amacı kullanıcılarının anonimliğini sağlamak olan ücretsiz bir araçtır. Tor yönlendirdiği trafiği, veri paketlerinin kaynak ve hedef noktalarını ağdaki her kullanıcıdan ve bu bilgiye ulaşabilecek herkesten gizlemek suretiyle kullanıcılarının anonimliğini ve güvenliğini sağlamak amacındadır. Ayrıca iletilen paketlerin içeriğinin de şifrelenmesi sayesinde Tor – öncelikli amacı bu olmasa da – iyi bir engelleme aşma aracıdır[175]. Zira yapılan testlerde[176] Tor'un her

[172] About Psiphon inc, http://psiphon.ca/?page_id=94
[173] Roberts/Zuckerman/Palfrey, a.g.e., s. 59.
[174] Bkz. yuk. § 4 II A 1. d.
[175] Roberts/Zuckerman/Palfrey, a.g.e., s. 72.
[176] Roberts/Zuckerman/Palfrey, a.g.e., s. 72.

türlü filtrelemeyi aşmada başarılı olduğu ortaya konmuştur. Ancak trafik aktarım hızı, trafik yönlendirme kriterleri açısından düşünüldüğünde, birçok etkene dayandığından ve güçlü bir şifreleme kullanıldığından dolayı diğer araçlara göre oldukça yavaştır.

Tor ağındaki proxy sunucular, proxy sunucusu olmaya gönüllü olan Tor kullanıcılarından oluşmaktadır. Anonimlik sağlayıcı diğer araçlardan farklı olarak Tor'u farklı kılan en önemli özelliği, ağdaki gönüllü proxy makinelerinin veri paketinin bir sonraki durağının hangi makine olacağını bilemiyor olmasıdır. Yani paket tamamen rastgele bir rota izlemektedir. Dolayısıyla erişilen içeriğin hukuka aykırı bir içerik olduğunun tespit edilmesi bir yana, teknik olarak bu içeriğin hangi hedefe ulaşacağı dahi bilinememektedir.

Tor trafiğinin çıkış noktalarında elbette şifresi çözülmektedir ki veri kullanıcıya ulaştığında anlamlı bir içerik oluştursun. Bu durumda akıllara şu soru gelmektedir: Tor ağının yöneticileri teorik olarak bu çıkış noktalarına erişebilmektedirler. Bu yetkilerini kötüye kullanma ihtimalleri var mıdır? Ayrıca Tor'un ilk çıkış sebebinin Amerikan Deniz Kuvvetleri'nin iletişim güvenliğini sağlamak olduğu[177] düşünüldüğünde akıllara hayal gücünü çok da zorlamayacak soru işaretleri gelebilmektedir.

6. Hamachi

Hamachi, VPN (IP tünelleme)[178] aracı olarak hem ticari hem ücretsiz bireysel kullanımı olan bir yazılımdır. Hamachi, kullanıcılarına özel sanal ağlar kurarak İnternet üzerinden, İnternetten izole, güvenli bir iletişim imkânı sağlamaktadır. Hamachi kullanıcılar arasındaki veri alışverişini şifrelemektedir ve kendi sunucularını barındıran bir sistem yerine, kullanıcılarının bu görevi yerine getirmesini gerektiren bir model ile çalışmaktadır[179].

Öncelikli ortaya çıkış amacı VPN kullanılarak güvenli iletişimi sağlamak olan araç, engelleme aşma amaçlı olarak da kullanılabilmektedir. Zira İnternet üzerinde iki bilgisayar arasında VPN ağı kurularak, filtreleme yapılan ülkede bulunan bilgisayarın filtreleme yapılmayan bir ülkede bulunan başka bir bilgisayara bağlanması suretiyle, İnternete erişimi kısıtlanmış olan bilgisayarın İnternete diğer makine üzerinden bağlanması ve engelleme aşma yapması sağlanabilir. Ancak istikrarlı çalışabilen bir sürümü henüz çıkmadığı için engelleme aşma amaçlı olarak kullanımı ve testleri tam anlamıyla yapılamamıştır[180].

---

[177] Tor: Overview, https://www.torproject.org/about/overview.html.en
[178] Bkz. yuk. § 4 II A 1. c.
[179] Roberts/Zuckerman/Palfrey, a.g.e., s. 81.
[180] Roberts/Zuckerman/Palfrey, a.g.e., s. 81.

7. Engelleme Aşma Araçları Değerlendirme ve Riskler

İnternetin özgür doğası gereği, İnternette erişim engelleme yapıldıkça engelleme aşma girişimleri de mutlaka olmaktadır. Ülkemizde Youtube engellemesi yaşandığı dönemde[181] bile www.youtube.com'un en çok ziyaret edilen beşinci web sitesi[182] olması, özellikle popüler web siteleri için engellemelerin genelde engelleme aşma girişimleriyle karşılaştığını göstermektedir. Youtube'un engellemelere rağmen bu kadar popüler olması ülkemizde engelleme aşma yöntemlerinin oldukça yaygın şekilde kullanıldığının en büyük göstergesi olmaktadır.

Engelleme aşma yöntemlerinin yaygın olarak kullanılması beraberinde birçok güvenlik riskini getirmektedir. Engelleme aşma yöntemleri arasında en güvenli olanları – kendileri de pek çok risk içerse de- bu işe yönelik hazırlanmış yazılımlardır. Ancak yapılan bir araştırmaya göre bu yazılımların filtrelemeye maruz kalan İnternet kullanıcıları arasında kullanım oranı tüm dünyada %3'ü aşmamaktadır[183]. Geri kalan İnternet kullanıcıları ise Google üzerinden genellikle "*proxy*", "*tunnel*", vb. arama terimlerini kullanarak basit web proxylere erişmekte ve erişimi engellenmiş web sitelerine bu yolla ulaşmaktadırlar[184].

Her ne kadar engelleme aşma yazılımları web proxylere göre daha güvenli kabul edilse de, bu yazılımlar da saldırılara açıktır. Ayrıca bu yazılımları anonimliğini koruma ve bu yolla suç işleme amaçlı kullananların varlığı da göz önüne alınacak olursa, engelleme aşma yazılımlarının gizli servislerin ilgi alanına girdiği aşikârdır. Zira Tor[185] gibi dünyaca çok güvenli olarak bilinen ve anonimliği sağlama konusunda en iyi araçlardan biri olduğu, yapılan araştırmalarla ortaya konan[186] bir yazılımın bile gizli servisler ve polis tarafından takip edildiği iddia edilmektedir[187]. Tor kullanıcılarının ne tür içeriklere eriştiğinin ya da iletişim sırasındaki veri akışının içeriğinin teknik olarak elde edilmesi mümkündür. Çünkü Tor ağında çıkış noktası olarak bilinen proxy makineleri en son içeriği kullanıcıya sunmadan önce şifreli veriyi çözer. Dolayısıyla istihbarat servislerinin çıkış noktalarından geçen trafiği dinlemeleri, iletişimin gizliliğinin sona ermesi için yeterli olacaktır.

Tor ağındaki çıkış noktalarını işleten ağ yöneticilerinin kendi makinelerinden geçen trafiği dinlemeleri teknik olarak mümkündür[188]. Bu durumda da ağı kullanan kullanıcıların iletişim gizliliğinin ihlal edilmesi mümkün olup, kişisel bilgilerinin de üçüncü şahısların eline

---

[181] Youtube yasağı ülkemizde Ekim 2010'da kaldırılmıştır. Bkz. http://www.leylakeser.org/search/label/Youtube.

[182] Ergün Dinçer, En Çok Ziyaret Edilen Site Sıralamasında Facebook, 2010 Yılında Google'u Geçti, 3 Ocak 2011, http://www.sosyalmedyapazarlama.com/2011/01/en-cok-ziyaret-edilen-site-siralamasinda-facebook-2010-yilinda-googleu-gecti/

[183] Hal Roberts/Ethan Zuckerman/Jillian York/Robert Faris/John Palfrey, 2011 Circumvention Tool Usage Report, The Berkman Center for Internet & Society, October 2010, http://cyber.law.harvard.edu/publications/2011/2011_Circumvention_Tool_Evaluation, a.g.e., s. 2.

[184] Konuyla ilgili ayrıntılı değerlendirme için bkz. aşa. §4 II C.

[185] Bkz. yuk. § 4 II B 5.

[186] Roberts/Zuckerman/Palfrey, a.g.e., s. 72.

[187] Konuya ilgili haber için bkz. turk.internet.com, "ABD'de TOR Yazılımını Kullanarak Takipten Kurtulmaya Çalışan Uyuşturucu Çetesi Çökertildi", http://turk.internet.com/portal/yazigoster.php?yaziid=36752

[188] Roberts/Zuckerman/Palfrey, a.g.e., s. 76.

geçmesi tehlikesi bulunmaktadır. Tor gibi proxy mantığıyla çalışan bütün engelleme aşma araçlarında benzer tehlike söz konusudur.

Tor uygulaması üzerine yapılan araştırmalar göstermektedir ki, Tor ağında çıkış noktası işleterek Tor kullanıcılarının hassas verilerini ele geçiren pek çok İnternet kullanıcısı bulunmaktadır. Ayrıca bu kullanıcıların bir kısmı Tor kullanıcılarına elçiliklerin ve büyük şirketlerin bilgisayar sistemleri üzerinden erişim sağlamışlardır[189]. Öte yandan Tor çıkış noktalarında faaliyet gösteren kötü niyetli kişiler, Tor kullanıcılarına kendi sunucularından ulaştırılacak içeriği ele geçirmek bir yana, makineleri üzerinden akan trafiği değiştirebilmektedirler. Zira geçmişte üzerlerinden geçen trafiği değiştiren, içeriğe reklamlar ekleyerek içeriği istemciye ulaştıran routerlar tespit edilmiştir[190].

Engelleme aşma araçları hem anonimliği sağlamak hem de içeriğin filtrelenmesini önlemek amacıyla kullanıcılarının veri trafiğini şifrelemektedirler. Ancak bu araçların birçoğu açık kaynak kodlu yazılımlar olduğundan genellikle hangi şifreleme tekniklerini kullandıkları bilinmektedir. Dolayısıyla veri trafiği saldırılara karşı tam olarak korunamamaktadır. Çünkü ağ trafiğinin yavaşlamaması için çok güçlü şifreleme algoritmalarından kaçınılmaktadır.

C. Engelleme Aşma Yöntemleri Yan Etkileri ve Değerlendirme

Dünyada en sık kullanılan engelleme aşma yöntemi proxy yöntemidir. Proxy kullanımının hem kullanıcı açısından, hem genel olarak ülke açısından ciddi yan etkileri bulunmaktadır. Proxy kullanımı, İnternet kullanıcısının erişime engellenen içeriğe ait tüm IP paketlerini aradaki proxy sunucusu üzerinden aldığı tekniktir. Bu yüzden kullanılan proxy sunucusu güvenilir bir partiye ait değilse kullanıcının anonimliği ve mahremiyeti tehlikede demektir. Proxy sunucusunu işleten kişi ya da kişiler sunucu üzerinden akan veri trafiğini izleyebilmektedirler. Bu nedenle bazı ülkeler halka açık proxy hizmeti vererek hem istihbarat toplamayı, hem de İnternette vatandaşlarını izleyebilmeyi amaçlamaktadırlar. Bazı ülkeler bunun da ötesine giderek farklı ülkelerden kullanıcılara da proxy hizmeti sağlayıp o ülkelerden de istihbarat elde etmektedirler. Tor[191] uygulamasının da ilk etapta Amerikan Deniz Kuvvetleri'nin iletişim güvenliğini sağlamak amacıyla ortaya çıkmış ancak sonraları istihbarat toplama amaçlı tüm dünyanın kullanımına sunulmuş bir yazılım olduğu sanal dünyada ve uluslar arası kamuoyunda sıkça dillendirilen söylentilerden biridir. Ayrıca çoklu proxy kullanımı (trafik yönlendirme) yöntemi de görünüşte güvenli ve tespit edilmesi oldukça zor bir yöntem olsa da, bu tür proxy ağlarının gizli servislerce desteklendiği ve çıkış noktalarının istihbarat elde etme amaçlı olarak dinlendiği iddia edilmektedir. Ülkemiz açısından düşülecek olursa, özellikle açık proxy (open proxy) kullanımı sonucunda genellikle yurtdışından hizmet veren proxy sunucular üzerinden akan veri trafiği yurtdışına yönlenmekte ve bu trafiğin kimin ya da kimlerin önüne düştüğü bilinememektedir.

---

[189] Damon McCoy/Kevin Bauer/Dirk Grunwald/Tadayoshi Kohno/Douglas Sicker, Shining Light in Dark Places: Understanding the Tor Network.
[190] McCoy/Bauer/Grunwald/Kohno/Sicker.
[191] Bkz. yuk. § 4 II B 5.

Proxy kullanımının bir başka türü de CGI proxydir. CGI proxy kullanımı temel olarak proxy sunucunun kullanıcılara sağladığı alternatif arayüz üzerinden gerçekleşir. Çoğunlukla bu arayüz İnternet tarayıcı uygulaması üzerinden sağlanan alternatif bir URL alanından ibarettir. CGI proxy yöntemini kullanan İnternet kullanıcıları için en büyük risklerden bir tanesi, girmek istedikleri adresi bu alternatif URL alanı yerine İnternet tarayıcı uygulamasının adres alanına girmeleridir[192]. Bu durumda kullanıcının erişmeye çalıştığı engelli web sitesi kullanıcı açısından gizli bir bilgiyse, erişim isteği İSS'ye ulaşmakta ve gizli bilgi dışarı sızmış olmaktadır.

DNS engellemesini aşma amaçlı kullanılan DNS değişikliği (DNS yönlendirme) yöntemi, bu yöntemi kullanarak engellenen sitelere erişmeye çalışan İnternet kullanıcıları için çok büyük bilgi güvenliği riskleri taşımaktadır. DNS değişikliği yöntemi için genellikle açık DNS (Open DNS) sunucular kullanılmaktadır. Yapılan araştırmaların tahminî sonuçlarına göre İnternette 17 milyon civarında açık DNS sunucusu hizmet vermektedir[193]. Tüm bu DNS sunucularının yaklaşık 68000 tanesi DNS sorgularına yanlış cevaplar vermektedir[194]. Açık DNS sunucuları genellikle İnternet korsanlarının hedefi olmaktadır. Sorgulara yanlış cevaplar veren DNS sunucuları korsanlar tarafından manipüle edilen sunucudardır. Engelleme aşma amacıyla açık DNS sunuculara yönelen kullanıcılar korsanların hedefi haline gelmektedir. Korsanlar tarafından kontrol edilen DNS sunuculardan birine denk gelindiğinde kullanıcılar "*phishing*"[195] tehlikesiyle karşı karşıya kalmaktadırlar. Phishing tuzağına düşen İnternet kullanıcılarının kişisel verilerinin gizliliği tehlikeye düşmektedir. Bunun sonucunda kredi kartı bilgileri, eposta hesap bilgileri gibi bilgiler korsanların eline geçebilmekte ve kullanıcılar açısından büyük maddi ve manevi zararlar ortaya çıkmaktadır.

Ülkemizde TİB'in Youtube'u kapatmasıyla Türkiye'deki çoğu bilgisayar zombi[196] olma tehlikesi altında kalmıştır. Çünkü Youtube ülkemizde de dünyada olduğu gibi çok popüler bir web sitesidir. Zaten engellemeye rağmen Youtube'un ülkemizde en çok ziyaret edilen web siteleri sıralamasında beşinci[197] olması da Youtube'un popülaritesi hakkında yeterli fikir vermektedir. Ayrıca Youtube'un erişimi engellenmiş olmasına rağmen böylesine erişiliyor olması ülkemizde engelleme aşma yöntemlerinin birçok İnternet kullanıcısı tarafından kullanılıyor olduğuna işaret etmektedir. Bu da çoğu İnternet kullanıcısı için büyük bir bilgi güvenliği riski demektir. Ayrıca ülkemizdeki bilgisayarların çoğunun zombie olması, bu bilgisayarların İnternet korsanlarının kontrolünde yasa dışı DDoS[198] saldırılarına alet olabileceği anlamına gelmektedir. Nedeni, insanların basit web proxy ve tünel uygulamalarını barındıran web sitelerini sıklıkla kullanmaları ve bu tarz sitelerden bilgisayarlarına worm

---

[192] Roberts/Zuckerman/Palfrey, a.g.e., s. 15.
[193] Robert McMillan, DNS attack could signal Phishing 2.0, December 2007, http://www.computerworld.com/s/article/9052198/DNS_attack_could_signal_Phishing_2.0.
[194] McMillan.
[195] Bkz. yuk. § 2 III B 3.
[196] Bkz. yuk. § 2 III B 3.
[197] Bkz. yuk. § 4 II B 7.
[198] Bkz. yuk. § 2 III B 3.

(solucan yazılım)[199] bulaşmasıdır. Ayrıca bu yöntem, ülkeler arasındaki siber savaşlarda en çok kullanılan yöntemlerdendir.

§5. SONUÇ

İnternet bir kitle iletişim aracı olarak düşünüldüğünde filtrelenmesinin, ortaya çıkacak toplumsal zararları azaltmak açısından, gerekli görüleceği durumlar olabilir. Ancak İnternet ne sadece bir kitle iletişim aracı ne de sadece bir kişisel iletişim aracı olarak tanımlanabilir. Dolayısıyla karşımıza şu iki temel sorun çıkmaktadır; birincisi otoritenin içeriğe ya da erişime müdahalesinin demokrasiye ve temel hak ve özgürlüklere ne kadar zarar verdiği sorunu, ikincisi yapılan bu müdahalenin İnternetin yukarıda bahsedilen kendine özgü doğasına ne kadar uygun olduğu sorunudur[200]. Bu yüzden İnternette sansür olgusu ancak bir sorunsal olarak nitelenebilir.

İnternet kaynaklı eylemlerin hukuki boyutu ilk kez 90'lı yılların başında tartışılmaya başlanmıştır. İnternetin gazete, radyo ve televizyon gibi en etkili olduğu zannedilen iletişim araçlarından daha etkili bir iletişim aracı olduğu gerçeği fark edilene kadar ilk müdahaleler hep İnternet ortamında suçla mücadele etmek amacıyla yapılmıştır. Ancak bugün aşikârdır ki, özellikle web 2.0 olarak bilinen kavram İnternet bünyesinde yaygınlaşınca devletler İnternet olgusunu kontrol etmenin ve halklar üzerindeki etkisinin yönlendirilebilirliğinin oldukça zor olduğu ve sürekli bir mücadele gerektirdiği gerçeğiyle tanışmışlardır. Bu yüzden dünyanın farklı yerlerinde, farklı yönetim şekillerinin hüküm sürdüğü ülkelerde farklı İnternet politikaları üretilmeye başlamıştır. Özellikle otoriter rejimler, halkları üzerindeki iktidar ve etki gücünü kaybetmemek amacıyla İnternete oldukça sıkı sansür uygulayan politikalar geliştirmektedirler. İnterneti sansürlemek, bir anlamda temel insan hak ve özgürlüklerini sınırlamak demektir. Ancak İnternet sıkı bir şekilde sansürlenmeyecek kadar değerli, tamamen kendi haline bırakılmayacak kadar da tehlikeli bir olgudur. Bu yüzden aradaki hassas dengeyi sağlamak gerekir. Önceki bölümlerde de değinildiği üzere, dünyadaki ve ülkemizdeki uygulamalara bakıldığında henüz bu dengenin sağlanmaktan çok uzak olduğu görülmektedir.

İnternet modern dünyada ekonomik, politik, sosyal ve kültürel anlamlarda hem gündem belirleyen hem de kitleleri yönlendiren bir konuma gelmiştir. İnternet tüm dünyadaki bilgisayarları birbirine bağlayan bir bilgisayar ağı olduğundan küresel bir olgudur. Dolayısıyla İnterneti düzenlemek için yerel kanun ve düzenlemeler yeterli olmamaktadır. Günümüz itibariyle de henüz İnterneti düzenlemek ve temel insan hak ve özgürlüklerine en az zarar veren ve aynı zamanda insanlığın ortak değerlerine sahip çıkan uluslararası bir irade olduğundan söz etmek çok mümkün olmamaktadır. Avrupa Birliği üye ülkelerinin çocuk pornografisi, fikri mülkiyet hakları ihlalleri ve ırkçılık söylemlerine karşı mücadele etmek

[199] Worm, bir bilgisayar virüsü türü olup bağımsız çalışan bir uygulamadır. Bir bilgisayara bulaştıktan sonra kendini sürekli kopyalayarak ağdaki diğer bilgisayarlara da bulaşır. Bu tür yazılımların nihai hedefi ulaştıkları ağdaki bilgisayarları zombileştirerek, bu makineleri DDoS saldırılarına alet etmektir.
[200] Kaya, a.g.e., s. 2.

amacıyla ortak yayımladıkları mevzuat ve düzenleme maddeleri de – önceki bölümlerde bahsedildiği üzere – maksadını aşan uygulamalar nedeniyle amaçlarına ulaşmaktan uzak çalışmalardır.

Ülkemizde İnternette işlenen suçlar başta olmak üzere, İnternet içeriğine müdahale etmek amaçlı olarak – İnternete özel – ilk düzenleme çalışması 2007 yılında, 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun adıyla yapılmıştır. 2007 yılından önce de Türkiye İnternet içeriğine gerekli gördüğü durumlarda müdahale etmiştir. Ancak bu müdahaleler genel hükümlere dayanılarak yapıldığından dolayı kamuoyu tarafından eleştirilmiştir. Zira Anayasanın 13. maddesine göre temel hak ve hürriyetlere ilişkin sınırlamaların ancak kanunla yapılması gerekmektedir. Ayrıca İnternet kullanımının hızlı bir şekilde artması, İnternetin hayatın her alanına girmesi ve işlenen suçların hızla İnternet ortamına kayması İnternetin kontrol edilmesi ihtiyacını artırmıştır. Ortaya çıkan ihtiyaçlar neticesinde 5651 sayılı Kanun çıkarılmıştır.

5651 sayılı Kanun çizdiği çerçeve ile engelleme sebeplerini net olarak ortaya koymakta olduğundan bu yönüyle, dünya uygulamaları dikkate alındığında, örnek bir düzenlemedir. Zira dünya uygulamalarında "*ulusal güvenlik*", "*kamu yararı*", "*genel ahlâkın korunması*" gibi muğlâk ifadeler erişim engelleme sebepleri olarak kullanılabilmekte ve keyfi uygulamalara açık kapı bırakılabilmektedir. Ayrıca 5651 sayılı Kanun'da erişim engellemelere sebep teşkil edecek suçların net olarak ifade edilmesi Anayasanın 13. maddesine de uygunluk arz etmektedir.

Kanun'un eleştirilen bir diğer yönü ise toplu kullanım sağlayıcılara getirdiği yükümlülüklerin çerçevesinin ayrıntılarıyla çizilmemiş olmasıdır. Zira toplu kullanım sağlayıcılar Kanun'a göre, kullanıcılarının hukuka aykırı içeriğe erişmemeleri için gerekli tedbirleri almakla yükümlüdürler. Ancak Kanun'da bu tedbirler için herhangi bir bilgi güvenliği standardına ya da benzeri bir direktife referans verilmemiştir. Ayrıca toplu kullanım sağlayıcılara getirilen trafik datası (log) tutma yükümlülüğü de, özellikle bilişim dünyasında, sistem ve yöneticileri arasında Kanun'la ilgili en çok tartışılan ve anlaşılmasında güçlük yaşanan hususlardan biri olmuştur.

5651 sayılı Kanun, hukuka aykırı olduğu kanısı oluşmasına sebebiyet veren ya da bu konuda herhangi bir şüphe uyaran her türlü içerik hakkında erişimin engellenmesi kararını öngörmektedir. Ancak bu durum, erişimi engellenecek içeriğin sahibine savunma hakkını elinden almaktadır. Erişim engelleme kararı verilmeden önce uyar – kaldır yöntemi ile içerik sahibinden söz konusu içeriğin yayından kaldırılması istenmelidir. Aksi durumda erişim engelleme yöntemine gidilmelidir.

5651 sayılı Kanun tarafından hukuka aykırı içerikle mücadele etmek için yöntem olarak belirlenen erişim engelleme yöntemi hem orantılılık unsuruna hem de ceza sorumluluğunun şahsiliği ilkesine aykırıdır. Zira ülkemizde ciddi tartışma yaratan blog sitelerinden bazılarının, bazı kullanıcıların kendi sayfalarında yayımladığı içerik dolayısıyla, erişime kapatılması bütün blog kullanıcılarını mağdur etmiştir. Analoji yapmak gerekirse, bıçakla adam öldürülmesi neticesinde bıçak kullanımının –ekmek kesmek için dahi olsa-

yasaklanması gibi Youtube yahut Blogger gibi web sitelerinin erişime kapatılması da kamu yararına hizmet etmeyecektir. Bu yüzden; düşünce ve ifade özgürlüğü başta olmak üzere temel insan hak ve özgürlüklerini dikkate alan ve incitmemeye özen gösteren, toplumsal uzlaşı çerçevesinde şekillendirilmiş, bir tek hukuka aykırı içerik yüzünden bütün kullanıcıların cezalandırılmayacağı ve dünyaya örnek teşkil edecek yasal düzenlemeler üzerine kafa yorulmalı ve gerekli adımlar bir an önce atılmalıdır. Zira ülkemizin kaçırmış olduğu sanayi devriminden sonra bilişim devrimini kaçırmaması adına bilgi toplumu olma yolunda zaman kaybına tahammülü yoktur.

Kanun'un tüm eleştirilen yönlerinin ötesinde, Kanun'da İnternetteki hukuka aykırı içerikle mücadele yöntemi olarak erişim engellemenin öngörülüyor olması birçok bilgi güvenliği zafiyetini de beraberinde getirmektedir. Zira erişim engelleme tekniklerinin geliştiği ölçüde, engelleme aşma teknikleri de gelişmektedir. Ortaya konulan istatistikler ve yapılan çalışmalar Türk toplumunun erişim engellemeyi, engellenen web sitelerini ziyaret etmek için engel olarak görmediğini – özellikle engelli olduğu dönemde Youtube'un ülkemizde en çok tıklanan web siteleri arasına girmesiyle – göstermektedir. Erişim engellemelere bu kadar karşı konulan, engelleme yöntemlerinin bu denli bilindiği ve bu sıklıkla kullanıldığı bir ülkede İnternet kullanıcılarının bilgi güvenliğinin tehlikede olmadığını söylemek imkânsızdır. Özellikle de engelleme yöntemi olarak DNS engellemesinin kullanıldığı ülkemizde kullanıcılarının kendilerine ait DNS sunucuları bulunmadığı müddetçe, hangi engelleme aşma yöntemi kullanılıyor olursa olsun, güvenlik riskleri bulunmaktadır. Bu riskler risk olmaktan çıkıp gerçeğe dönüştüğü zaman ise en başta kişi mahremiyeti ve kişilerin Anayasa ile öngörülen iletişimin gizliliği ilkesi ihlal edilmiş olmaktadır. Bunun ötesinde kişilerin sahip oldukları ve kendileri için maddi ya da manevi değer ifade eden her türlü bilgi teknik nedenlerle kaybedilebilmektedir. Ayrıca bu türlü maddi ya da manevi değer ifade eden bilgilerin kötü niyetli kişilerin ellerine geçmesi de kuvvetle muhtemel olup, bu kişiler kurbanlarını çoğu zaman maddi veya manevi zararlara uğratmaktadırlar. Yukarıdaki bölümlerde de işlenen, ülkemizde en çok kullanılan engelleme aşma terimleri Google arama motoruna yazıldığında gelen sonuçların tamamına yakını bünyesinde zararlı yazılımlar barındıran web siteleridir.

İnterneti düzenlemek için ülkeler bazında yerel kanunların yeterli olmaması nedeniyle düzenlemelerin de uluslararası boyutlarının olması gerekmektedir. "*Netizen*"lik[201], yani İnternet vatandaşlığı kavramının geliştirilerek uluslararası düzenlemelerin netizen etrafında şekillenmesi ve İnternet ortamı da ülkeler üstü bir yaşam alanı olarak kabul edilerek küresel vatandaşlık düzenlemeleri yapılması, tüm dünyada ifade hürriyeti açısından olumlu gelişmelere kapı açabilir. Ayrıca şu anda faaliyet göstermekte olan IWF (Internet Watch Foundation) gibi sivil kuruluşların çalışma kapsamı geliştirilmeli, yetkileri artırılmalı ve küresel bir irade ortaya koyularak bu kuruluşların İnternet yönetişimi için işbirliği yapmaları sağlanmalıdır. Ancak bu şekilde devletlerin ideoloji gölgesi, düşünce ve ifade hürriyeti üzerinden kaldırılabilir.

[201] Merriam-Webster sözlüğüne göre netizen, internetin çevrimiçi toplumunun aktif bir katılımcısı olarak tanımlanmaktadır. Netizen, İngilizce "net" (ağ) ve "citizen" (vatandaş) kelimelerinin birleşiminden oluşmuş bir kelimedir.

İnternet yönetişimi adına bütün çözüm önerileri daha demokratik ve özgür bir dünya için olduğundan bu konuda sadece devletlere ya da tüzel kişilere değil, bütün bireylere görevler düşmektedir. Aslında çözümün en önemli ayağını da bireylere düşen görevler oluşturmaktadır. Bireylerin, yukarıda bahsedilen sivil organizasyonlara sağlayacağı geri bildirimler daha temiz bir İnternet için önemli bir katkı olacaktır. Bu sayede İnternet kavramı bilinçli bireyler sayesinde olgunlaşacak ve kendi kendini düzenleyebilir (self-regulating Internet) hale gelecektir. Ayrıca İnternet kullanıcılarının bilinçlendirilmesi için gerekli çalışmalar otoriteler eliyle yapıldıkça sorumlu bireylerin oranı artacak ve özellikle çocukları İnternetin zararlı etkilerinden koruma misyonunu bu sorumlu bireyler üstlenecektir. Zira çocukların İnternetin zararlı etkilerinden korunması için en büyük görev ebeveynlere düşmektedir. Çocuklar İnternetten mahrum bırakılmamalı ve bilgi toplumunun gelecekteki mimarları olarak da onlar İnternet ile baş başa bırakılmadan önce çocuk filtresi, güvenlik duvarı, vb. modern teknolojilerin elverdiği ölçüde gerekli önlemler alınmalıdır.