TÜRKİYE VE DÜNYADA İNTERNET ERİŞİMİNİN ENGELLENMESİ İLE İLGİLİ DÜZENLEMELER

YÜKSEK LİSANS

Mehmet ERYILMAZ

DANIŞMAN

Doç.Dr. Fehmi AKIN

İNTERNET VE BİLİŞİM TEKNOLOJİLERİ YÖNETİMİ ANABİLİM DALI

Haziran 2015

AFYON KOCATEPE ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

YÜKSEK LİSANS TEZİ

TÜRKİYE VE DÜNYADA İNTERNET ERİŞİMİNİN ENGELLENMESİ İLE İLGİLİ DÜZENLEMELER

Mehmet ERYILMAZ

DANIŞMAN
Doç.Dr.Fehmi AKIN

İNTERNET VE BİLİŞİM TEKNOLOJİLERİ YÖNETİMİ ANABİLİM DALI

Haziran 2015

TEZ ONAY SAYFASI

Mehmet ERYILMAZ tarafından hazırlanan "**Türkiye ve Dünyada İnternet Erişiminin Engellemesi ile İlgili Düzenlemeler**" adlı tez çalışması lisansüstü eğitim ve öğretim yönetmeliğinin ilgili maddeleri uyarınca 17/06/2015 tarihinde aşağıdaki jüri tarafından oy birliği/oy çokluğu ile Afyon Kocatepe Üniversitesi Fen Bilimleri Enstitüsü İnternet ve Bilişim Teknolojileri Yönetimi Anabilim Dalı'nda **YÜKSEK LİSANS TEZİ** olarak kabul edilmiştir.

Danışman **:** Doç.Dr. Fehmi AKIN

Başkan **:**

Üye **:**

Üye **:**

Afyon Kocatepe Üniversitesi
Fen Bilimleri Enstitüsü Yönetim Kurulu'nun
...../...../..... tarih ve
……. sayılı kararıyla onaylanmıştır.

…….
Prof. Dr. İbrahim EROL
Enstitü Müdürü

BİLİMSEL ETİK BİLDİRİM SAYFASI

Afyon Kocatepe Üniversitesi

Fen Bilimleri Enstitüsü, tez yazım kurallarına uygun olarak hazırladığım bu tez çalışmasında;

- Tez içindeki bütün bilgi ve belgeleri akademik kurallar çerçevesinde elde ettiğimi,
- Görsel, işitsel ve yazılı tüm bilgi ve sonuçları bilimsel ahlak kurallarına uygun olarak sunduğumu,
- Başkalarının eserlerinden yararlanılması durumunda ilgili eserlere bilimsel normlara uygun olarak atıfta bulunduğumu,
- Atıfta bulunduğum eserlerin tümünü kaynak olarak gösterdiğimi,
- Kullanılan verilerde herhangi bir tahrifat yapmadığımı,
- Ve bu tezin herhangi bir bölümünü bu üniversite veya başka bir üniversitede başka bir tez çalışması olarak sunmadığımı

beyan ederim.

17/06/2015

Mehmet ERYILMAZ

ÖZET

Yüksek Lisans Tezi

TÜRKİYE VE DÜNYADA İNTERNET ERİŞİMİNİN ENGELLENMESİ İLE İLGİLİ DÜZENLEMELER

Mehmet ERYILMAZ

Afyon Kocatepe Üniversitesi

Fen Bilimleri Enstitüsü

İnternet ve Bilişim Teknolojileri Yönetimi Anabilim Dalı

Danışman: Doç.Dr.Fehmi AKIN

Bilgisayarların, çeşitli yöntemlerle birbirine bağlanabilir hale gelerek bilgisayar ağlarını oluşturmaya başlaması, bilişim teknolojisinin dünyada bilginin küreselleşmesini ve kendisini hızla üretmesini ve dönüştürmesini sağlayan bir gelişme olmuştur. Teknolojik gelişmelerin fitilini ateşleyen en önemli etken, dünya çapındaki irili ufaklı bilgisayar ağlarının kurulması ve varlığı değil, bütün bilgisayar ağlarını kapsayan genel bir ağ olan İnternetin tesis edilmesidir. Web 1.0 teknolojisiyle kullanıcılar sadece İnternet sayfalarını izleyebilirken Web 2.0 teknolojisinin ortaya çıkmasıyla normal bir İnternet kullanıcısı bile yapmış olduğu yorumlar veya paylaşımlarla içerik yaratan konumuna gelmiştir. Hiçbir kaynak gösterilmeksizin kullanıcılar tarafından üretilen içerikler yüzünden İnternet bir bilgi çöplüğüne dönüşmektedir. İnternet ortamında oluşturulan bu bilgi kirliliği içinde faydalı materyaller olduğu kadar faydasız ve konusu suç teşkil eden unsurlar da sanal ortamda yerini almış durumdadır. İnternet ortamını hem faydasız bilgilerden arındırmak hem de konusu suç teşkil eden çocuk pornografisi, uyuşturucu maddelere yönlendirme, intihara teşvik, patlayıcı madde yapımı gibi özellikle çocukları ve gençleri olumsuz etkileyecek içerikten vatandaşlarını korumak için ülkeler ve toplumlar bir takım önlemler almak zorunda kalmışlardır. Bazı ülkelerin yönetim biçimi, kültürel, siyasi ve dini sebeplerle almış olduğu önlemler sansür boyutuna ulaştığı için yoğun eleştirilere maruz kalırken bazı ülkelerde ise kullanıcıların eğitilerek zararlı içeriğin kullanıcı tabanlı bir yaklaşımla önüne geçilebileceği tezi savunulmaktadır. Çalışmada İnternet erişim engellemesinin teknik boyutu, ülkemizde uygulamada olan 5651 sayılı kanun kapsamında katalog suçlar, kişilik haklarının ihlali ve özel hayatın gizliliğinin ihlali sebebiyle erişim engellemeleri, bazı ülkelerdeki çocukların cinsel istismarı, terörle mücadele ve yönetim kaynaklı İnternet erişiminin engellenmesi ile ilgili düzenlemeler incelenmiştir.

2015, x + 99 sayfa

Anahtar Kelimeler: 5651 sayılı kanun, İnternet erişiminin engellenmesi, İnternet, erişim engelleme yöntemleri.

ABSTRACT
M.Sc Thesis

REGULATIONS ON DENIAL OF ACCESS IN TURKEY AND THE WORLD

Mehmet ERYILMAZ

Afyon Kocatepe University

Graduate School of Natural and Applied Sciences

Department of Internet and Information Technologies Management

Supervisor: Doç.Dr.Fehmi AKIN

Computers being able to be connected with different methods and starting to create computer networks was a development that enabled computer science to make information global around the world and produce and transform itself faster. The most important event that triggered technological developments was not the small and large scale computer networks being built around the world, but the establishment of the "Internet", which includes all computer networks. With its new structure dubbed "Web 2.0", the Internet took its users from Web 1.0, being the spectator of the content, to being the creator of it with comments and posts. The Internet is becoming a garbage dump full of information with all the content created by users without any references or sources. There are bad and sometimes criminal materials as well as good materials in this pollution of information created on the İnternet. Governments and communities had to take measures to protect children and the youth from content that will affect them negatively such like child pornography, promotion of drugs, encouragement of suicide making of explosives, etc. While some countries' way of managing this issue is intensely criticized due to cultural, political and religious reasons, in other countries, it is believed that educating the users will eliminate the harmful content with a user based approach. In study, the technical aspects of blocking of access on the İnternet, the law No.5651 that is in effect in our country and other implementations in other countries for the blocking of access on the İnternet has been investigated.

2015, x + 99 sayfa

Key Words: Law No. 5651, Blocking Access Of Internet, Methods Of Blocking Access.

TEŞEKKÜR

Bu araştırmanın konusu, çalışmalarımın yönlendirilmesi, sonuçların değerlendirilmesi ve yazımı aşamasında yapmış olduğu büyük katkılarından dolayı tez danışmanım Sayın Doç.Dr. Fehmi AKIN'a, araştırma ve yazım süresince yardımlarını esirgemeyen Zehra GÜLBUDAK'a, kardeşim Menekşe ERYILMAZ'a her konuda öneri ve eleştirileriyle yardımlarını gördüğüm hocalarıma ve arkadaşlarıma teşekkür ederim.

Bu araştırma boyunca maddi ve manevi desteklerinden dolayı aileme teşekkür ederim.

Mehmet ERYILMAZ
AFYONKARAHİSAR, 2015

İÇİNDEKİLER DİZİNİ

Sayfa

KISALTMALAR DİZİNİ

Kısaltmalar

AAMS	Italian Monopoly Administration Authority
AB	Avrupa Birliği
ABD	Amerika Birleşik Devletleri
ADSL	Asymmetric Digital Subscriber Line
AK	Avrupa Konseyi
ARJEL	Autorité de Régulation des Jeux en Ligne
ARPANET	Advanced Research Projects Agency Network
CDA	Communications Decency Act
CIA	Central Intelligence Agency
CIPA	Children's Internet Protection Act
CITC	Communications and Information Technology Commission
CMK	Ceza Muhakemesi Kanunu
COPA	Child Online Protection Act
CPU	Central Processing Unit
DDOS	Distributed Denial of Service Attack
DNS	Domain Name System
DRM	Digital Rights Management
DSL	Digital Subscriber Line
EARN	European Academic and Research Network
FSM	Freiwilligen Selbstkontrolle Multimedia
GEMA	Gesellschaft Für Musikalische Aufführungs
HTML	Hyper Text Markup Language
HTTP	Hyper Text Transfer Protocol
IANA	İnternet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
IOS	iPhone OS
ISP	Internet Service Provider
ISS	Internet Servis Sağlayıcısı
IWF	Internet Watch Foundation
LICRA	League Against Racism and Anti-Semitism
MIT	Massachusetts Institute of Technology
NSFNET	National Science Foundation Network
ODTÜ	Orta Doğu Teknik Üniversitesi
OECD	Organisation for Economic Cooperation and Development
OSI	Open Systems Interconnection
STMP	Simple Mail Transfer Protokol
TCK	Türk Ceza Kanunu
TCP/IP	Transmission Control Protocol / İnternet Protocol
TİB	Telekomünikasyon İletişim Başkanlığı
TLD	Top Level Domain
TOR	The Onion Router
TÜBİTAK	Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
TÜSİAD	Türk Sanayicileri ve İşadamları Derneği
TÜVEKA	Türkiye Üniversiteler ve Araştırma Kurumları Ağı
TTNET	Türk Telekom Net

URL	Uniform Resource Locator
VPN	Virtual Private Network
WAN	Wide Area Network
WIPO	World Intellectual Property Organization
Wİ-Fİ	Wireless Fidelity
WWW	World Wide Web

ŞEKİLLER DİZİNİ

Sayfa

1. GİRİŞ

Bilgisayarların, çeşitli yöntemlerle birbirine bağlanabilir hale gelerek bilgisayar ağlarını oluşturmaya başlaması, bilim teknolojisinin dünyada bilginin küreselleşmesini, kendisini daha hızlı üretmesini ve dönüştürmesini sağlayan bir gelişmedir. Teknolojik gelişmeleri tetikleyen en önemli olay, dünya çapındaki irili ufaklı bilgisayar bağlantılarının kurulması ve varlığı değil, bilgisayarlar arası bağlantıları kapsayan genel bir ağ olan İnternet kavramının tesis edilmesi olmuştur.

Tim Berners-Lee tarafından World Wide Web kavramı olarak ortaya atılan ve Web 1.0 olarak adlandırılan yapı, günümüzde İnternetin temel taşlarını oluşturan HTML sayfaları ile sanal ortamdaki dokümanların büyük bir hızla çoğalmasını sağlamıştır (Köse ve Özen 2010). İnternetin yeni yapısı olduğu değerlendirilen Web 2.0 sadece içerik izleyen İnternet kullanıcılarını içerik üreten statüsüne getirmiştir (İnt.Kyn.1). İçeriklerin kullanıcılar tarafından üretilmeye başlaması İnternet ortamında hızla çoğalan ve güvenilirlik seviyesi düşük bilgilerin artmasına sebep olmuştur. İnternet kullanıcıları karşılaştıkları her türlü sorunun çözümünü veya merak ettikleri her şeyi İnternet ortamı üzerinden öğrenmeye çalışmaktadır. Kullanıcılar tarafından üretilen, hızla yayılan ve denetimi zor olan bu tür yayınların içerisinde faydalı olanlar kadar zararlı yayınlarda bulunmaktadır (Köse ve Özen 2010).

1.1 Problemin Tespiti

Kullanıcılar tarafından üretilen, denetimi zor olan ve önlenemeyen şekilde yayılan bu bilgi kirliliği çocukları ve gençleri olumsuz etkileyecek, gençleri uyuşturucu madde kullanmaya ve intihara yönlendirecek ve hatta çocuk pornografisi, patlayıcı madde yapımı gibi suç teşkil eden unsurların oluşması kaçınılmaz olacaktır. Devletler vatandaşlarını korumak amacıyla bu tür yayınların önüne geçmek için tedbirler almak zorundadırlar. Alınan bu tedbirler bazı ülkelerde çok sert bir biçimde olabilirken bazı ülkelerde ise daha esnek ve yumuşak olarak uygulanmaktadır (Köse ve Özen 2010).

1.2 Çalışmanın Amacı

İnternet erişiminin engellenmesi her ne kadar hukuki kurallar ve mevcut yasalarla alınan kararlara bağlı olsa da engellemenin birde teknik boyutu bulunmaktadır. İnternet erişiminin engellenmesi için uygulanan teknikler ülke bazında kapsadığı alan göze alındığında şu şekilde sıralanmaktadır. Ülkeler öncelikle vatandaşlarının erişmesini istemediği içerikleri tüm ülkeyi kapsayan İnternet omurgasında engellemektedir. Mahkeme kararları veya filtreleme yazılımlarıyla yapılacak engellemeler İnternet Servis Sağlayıcılar bazında yapılmaktadır. Belirli bir birimde yapılacak olan engelleme o birimin kullandığı sunucu aracılığı ile sadece o birimi kapsayacak şekilde uygulanmaktadır. Son olarak kişisel bilgisayarlarda erişilmesi istenmeyen yayınlar filtreleme programları aracılığı ile engellenerek kişisel bilgisayar bazında engelleme yapılabilmektedir. Ülkemizde yapılan İnternet erişim engellemeleri İnternet Servis Sağlayıcıları aracılığı ile IP adresinin engellenmesi, Alan adının (DNS) engellenmesi ve Nesne Tabanlı (URL) engelleme şeklinde gerçekleşmektedir.

Çalışmada İnternet erişiminin engellenmesi ile ilgili olarak teknik ve hukuki tanımlar, İnternet yönetimi ile ilgili yetkili kurumlar, uluslararası alanda hazırlanmış ve ülkemiz tarafından da kabul edilmiş sözleşmeler, engellemenin Türkiye ve dünyadaki teknik ve hukuki boyutu ele alınmıştır.

2. LİTERATÜR BİLGİLERİ

2.1 İnternet Erişiminin Engellemesiyle İlgili Yapılan Çalışmalar

Türkiye'de İnternet erişiminin engellenmesiyle ilgili olarak 2007 yılında yürürlüğe giren "5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun" değişik çevrelerce İnternetin sansürlendiğine dair yoğun tartışmalara neden olmuştur. İnternet erişiminin engellenmesi konusunun geçmişi, yakın zamana dayanması sebebiyle çok fazla literatür bilgisi ve kaynağı bulunmamaktadır.

İnternet erişiminin engellenmesinin Türkiye'deki hukuki boyutunu inceleyen en önemli eserlerden biri Bilişim Suçları ve İnternet İletişim Hukukudur (Dülger 2013). Eserin Yedinci bölüm olan son kısmında 5651 sayılı yasayla getirilen düzenlemeler ele alınmıştır. Yine aynı yazarın Türkiye'de İnternet Sitelerinin Erişiminin Engellenmesi Konusunda Farklı Hukuk Disiplinleri Açısından Değerlendirmeler konulu TÜSİAD yayınında İnternet erişim raporu bulunmaktadır (Beceni ve Dülger 2011). Raporda "5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun" hakkında değerlendirmeler yer almaktadır.

Access Contested: Security, Identity, and Resistance in Asian Cyberspace adlı eserde İnternet üzerindeki kontrolleri sansür boyutuna ulaşmış Çin, Hindistan, Singapur, Tayland, Bruma, Malezya ve Güney Kore gibi bazı Asya ülkelerinin politikalarını incelemekte, bu ülkelerden dünyaya yapılan siber saldırıları ve saldırılara karşı alınacak önlemleri konu edinmektedir (Palfrey *et al.* 2011).

Geographies of Global İnternet Censorship isimli makalede İnternet erişim engellemesi ile ilgili olarak ülkelerin coğrafik dağılımlarına değinilmiştir. Eserde ayrıca coğrafi dağılıma göre İnternet erişimin engellenme sebepleri üzerine bağlantılar kurulmuş, engellemedeki siyasi, dini, kültürel boyutlar anlatılmıştır (Warf 2011).

Gazi Üniversitesi Hukuk Fakültesi dergisinde yayınlanmış Türk Hukukunda ve Mukayeseli Hukukta İnternet Sitelerine Erişimin Engellenmesi ve İfade Hürriyeti adlı makalede yazar, İnternet sitelerinin engelleme metotlarını, Türkiye'deki İnternet erişimi uygulamasını ve erişim engellemede dünyadaki mevcut uygulamaları ele almıştır (Kılınç 2010).

Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace adlı eser İnternet erişimine devletlerin müdahalesini konu almaktadır. Kitap 'opennet' girişiminin uzmanları tarafından yazılmış 6 bölümden oluşmaktadır ve eserde dünya çapında İnternet erişimin engellenmesi üzerinde durulmuş, 29 ülke hakkında ayrıntılı erişim engelleme politikaları hususunda bölgesel raporlar sunulmuştur (Deibert *et al.* 2010).

Ege Üniversitesi Hukuk Fakültesi Dergisinde yer alan Erişimin Engellenmesi, Hukuki Sorunlar ve Çözüm Önerileri isimli makalede yazar Türk hukukunda erişimin engellenmesi sorununu ele almış ve erişim engellemede gördüğü sorunlarla ilgili kendi çözüm önerilerini sunmuştur (Memiş 2009).

Teknik ve Hukuki Boyutuyla İnternet Erişiminin Engellenmesi ismiyle yayınlanan eser, 5651 sayılı kanunun 2007 yılında yürürlüğe girdiği halini ve zamanın mevcut erişim engelleme uygulaması, İnternet erişiminin teknik olarak engelleme yöntemleri, engellenen İnternet erişiminin alternatif yollarla nasıl aşılacağı, ABD, Çin, Güney Kore, Singapur ve Suudi Arabistan gibi ülkelerde İnternet erişim engellemesi hakkındaki mevcut uygulamaları ele almıştır (Kaya 2009).

Bilgi Dünyası dergisinde yer alan Türkiye'de İnternet Yasakları başlıklı makalede yazar erişim engellemeye yasakçı boyutuyla bakmış, Türkiye'de uygulanan 5651 sayılı kanun içeriğini, insan hakları, düşünme özgürlüğü, haberleşme özgürlüğü ve diğer hak ve özgürlüklerin ihlali olarak değerlendirmiş, dünyadaki uygulamalardan örnekler vermiştir (Bulut 2009).

Access Denied: The Practice and Policy of Global Internet Filtering adlı eser her biri

farklı yazarlarca hazırlanan 6 bölümden oluşmakta ve eserde küresel İnternet filtreleme, İnternet filtrelemede siyaset ve kontrol mekanizmaları, İnternet filtreleme araçları ve teknoloji, filtreleme ve uluslararası sistem, üzerine görüşler belirtilmektedir. Kitapta dünyada İnternet erişimin engellenmesinin birçok ülke tarafından bilgiye erişim ve inkâr, siyasi sebepler, cinsellik, kültür, din gibi sebeplerden kaynaklandığı belirtilmektedir (Zittrain *et al.* 2008).

Gelişen teknoloji sayesinde, İnternet erişiminin engellenmesi ve engellenen sitelere ulaşmak için alternatif yollara ilave olarak yeni metotlar ortaya çıkmıştır. Şubat 2014'te yayınlanan torba yasayla 5651 sayılı kanunda yapılan düzenleme, literatürde yer alan eserlerin hiçbirinde yer almamaktadır.

2.2 İnternet ve Erişim Engelleme ile İlgili Tanım ve Bilgiler

2.2.1 Bilgisayar

Kullanıcılardan aldığı verilerle aritmetik ve mantıksal işlemleri yapabilen ve yaptığı işlemlerin sonuçlarını hafızasında muhafaza edebilen, muhafaza edilen bilgilere istenildiğinde ulaşılabilen elektronik bir makinedir. Bir başka şekilde de, uzun ve karmaşık hesapları dahi büyük bir hızla yapabilen, lojik (mantıksal) bağlantılara dayalı karar verip, işlem yürüten makine olarak tanımlanabilir (Avşar ve Öngören 2010). Bilgisayarın çalışma yapısı, veri girişi (Klavye, Mouse, Kamera, Scanner, Fax-modem vb.), verinin saklanması (Hard disk, Disket, Flash bellek, Cd-rom vb.), verinin işlenmesi (CPU "Central Processing Unit"- Merkezi işlem birimi) ve verinin çıkışı (Ekran, yazıcı, çizici, modem vb.) olarak 4 ana başlık altında toplanmaktadır (İnt.Kyn.2).

2.2.2 Bilgisayar Ağları (Network)

Bilgisayarların bir kablo veya kablosuz teknoloji kullanılarak birbirlerine bağlanmasıyla oluşan yapıya bilgisayar ağı (network) denir (Yaycı 2007). Bilgisayar ağı, birden fazla bilgisayarın birleşmesi demektir. Kablo veya kablosuz teknolojiler kullanılarak

bilgisayarların birbirine bağlanması çabukluk, ekonomiklik ve kolaylık sağlar. İletişim kolaylaşır.

2.2.3 LAN (Local Area Network-Yerel Alan Ağı)

LAN (Local Area Network-Yerel Alan Ağı); Bir birlerine yakın mesafedeki bilgisayarların kablo, ağ kartı (Ethernet kartı) veya kablosuz teknoloji aracılığıyla bağlanmasıyla oluşan bilgisayarlar arası ağdır (Yaycı 2007).

2.2.4 WAN (Wide Area Network-Geniş Alan Ağı)

WAN (Wide Area Network-Geniş alan ağları); Coğrafi konum olarak birbirlerinden uzak mesafelerdeki bilgisayarlar arasında kurulan ağlardır (Yaycı 2007). İnternet erişimi bu tür ağlara örnektir.

2.2.5 İnternet

İnternetin tanımı ile ilgili olarak bugüne kadar üzerinde ortaklaşa anlaşılmış bir kavram bulunmamaktadır. Çeşitli elektronik ve yazılı arşivlerdeki İnternet dokümanlarında yer verilen tasvirlere bakarak, İnternetin dünya üzerinde mevcut bilgisayarların birbirlerinin kaynaklarını paylaşmasını sağlayan bir ağlar-arası-ağ olduğu söylenebilir (Tulum 2006). İnternet kavramında yer alan "net" sözcüğü ağ anlamına gelmektedir (Tümerdem 2013).

2.2.5.1 İnternetin Tarihçesi

İnternetin tarihsel kaynağı A.B.D ile Sovyetler Birliği arasındaki soğuk savaş dönemine kadar uzanır. Sovyetler Birliği'nin 1957 yılında Sputnik uydusunu uzaya göndermesinin ardından, Amerikan hükümeti, özellikle bir nükleer savaş tehlikesi karşısında, askeri iletişimin korunabilmesi amacıyla çeşitli arayışlara girmiş ve bu kapsamda, 1960'lı yıllardan itibaren ünlü eğitim kurumu M.I.T(Massachusetts Institute of Technology)'nin liderliğinde, olası bir savaş veya karışıklık durumunda, tek bir ana bilgisayar ünitesinden bağımsız olarak çalışabilen bir bilgisayar ağı kurulabilmesi amacıyla çeşitli

çalışmalar yapılmasını gündeme getirmiştir (Demir 2014). Amerika, ortaya çıkacak bir savaş veya karışıklık halinde dünyanın çeşitli yerlerine yerleştirilmiş savaş sistemlerini bilgisayarlar arası bir ağ ile yönetme kararı vermiştir. Bu doğrultuda merkeze bağımlılığı olmayan ve birbirinden bağımsız çalışabilen bilgisayarlardan oluşan bir ağ kurulabilmesi hedeflenmiştir (Avşar ve Öngören 2010). Bu amaçla Savunma Bakanlığı'nda ARPA isimli bir birim oluşturulmuş ve bu birim bazı askeri projelerin birbirinden uzakta olan bilgisayarların birbirine bağlanması yoluyla desteklenmesi üzerine çalışmalara başlamıştır. İlk önce ABD'nin California ve Utah eyaletleri arasında dört ayrı merkez arasında 1969 yılında veri transferi gerçekleştirilmiş, sonra bu model geliştirilerek ARPANET isimli askeri bir bilgisayar ağı kurulmuştur (Demir 2014). ARPANET'e bağlı bilgisayarlar yazılım ve donanım yönünden farklı tipte oldukları için TCP/IP adı verilen bir dil geliştirilerek bilgisayarlar arasında iletişim kurmaya başlanmıştır. 1980 yılında TCP/IP protokolü sivil kullanıma da açılmıştır (Avşar ve Öngören 2010). Bilgisayarlar arasında iletişim sağlayacak bu ortak dilin sivil hayatta kullanıma açılması sonucu 1980'li yıllarda İngiltere ve Japonya gibi ülkelerdeki bilgisayarlar birbirleriyle iletişime geçebilmişlerdir. 1989 yılında Cenevre'deki bir araştırma merkezinde Tim Berners-Lee tarafından World Wide Web (www) olgusu geliştirilerek İnternet kullanıcılarının birbirleriyle daha rahat iletişim kurmaları sağlanmış ve 1990 yılında ise World Wide Web'in dayandığı en temel dosya protokolü olan Hyper-Text Transfer Protocol (HTTP) geliştirilmiştir (Demir 2014). Özel sektör kuruluşlarının 1990'lı yıllarda kendi ağlarını geliştirmeleri sonucu İnternet askeri ve resmi kurumların yönlendirmesinden çıkmış günümüzdeki halini almıştır (Avşar ve Öngören 2010).

İnternet, tek başına hiçbir kurum ve ülkeye ait olmadığı için dolayısıyla bu ortamdaki faaliyetleri kontrol eden tek bir otorite de bulunmamaktadır (Yılmaz 2007). Bu sebeple, İnternetteki faaliyetler konusunda her ülke kültür ve yaşam tarzlarına paralel kendi kurallarını koymaktadır. Bununla birlikte, ülkeler gelecekte uygulanacak ortak bir hukukî metni hazırlama faaliyetlerine devam etmektedir (Yılmaz 2007).

İnternetin ortaya çıkışı yakın bir tarihe denk gelmesine rağmen Türkiye'de kullanılması maalesef bulunuşu ile aynı ya da yakın tarihlere rastlamamaktadır (Demir 2014). 1986

yılında tesis edilen EARN (European Academic and Research Network)/BITNET bağlantılı TÜVEKA (Türkiye Üniversiteler ve Araştırma Kurumları Ağı) ağı Türkiye'deki ilk geniş alan ağıdır. Daha sonraki yıllarda hattın yetersiz kalması mevcut ihtiyacı karşılayamaz hale gelmiştir. İhtiyacı karşılamak için ODTÜ ve TÜBİTAK 1991 yılı sonlarında ortak bir çalışma başlatmıştır. Bu çalışma sayesinde 1992 yılında ilk bağlantı Hollanda'ya yapılmıştır (İnt.Kyn.3). 12 Nisan 1993'e ODTÜ Bilgi İşlem Daire Başkanlığı sistem salonundaki yönlendiriciler kullanılarak Türkiye'deki ilk İnternet bağlantısı ABD'de NSFNet (National Science Foundation Network)'e TCP/IP protokolü üzerinden kurulmuştur. Müteakiben ülke genelindeki birçok üniversite ve resmi kuruluş ODTÜ üzerinden bağlanarak İnternet erişimine sahip olmuştur. Türkiye'de İnternetin ticari amaçlı kuruluşlara ve hane halkları gibi geniş kitlelere ulaşması 1996 yılından itibaren mümkün olmuştur (İnt.Kyn.3).

2.2.5.2 İnternetin İşleyişi

Protokol kelimesi ağ teknolojilerinden bahsedilirken muhtemelen en çok duyacağımız terimidir. İnternet iletişimin işleyişi de normal hayatta olduğu gibi ortak bir dil kullanılarak gerçekleşmektedir. İnternet ağ protokolleri bilgisayarlar arası işleyişi sağlayan ortak dildir. Hattın iki ucundaki bilgisayarlar aynı tür yazılım, model ve işleyişte olsalar da aynı protokolü (ya da protokoller) olmadığı sürece iletişim kuramazlar (İnt.Kyn.22). Protokoller karşılıklı olarak nasıl davranılacağını, hangi tür veriye ne tür verilerle cevap verilebileceğini bilirler ve protokol dışına çıkılmadığı sürece anlaşmazlık oluşması mümkün değildir (İnt.Kyn.22). Zaten dünyanın en yaygın ve kamuya açık bilgisayar ağı olan İnternet ağına bağlı olan bilgisayarların birbirleriyle iletişim kurabilmeleri için uymaları gereken ortak kurallar bulunmalıdır ve dolayısıyla bilgisayarlar arası iletişimi sağlayan temel protokoller gündeme gelmektedir. Bu protokollere kısaca İnternet protokolleri ya da TCP/IP protokoller ailesi denir (Demir 2014).

2.2.6 İntranet

İntranet, çoğunlukla TCP/IP tabanlı olup; sadece belli bir birim veya birim içindeki

bilgisayarları, yerel ağları ve geniş alan ağlarını birbirine bağlayan ağdır (Tümerdem 2013). İntranetin oluşturulma amacı, birim içerisindeki bilgileri ve bilgi işlem kapasitesini kullanıcılarla paylaşmaktır (Demir 2014). İntranet ayrıca, birim içi telekonferans uygulamalarında ve farklı birimlerdeki kişilerin bir araya gelebildiği iş topluluklarının oluşturulmasında da kullanılır. İntranet, tüm web özelliklerini sağlamanın yanında kullanıcılarına erişim yetki seviyesi belirleyerek hangi kullanıcının nereye, ne oranda ve nasıl erişeceğini denetleyebilmektedir (Demir 2014).

2.2.7 TCP/IP (Transmission Control Protocol/İnternet Protocol)

TCP/IP, bilgisayarlar arası veri gönderme ve alma organizasyonu sağlayan, bir yerden başka bir yere bilgi iletimine imkân veren pek çok veri iletişim protokolüne verilen genel isimdir (Demir 2014). Bilgisayar ağı üzerindeki bilgi gönderimi ve paylaşımı bir takım kurallar dâhilinde yapılmaktadır (Anonim 2011). Kullanılan bu kurallara "İnternet Protokolleri", ya da "TCP/IP Protokoller Ailesi" denir. Bir başka deyişle TCP/IP protokolleri bilgisayarlar arası veri iletişiminin kurallarını koyar (Anonim 2011).

Bu protokoller adeta birbirleriyle iletişim kuran milyonlarca bilgisayardan oluşan bir ağda yer alan değişik yapıdaki bilgisayarların kendi aralarında iletişim kurabilmeleri için oluşturulmuş olan bir anlaşma dilidir. TCP/IP protokolü haricinde bazı anlaşma dilleri oluşturulmuşsa da genel olarak kabul görmediğinden günümüz için İnternet ağında en çok kullanılan anlaşma dili TCP/IP protokolüdür (Demir 2014).

2.2.8 HTTP (Hyber Text Transfer Protocol)

HTTP (İngilizce Hyper Text Transfer Protocol, Türkçe Hiper Metin Transfer Protokolü) belirli bir kaynaktan paylaşılan ve ortak kullanıma açık olan hiper ortam bilgi sistemleri için uygulama seviyesinde bir iletişim kuralıdır (İnt.Kyn.5). En başta HTML sayfaları göndermek için yaratılmış olan bir protokol olup şimdiki zamanda ise her türlü bilgi ve verinin gönderimi için kullanılmaktadır. TCP üzerinden çalışır (İnt.Kyn.6). Gelen isteğe yanıt verme ilkesi ile çalışır. Sunucu bekler, İnternet kullanıcılardan gelen isteklere

yanıt verir. HTTP, İnternet kullanıcısıyla bir bağlantı oluşturmaz. HTTP daha çok, 80 numaralı TCP portu üzerinden güvenilir TCP bağlantılarını kullanır (Megep 2008). HTTP pasif bir protokoldür. Pasif bir protokol olması sebebiyle kendisi bağlantı kurmaz ve bağlantı durumuyla ilgilenmez. Sadece kendisine gelen istek olduğunda istenilen verileri gönderir (Megep 2008).

1990 yılından beri Dünya Çapında Ağ (www) üzerinde küresel bilgi girişimi için HTTP kullanılmaktadır. HTTP/0.9 olarak bahsedilen ilk versiyonu İnternet üzerinden ham verinin taşınması amacıyla kurulmuş basit bir iletişim kuralıydı (İnt.Kyn.5). HTTP/1.0, ise taşınan verinin meta bilgilerini ve istek/yanıt semantiği düzenleyicilerini içeren ve MIME ilgileri taşıyan verilerin taşınabilmesi gibi ilkler ile bir önceki sürümü genişletmiştir. HTTP/1.0 yine de hiyerarşik proxy sunucuların, önbelleğin, kalıcı bağlantı ihtiyaçlarının ve sanal sunucuların etkilerini karşılamakta yetersiz kalmaktaydı (İnt.Kyn.5). Bu yetersizliğin ortadan kaldırılması için doğal olarak HTTP/1.1 ortaya çıkmıştır. HTTP/1.1 protokolü, sunucu ve İnternet kullanıcısı arasında bir bağlantının kurulabilmesi için istek ve yanıt mesajlarına uygun hazırlanmış bir web dili belirler (Megep 2008). HTTP/1.1 versiyon olarak iletişim kuralının güvenilir bir biçimde uygulanmasında ihtiyaç duyulan dizisel gereksinimleri kapsamakta ve bir önceki HTTP/1.0 sürümüne sahip iletişim kuralından çok daha güvenli olarak görülmektedir (İnt.Kyn.5).

2.2.9 FTP (File Transfer Protocol)

FTP (İngilizce File Transfer Protocol, Türkçe Dosya İletim Protokolü) dosya göndermek ve dosya almak için kullanılmaktadır. HTTP'den farklı olarak İnternet kullanıcısının sisteme giriş yapmasını gerektirmektedir. Veri ve komut alış verişi için iki ayrı port kullanır ve TCP üzerinden çalışır (İnt.Kyn.6). Herhangi bir dosyayı FTP kullanarak başka bir TCP/IP ağı üzerindeki kullanıcıya göndermek için o ağdaki bilgisayarda geçerli bir İnternet kullanıcı ismi ve şifresi gerekmektedir. Birçok FTP sunucusu, kullanıcı ismi ve parola olmadan erişim için "anonim FTP" (anonymous FTP) desteği verir, bu kullanım için kullanıcı adı olarak anonymous parola olarak ise bir email adresi girilmesi gerekmektedir (İnt.Kyn.7). FTP, dosya transferi ve komut

transferi için farklı portlar kullanmaktadır. Bir FTP bağlantısını açtığınızda port 20 ve port 21 olmak üzere iki porta birden bağlanmış olursunuz. Bu iki port iki farklı göreve sahiptir. Port 20, veri portudur, port 21 ise denetim portudur. (Megep 2008).

FTP Amerika Savunma Bakanlığının ARPANET üzerinde 1960'lardan 1980'lere kadar kullandığı eski bir protokoldür. Öncelikli vazifesi; bilgisayarlar arasında kararlı ve güvenilir bir şekilde dosya transferi sağlamaktır. FTP bu güvenilirliği ve kararlılığı İnternet üzerine taşıdığı için günümüzde de halen kullanılmaktadır (Megep 2008).

2.2.10 World Wide Web (www)

Sözcük anlamı olarak dünyayı saran ağ anlamına gelen world wide web'e kısaca "web" denilmektedir. Web; film, animasyon, ses, yazı, resim gibi birbirinden farklı verilerin aktarılmasını sağlayan bir sistem niteliğindedir. Günlük yaşantımızın adeta bir parçası haline gelen world wide web ile HTTP (Hyper Text Transfer Protocol) kullanılarak veri transferi gerçekleştirilmektedir (Demir 2014). Web sayfaları metin halindeki bilgilerin yanı sıra resim, video gösterme gibi imkânlara sahip olup, daha ilginç ve etkileyici şekilde bilgi sunduğu için bilgiye ulaşım aracı olarak yaygın bir şekilde kullanılmaktadır (Tümerdem 2013).

World Wide Web (www) kavramı ilk defa Tim Berners Lee tarafından ortaya atılmıştır (Köse ve Özen 2010). Tim Berners Lee World Wide Web kavramının yaygınlaşması ve birçok şirkete servetler kazandırmasına rağmen maddi konudan uzak durmuş ve geliştirdiği teknolojinin kamusal alanda kalması, bilim insanları ve öğrenciler için ulaşılabilir olmasına gayret etmiştir (İnt.Kyn.22).

World Wide Web (www) belgeler arasında geçiş imkânı sağlamaktadır. Bu geçiş web belgesindeki hypertext linke tıklanarak gerçekleştirilir. Bu şekilde aynı sunucudan veya bir başka sunucudan bir belge çağrılabileceği gibi sunucuda yüklü olmayan kişinin bilgisayarında bulunan bir belgede çağrılabilir. Web hizmet merkezlerine ulaşmayı sağlayan ara birim programlarına "web tarayıcısı" denilmektedir (Tümerdem 2013).

2.2.11 Web Tarayıcı (Web Browser)

İnternet sayfalarına web tarayıcı (web browser) denilen kullanıcı ara birim programları ile erişilmektedir. İnternette yer alan dokümanların yazıldığı bilgisayar dili deşifre edilip kullanıcının bu dokümanları bilgisayar ekranında yazılar, resimler ve benzeri şekiller olarak görmesini sağlayan aracı programlardır. Bilgisayar donanım açısından her ne kadar mükemmel olsa da İnternet nesnelerini kullanıcıların anlayabileceği hâle getiren tarayıcılar olmadan İnternetten faydalanmak mümkün değildir (Anonim 2011). En çok kullanılan web tarayıcıları çıkış tarihleriyle beraber şunlardır: WorldWideWeb (1991), Mosaic (1993), Netscape Navigator ve Netscape Communicator (1994), İnternet Explorer (1995), Opera (1996), Mozilla Navigator (2002), Safari (2003), Mozilla Firefox (2004), Google Chrome (2008), Yandex Browser (2012) (İnt.Kyn.8).

2.2.12 Elektronik Posta (e-mail)

Elektronik posta İnternete bağlı çok sayıdaki kullanıcının kendi aralarında birbirleriyle veri transferi için kullandıkları elektronik mesaj iletim sistemidir (Tulum 2006). Halen İnternet hizmetleri içinde en fazla kullanılan hizmet türüdür.

2.2.13 IP Adresi

IP Adresi (İnternet Protocol Address), İnterneti veya TCP/IP protokolünü kullanan diğer paket anahtarlamalı ağlara bağlı cihazların, ağ üzerinde birbirlerine veri transferi yapmak için kullandıkları adrestir (İnt.Kyn.9). TCP/IP şebekesinde bulunan bilgisayar ya da cihazların kimlik numarasıdır (Evren ve Güngör 2002). TCP/IP protokolünü kullanan şebekeler veri paketlerini IP adreslerine yönlendirir. IP adreslerinin formatında 32 bit numara adresi bulunmakta olup, dört rakam birbirlerinden aralarına noktalar konmak üzere ayrılmaktadır. Her numara 255'e kadar olabilir. Örneğin 115.17.140.3 bir IP adresi olabilir (Evren ve Güngör 2002).

2.2.14 Alan Adı (Domain Name)

İnternet bağlantılarında sayıların bazı durumlarda çeşitli sorunlar teşkil etmeleri nedeniyle aynı basamaklar yerine sözcükler gösteren ve sözcükler bilgisayara girildiğinde doğru adresi bulan, bu işlemlerin yapılmasını sağlayan "Alan Adı Sistemi" (Domain Name System) denilen yazılımın geliştirilmesi İnternet erişimini daha kolay bir hale getirmiştir (Tulum 2006). Örneğin 216.58.217.36 gibi çok basamaklı, akılda kalması zor ve birbirinden farklı rakamlar yerine www.google.com yazılmak suretiyle aynı işlem yapılarak google arama motoru sitesine ulaşılabilmektedir (İnt.Kyn.10).

Herhangi bir alan adı, Alan Adı Sistemine göre noktalarla ayrılan dört farklı ana bölümden oluşmaktadır. Soldan sağa doğru gidildiğinde birinci bölüm kullanılan TCP/IP alt protokolünü göstermektedir (İnt.Kyn.11). Bundan www, ftp, irc, gopher alanları anlaşılır. İkinci bölüm ilgili bilgisayarın ismidir. Üçüncü bölüm bilgisayarın bağlı olduğu kurumun hangi türden bir kuruluş olduğunu gösterir. Örnek verecek olursak "com" ticari kuruluşları gösterir, "edu" kısaltması eğitim kuruluşları ve üniversiteleri gösterir. Dördüncü kısaltma ise bilgisayarın bulunduğu ülkeyi gösterir. Örneğin "uk" İngiltere'yi , "tr" Türkiye'yi göstermektedir (İnt.Kyn.12).

İnternetin ilk olarak ABD ortaya çıkması sebebiyle bu ülkeye ait kısaltma yoktur ve bazı uluslararası kuruluşlar bu ülkedeymiş gibi alan adı alabilmektedir. Örneğin "www.mynet.com" gibi (İnt.Kyn.13).

2.2.15 Nesne Tabanı (URL) Adresi

Uniform Resource Locator (URL) yani Nesne tabanı, İnternette bulunun herhangi bir resim, yazı veya müzik gibi bir kaynağa karşılık gelen standart bir formatta uygun karakter dizgisidir (Dülger 2013). Uniform Resource Locator (URL), İnternet üzerindeki bir kaynağın tam olarak bulunduğu yer veya bir başka deyişle koordinatıdır. Kişinin İnternette gezinirken bir kaynağa tıkladığında adres çubuğunda görünen tam adrestir (Dülger 2013).

2.2.16 Sunucu (Server)

Sunucular, dijital verileri kapasiteleri oranında muhafaza ederek diğer erişim cihazlarına hizmet sağlayan bilgisayarlar ya da programlarıdır (Demir 2014). İnternet servis sağlayıcıları, üstlendikleri hizmetleri yerine getirebilmek için sunucuları kullanırlar. Bir ana bilgisayar olarak da düşünülebilecek olan sunucu, bir ya da birden fazla ağa bağlanabilen bir cihaz olarak da ifade edilebilir (Demir 2014).

2.2.17 Proxy Sunucusu

Proxy sunucu, herhangi bir web tarayıcısı ve İnternet arasında aracı işlevini gören bilgisayarlardır. Proxy sunucular, sık sık kullanılan web sayfalarının bir kopyasını depolayarak web hızının artmasını sağlamaktadır (İnt.Kyn.14). Bir proxy sunucusu, sizden aldığı istekleri yürütür ve sonucu yine size bildirir. Örnek verecek olursak Proxy sunucu kullanarak "mynet.com" sitesine bağlanıldığında Proxy mynet.com' a istek gönderir ve elde ettiği verileri kullanıcıya sunar. Dolayısıyla da kullanıcı mynet.com' a direkt bağlanmış olmaz. Aynı zamanda, bu bilgiler proxy sunucusu üzerinde muhafaza edilir ve bir dahaki erişimde kullanıcının istediği verileri doğrudan ilgili İnternet sitesinden değil de, proxy sunucusundan gelir. Önbellekten gelen verilerin iletişimi daha hızlı olmaktadır. İnternete erişim için bir proxy servisine ihtiyaç olmadığı bilinmelidir. (İnt.Kyn.15). Ayrıca Proxy sunucu üzeride tutulan günlükler çeşitli programlar yardımıyla raporlara dönüştürülüp bunların sonradan incelenmesi sağlanabilir. Kim nereye ne zaman girmiş gibi soruların cevabı bu alanda bulunabilir (İnt.Kyn.16).

2.2.18 Router

Route yön, router ise yönlendirici anlamına gelmektedir. Bir ağdaki aktif donanım olarak routerlar yönlendirme işlemi yapmaktadırlar. Ağdaki bilgisayarların yönlerini bulmalarını sağlarlar. Başka bir deyişle ağdaki IP paketlerini herhangi bir bilgisayar ağından başka bir bilgisayar ağına taşımaya yarayan cihazlardır (İnt.Kyn.17). Yönlendirme için OSI (Open Systems Interconnection) yedi katman modelinin üçüncü katmanı olan ağ katmanı kullanmaktadır. Bir router'ın amacı gelen ağ paketlerini

incelemektir. Paketlerin, ağdan geçebilmesi için en iyi yolu belirler ve switch'ten porta doğru bir şekilde gitmelerini sağlar. Router'lar özellikle büyük ağlarda akışı sağlayan ve trafiği düzenleyen en önemli cihazladır. (İnt.Kyn.17).

2.2.19 Modem

Modem, tanım olarak "Modülatör" ve "De modülatör" kelimelerinin birleşiminden oluşmaktadır. Çevirge ya da Modem, bilgisayarların İnternete bağlanmasını sağlayan ve bir bilgisayarı kendinden daha uzak yerdeki bilgisayarlara bağlayan cihazdır (Birsen 2014). Modem, verileri ses sinyallerine, ses sinyallerini verilere dönüştürerek verileri bir yerden başka bir yere taşır (Birsen 2014). Bilgisayarın ana veri yoluna direkt monte edilebilene dahili modem, bilgisayara dışarıdan kabloyla bağlanana ise harici modem denmektedir (Osman et all. 2013). Mobil cihazlar aracılığı ile kurulan İnternet bağlantılarında cihaz harici modem rolünü üstlenmektedir (Osman et all. 2013)

2.2.20 Erişim

Yönetmelik ve kanun, aynı tanımı vermektedir. Erişim bir İnternet ortamına bağlanarak kullanım olanağı kazanılmasıdır. Buna göre, erişim bir İnternet sitesine İnternet ağı yoluyla ulaşabilmeyi ifade etmektedir (İnt.Kyn.18).

2.2.21 İnternet Kontrol Noktaları

İnternete erişim engellemesi aşağıdaki kontrol noktalarından herhangi birinde olabileceği gibi bunların tümünde ya da herhangi birinde yapılacak bir filtreleme ile de mümkün olmaktadır (İnt.Kyn.19).

2.2.21.1 İnternet Omurgası

Büyük çaplı İnternet ağ işletmecileri ya da büyük alanları kapsayan ağlar omurga sağlayıcı olarak telaffuz edilmektedir. Öte yandan bu alt yapıların omurga olarak tanımlanabilmeleri için geniş coğrafi alana yayılmış olmaları ve küçük çaplı İnternet

Servis Sağlayıcılara veri transfer hizmeti vermeleri gerekmektedir (Güngör ve Evren 2002). Devletler tarafından genel olarak yapılacak İnternete erişim engellemesinde, ulusal içerik filtreleme programları ve engelleme teknolojileri kullanılarak tüm ülke genelinde İnternet erişimini etkileyen, omurga düzeyinde filtreleme yapılabilir (İnt.Kyn.19).

2.2.21.2 İnternet Servis Sağlayıcıları

İngilizce adı İnternet Service Provider (ISP) olarak bilinmektedir. 5651 sayılı kanunda erişim sağlayıcı olarak yer almaktadır. İnternet servis sağlayıcıları bilgisayar kullanıcılarının İnternete bağlanmasını, İnternet üzerinden iletişim kurmasını ve İnternetin tanıdığı olanakları kullanmalarını sağlayan aracı gerçek veya tüzel kişilerdir (Tümerdem 2013). Geniş anlamıyla İnternet hizmeti sunan herhangi bir oluşuma İnternet Servis Sağlayıcısı denebilir (Güngör ve Evren 2002). Bu tanım çerçevesinde çevirmeli İnternet erişimi sunan bir işletmeciden uluslararası Telekomünikasyon Birliğine kadar İnternet hizmeti veren her türlü kuruluş İnternet Servis Sağlayıcısı olarak görülebilir (Güngör ve Evren 2002).

İnternet Servis Sağlayıcıları bu hizmeti belirli bir ücret karşılığı vermektedirler. Bir İnternet Servis Sağlayıcısına bağlanmanın en çok kullanılan yolu telefon hattı ya da geniş bant bağlantısıdır. Birçok İnternet Servis Sağlayıcısı e-posta hesapları, web tarayıcıları gibi ek hizmetler ile beraber web sitesi oluşturmak için alan da sağlamaktadır.

İnternet Servis Sağlayıcılar İnternetle ilgili farklı hizmetler sunabilmektedirler. Aşağıda bu hizmetlerin bir bölümü verilmiştir:

- ADSL
- Dial-up
- Kablo İnternet
- Genişbant
- E-Posta
- Datacenter Hizmetleri

- Colocation
- Dedicated Sunucular
- Kişisel Web Alanı
- VoIP
- Kablosuz Servis Sağlayıcı (İnt.Kyn.17)

Devletlerin bir diğer erişim engelleme politikası da İnternet Servis Sağlayıcıları tarafından yürütülmektedir (İnt.Kyn.19).

2.2.21.3 Kurumlar

Kurumlar içerisinde kullanılan intranet ağlar, kamu kuruluşları, okullar veya İnternet kafelerde teknik engelleme ve / veya öz sansür yöntemi ile filtreleme yapılabilmektedir (İnt.Kyn.19). Bazı ülkelerde, engelleme hükümetlerin emriyle gerçekleşir. Kurumsal düzey filtrelemeye işyeri bilgisayarlarının eğlence için kullanımının önlenmesi, İnternet kafelerde yaş doğrulama sistemleri kullanılması vb. durumlar örnek olarak gösterilebilir.

2.2.21.4 Bireysel Bilgisayarlar

Ev ya da bireysel bilgisayar düzeyinde filtreleme belirli sitelere erişmek için tek bir bilgisayarın yeteneğini kısıtlayan filtreleme yazılımı kullanımı ile gerçekleşmektedir (İnt.Kyn.19). Daha çok aileler tarafından çocukların İnternet üzerinden erişebilecekleri zararlı ortamlardan uzak tutulması için kullanılmaktadır.

2.2.22 Yer Sağlayıcı (Hosting)

İnternete açık hizmet ve içerikleri muhafaza eden sistemleri sağlayan veya işleten gerçek veya tüzel kişilerdir. Yer sağlayıcıların yapmış olduğu faaliyetin ticari amacı olsun veya olmasın yönetmelik gereğince gerçek veya tüzel kişilerin “Yer Sağlayıcılığı Faaliyet Belgesi” almaları zorunludur (İnt.Kyn.20).

Yer Sağlayıcılığı Faaliyet Belgesi almak için;

1) http://faaliyet.tib.gov.tr/yetbel adresindeki mevcut sisteme kayıt olarak giriş yapıp buradaki yer sağlayıcı başvuru formunun doldurulması ile başvuruda bulunulmalıdır,

2) Yönetmeliğin Ek 5'inde örneği olan dilekçe ve elektronik ortamda doldurulan başvuru formunun çıktısı ile beraber Telekomünikasyon Kurumu - İletişim Başkanlığı / Cevizlidere Caddesi No:11 Balgat / ANKARA adresine gönderilir. Tüzel kişiler (Anonim ve Limited Şirketler) başvuru formu ve dilekçe haricinde ayrıca şirketin Ticaret Siciline tescil edildiğini belirten son altı ay içinde alınmış olan Ticaret Sicil Kaydının aslı veya noter tasdikli suretiyle Şirkete ait imza sirküleri aslı veya noter tasdikli suretini göndermelidirler (İnt.Kyn.20).

5651 sayılı kanunda yer sağlayıcılarla ilgili olarak "Yer sağlayıcı, yer sağladığı içeriği kontrol etmek veya hukuka aykırı bir faaliyetin söz konusu olup olmadığını araştırmakla yükümlü değildir. Yer sağlayıcı, yer sağladığı hukuka aykırı içeriği bu Kanunun 8 inci ve 9 uncu maddelerine göre haberdar edilmesi halinde yayından çıkarmakla yükümlüdür. Yer sağlayıcı, yer sağladığı hizmetlere ilişkin trafik bilgilerini bir yıldan az ve iki yıldan fazla olmamak üzere yönetmelikte belirlenecek süre kadar saklamakla ve bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini sağlamakla yükümlüdür. Yer sağlayıcılar, yönetmelikle belirlenecek usul ve esaslar çerçevesinde yaptıkları işin niteliğine göre sınıflandırılabilir ve hak ve yükümlülükleri itibarıyla farklılaştırılabilirler Yer sağlayıcı, Başkanlığın talep ettiği bilgileri talep edilen şekilde Başkanlığa teslim etmekle ve Başkanlıkça bildirilen tedbirleri almakla yükümlüdür" (5651 S.K. 2014) denmektedir.

2.2.23 İçerik Sağlayıcı

İnternet ortamı üzerinden İnternet kullanıcılarının hizmetine sunulan bilgi veya veriyi oluşturan, değiştiren ve sağlayan gerçek veya tüzel kişileri ifade etmektedir (5651 S.K.). Buradan da anlaşılıyor ki İnternet sitelerine yorum, yazı vb. yazan ya da resim, müzik vb. içerikler ekleyen kullanıcıları ya da bir İnternet sitesi, blog vb. şeklinde İnternette

sayfa açan bütün gerçek ve tüzel kişiler anlaşılmaktadır (İnt.Kyn.21). Örnek verecek olursak herhangi bir kullanıcı gazeteci kendi bloğunda yazdığı yazıları açısından içerik sağlayıcıdır veya bir üniversite, kendi İnternet sitesindeki bütün içerik açısından içerik sağlayıcıdır. Haber sitelerindeki kendi girmediği haberlerin altına yorum yazan kullanıcılar ilgili yorumları açısından içerik sağlayıcısı durumundadır. CNNTurk.com özelinde düşünecek olursak, editörler, muhabirler ve yorum yazarak katkı sağlayan okuyucular içerik sağlayıcıdır (İnt.Kyn.21).

5651 sayılı kanunun 4. maddesinde içerik sağlayıcının sorumluluğu şu şekilde düzenlenmiştir. İçerik sağlayıcılar İnternet ortamında paylaştığı her türlü içerikten dolayı sorumludur. İçerik sağlayıcılar, bağlantısını sağladıkları başkasına ait içeriklerden sorumlu değildirler. Fakat sunuş biçiminden, bağlantısını sağladığı içeriği benimsediği için ve kullanıcının söz konusu içeriğe ulaşmasını amaçladığını açıkça belli ediyor ise genel hükümlere göre sorumludur. Telekomünikasyon İletişim Başkanlığının (TİB) 5651 sayılı kanunda ve diğer kanunlarla verilen görevlerinin yapılması kapsamında içerik sağlayıcıdan talep ettiği bilgileri talep edilen şekilde TİB'e teslim etmek ve Başkanlıkça kendisine bildirilen tedbirleri almakla sorumludur (5651 S.K. 2014).

2.2.24 İnternet Toplu Kullanım Sağlayıcı

Kullanıcılara belirli yer ve belirli sürelerde İnternet ortamı kullanma imkanı sağlayan gerçek ve tüzel kişiler İnternet toplu kullanım sağlayıcıları ifade eder (İnt.Kyn.21). Örneğin kablosuz ağ bağlantısını kullanımınıza açan kahve dükkânı ya da kaldığınız otel, bindiğiniz şehirlerarası otobüs, okuduğunuz üniversite, maaşlı çalıştığınız işyeri.

2.2.25 Ticari Amaçla İnternet Toplu Kullanım Sağlayıcı

Belirli süre ve belirli yerlerde ücret karşılığı İnternet toplu kullanım faaliyeti yürüten, bunun yanında bilgi, beceri ve zeka artırdığı düşünülen oyunların oynatılmasına olanak sağlayan gerçek ve tüzel kişiler ticari amaçlı İnternet toplu kullanım sağlayıcılarını ifade etmektedirler. Örnek verecek olursak İnternet kafeler ticari amaçlı İnternet toplu

kullanım sağlayıcılarıdır (İnt.Kyn.21). Ticarî amaçlı toplu kullanım sağlayıcılar bu hizmeti verebilmek için mahallî mülkî amirden izin belgesi almak zorundadır. Ticari amaçlı toplu İnternet sağlayıcıların yapmış olduğu faaliyetleri mahalli mülki amirler denetlerler. İzin belgesinin alınması ve bu yerlerin denetime ilişkin bilgiler yönetmelikle düzenlenmektedir. Ticari amaçlı olsun veya olmasın bütün İnternet toplu kullanım sağlayıcılar, konusu suç oluşturan içeriklere erişimin engellenmesi ve kullanımının önlenmesi için yöneltmelikte yer alan tedbirleri almak zorundadır (5651 S.K. 2014).

3. MATERYAL VE METOT

Bu çalışmada betimsel literatür taraması araştırma metodu kullanılmıştır. Türkiye'de İnternet erişiminin engellenmesiyle ilgili olarak 2007 yılında yürürlüğe giren ve en son Şubat 2014'te düzenleme yapılan 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'dan yararlanılmıştır. Türkiye'deki erişim engelleme düzenlemesiyle öne çıkan diğer kaynaklar ise Dülger (2013)'in eseri Bilişim Suçları ve İnternet İletişim Hukuku, Beceni ve Dülger (2011)'in eseri Türkiye'de İnternet Sitelerinin Erişiminin Engellenmesi Konusunda Farklı Hukuk Disiplinleri Açısından Değerlendirmeler, Kılınç (2010)'ın eseri Türk Hukukunda ve Mukayeseli Hukukta İnternet Sitelerine Erişimin Engellenmesi ve İfade Hürriyeti, Memiş (2009)'in eseri Erişimin Engellenmesi, Hukuki Sorunlar ve Çözüm Önerileri ile Kaya (2009)'nın eseri Teknik ve Hukuki Boyutuyla İnternet Erişiminin Engellenmesidir.

Bazı ülkelerde uygulanan erişim engelleme düzenlemeleri ile ilgili olarak incelenen eserler Palfrey vd. (2011)'nin eseri Access Contested: Security, Identity, and Resistance in Asian Cyberspace, Warf (2011)'ın eseri Geographies of Global İnternet Censorship, Deibert vd (2010)'nin eseri Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace ve Zittrain vd. (2008)'nin eseri Access Denied: The Practice and Policy of Global Internet Filtering'dir.

4. İNTERNET ERİŞİMİNİ TEKNİK OLARAK ENGELLEME VE ENGELLEMEYİ AŞMA YÖNTEMLERİ

Yönetim politikaları ile paralel olarak devletler mahkeme kararıyla ve mahkeme kararı olmaksızın veya İnternet erişimi ile ilgili hukuki düzenlemeleri gerekçe göstererek kendince sakıncalı gördüğü İnternet sitelerini erişimi engellemektedir. Devletlerin geliştirdiği engelleme metotlarına karşı engellemeyi aşma teknikleri de günden güne gelişmekte, legal veya illegal olarak yayılmaktadır.

4.1 Erişim Engelleme Yöntemleri

Devletler farklı neden ve farklı tekniklerle İnternet içeriğine, dolayısıyla İnternet erişimine müdahale etmektedir (Kaya 2010). Devletler belirli faaliyetlerin İnternet üzerinden gerçekleştirilmesini tamamıyla yasaklayabildikleri gibi, vatandaşların tüm İnternet aktivitelerini takip etmeyi de tercih edebilmektedir. Hukuka aykırı veya zararlı bir içeriği tespit ettiklerinde ise o içerikten vatandaşlarını korumak için erişim engelleme denilen müdahale yöntemlerine başvurmaktadır (Kaya 2010).

Türkiye'de İnternet erişiminin engellenmesindeki yetkili kurum TİB'dir (5651 S.K.). TİB'in İnternet sayfasında erişim engellemede uyguladıkları metotlarla ilgili olarak "Başkanlığımız, 5651 sayılı Kanunun 8'inci maddesi kapsamında erişim engelleme yöntemi olarak URL'den erişim engelleme, alan adından erişim engelleme, veya IP adresinden erişim engelleme yöntemlerini kullanmaktadır (İnt.Kyn.23)." denilmektedir.

4.1.1 IP Adresinden Erişim Engelleme

En temel ve kolay erişim engelleme metodu İnternet sitelerinin yer aldığı sunucuların IP adresinden erişimin engellenmesidir. İnternetteki verilerin paketler halinde doğru noktalara ulaştırmakla yükümlü İnternet Servis Sağlayıcılardaki cihazlar router'dır. Bunlar IP adresine bakar ve hangi yoldan yollanacağına karar verir. IP paketi oradan başka bir router'a yollar. Yolladığı yerdeki router alır doğru yere atar ve paketler hedefine varır. IP tabanlı erişim engellemede İnternet Servis Sağlayıcılar router'lara

engellenen IP adreslerini tanımlarlar ve İnternet erişiminin engellenmesi gerçekleşmiş olur (İnt.Kyn.24). Erişim engellemenin kapsamı açısından yapılacak tercihe göre, İnternet Servis Sağlayıcısı nezdinde ya da İnternet omurgasında ilgili İnternet sitesinin IP adresinin engellenmesi mümkündür (Dülger 2013). IP engelleme için ek bir donanım yatırımı yapılmasına gerek yoktur ve maliyeti ucuzdur. Genellikle devletler tarafından İnternet Servis Sağlayıcıların kullanacağı teknik açısından bir zorunluluk bulunmamaktadır. Ek bir donanım gerektirmediği ve maliyeti çok ucuz olduğu için İnternet Servis Sağlayıcılar tarafından IP adresinden erişim engellemesi tekniği kullanılmaktadır (Dülger 2013).

IP adresinden erişimin engellenmesi ilgili İnternet sitesinin tüm servislerini İnternet erişime kapatmaktadır. İnternet kullanıcıları ilgili siteyi ziyaret edemeyeceği gibi sitesinin e-posta servisine de ulaşamayacaktır. IP adresinden erişim engellemesinin servis temelli olarak yapılması teknolojik olarak mümkündür (Dülger 2013). Her bir İnternet servisinin kendine özgü port olarak adlandırılan bir alt bağlantı numarası vardır. İnternet trafiği temel olarak 80 numaralı port üzerinden yayın yaparken, e-posta servisleri Simple Mail Transfer Protokol (STMP) protokolü üzerinden 25 numaralı portu kullanmaktadır. Sadece 80 portu üzerinde yapılacak bir sınırlama ile web trafiği engellenirken, web sitesinin diğer temel servisleri kullanmaya devam etmesi sağlanabilir (Kaya 2010).

4.1.2 Alan Adından (DNS) Erişim Engelleme

İnternet sitelerine erişim için kullanılacak IP adreslerinin hatırlanmaları zor olduğu için Domain Name System (DNS) Alan Adı Sistemi geliştirilerek, IP adresleri yerine geçen "Alan Adı" olarak adlandırılan harf dizinlerinin kullanılmasını sağlamıştır (Kaya 2010). İşte her erişim sağlayıcının bu çevirme işini yapan kendine ait DNS sunucuları mevcuttur. Tarayıcınıza bir alan adı yazdığınızda tarayıcı önce DNS sunucusuna sorar ve cevap alınca da ilgili siteye bağlanır. DNS engellemesi yapıldığında söz gelimi TTnet'in DNS server'ına dahil olduğumuzu var sayarsak, eğer bir sayfa yasaklanmışsa İnternet Servis Sağlayıcısı o sayfanın IP adresini DNS sunucusundan kaldırır, o yüzden istenilen sayfaya ulaşılamaz (İnt.Kyn.25). Örneğin sunucudan 72.14.235.104 IP adresi

silinirse Google arama motoru içeriğine (www.google.com) ulaşılamaz (Kaya 2010).

Alan adı sistemi hiyerarşik şekilde yapılanmıştır. Alan adı için en üst düzey yönetim A kök sunucusu tarafından gerçekleştirilmekte ve diğer 12 kök sunucu A kök sunucusu değerlerini referans almaktadır (Kaya 2010). Kök sunucuların altında jenerik (generic), ülke kodu (country code) ve altyapı (infrastructure) göre ayrılmış üst düzey alan adları (Top Level Domains) vardır. Alan adları "ilk gelen alır" prensibine göre bireylere veya kurumlara tahsis edilmektedir. Ülke kodlu uzantılar için ise devletlerin bazı sınırlamalar koyması mümkündür (Kaya 2010).

Alan adından erişim engellemenin IP adresinden erişim engellemede olduğu gibi büyük bir dezavantajı bulunmaktadır. IP adresinden erişim engellendiğinde ilgili site tüm alt içeriklerle beraber İnternet erişimine kapatılmaktadır (İnt.Kyn.24). Dünya çapında İnternet hizmet veren ve fazlaca kullanıcısı bulunan ücretsiz blog, e-posta veya benzeri hizmetler veren bir İnternet sitelerinin erişime engellenmesi ağır sonuçların ortaya çıkmasına sebep olmaktadır. Örneğin, "T.C. Diyarbakır 1. Sulh Ceza Mahkemesi 20 Ekim 2008 tarihinde popüler blog servisi www.blogger.com web sitesinin erişimini www.justin.tv. adlı web sitesinin yayınladığı LigTv maçlarının bir blog üzerinden sunulmasından dolayı engellemiştir. Site üzerindeki engelleme yasaktan dört gün sonra delil yetersizliğinden dolayı kaldırılmıştır. Blogger.com sitesi kullanıcılarına alt düzey alan adı (subdomain) olarak ücretsiz blog kurmalarına izin vermektedir. Sitenin bu şekilde yapılanması sayesinde, kullanıcı blogları içerik olarak birbirinden bağımsız bir şekilde yayınlarını sürdürmekte ve hukuka aykırı içerik ortaya çıktığında sadece o kullanıcıya ait blogun kapatılması mümkün olmaktadır. Buna rağmen mahkeme ilgili blogları kapatmak yerine tüm web sitesinin erişimini engellemiştir. Bunun sonucunda, masum milyonlarca blog da otomatik olarak engellenmiştir. Diğer bir deyişle, birden fazla web sitesini barındıran sunucu üzerinde IP adresinden erişim engellemede olduğu gibi ceza sorumluluğunun şahsiliği ilkesi ihlal edilmiş olmaktadır" (Kaya 2010).

4.1.3 Nesne Tabanlı (URL) Erişim Engelleme

5651 Sayılı İnternet Yasasının güncellemesiyle gündeme gelen URL (Uniform

Resource Locator) web tarayıcıların adres satırında yazan ve gitmek istediğiniz sayfayı tam olarak anlatan karmaşık harf, sayı ve karakterlerdir (İnt.Kyn.24). URL İnternette resim, yazı veya müzik gibi bir kaynağa karşılık gelen standart bir formatta uygun bir karakter dizgisidir. URL İnternet üzerindeki bir kaynağın tam olarak bulunduğu yer, bir başka deyişle o yerin koordinatıdır (Dülger 2013). Nesne tabanlı (URL) erişim engellemesi yalnızca hukuka aykırı içeriğe erişimin engellenmesi amacıyla uygulanan bir tekniktir. Bu yöntemin en önemli avantajının hukuka aykırı bir içerik için tüm İnternet sitesinin erişime engellenmesinin önlenmesi olduğu ifade edilmektedir (Dülger 2013).

5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanuna, Şubat 2014'te torba yasa ile yapılan düzenlemeyle URL adresinden erişim engelleme hükmü girmiştir. Kanunun 9/A maddesinde "İnternet ortamında yapılan yayın içeriği nedeniyle özel hayatının gizliliğinin ihlal edildiğini iddia eden kişiler, Başkanlığa doğrudan başvurarak içeriğe erişimin engellenmesi tedbirinin uygulanmasını isteyebilir. Yapılan bu istekte; hakkın ihlaline neden olan yayının tam adresi (URL), hangi açılardan hakkın ihlal edildiğine ilişkin açıklama ve kimlik bilgilerini ispatlayacak bilgilere yer verilir. Bu bilgilerde eksiklik olması hâlinde talep işleme konulmaz. Başkanlık, kendisine gelen bu talebi uygulanmak üzere derhâl Birliğe bildirir, erişim sağlayıcılar bu tedbir talebini derhâl, en geç dört saat içinde yerine getirir. Erişimin engellenmesi, özel hayatın gizliliğini ihlal eden yayın, kısım, bölüm, resim, video ile ilgili olarak (URL şeklinde) içeriğe erişimin engellenmesi yoluyla uygulanır" (5651 S.K. 2014) ibaresi yer almaktadır.

4.1.4 Proxy Sunucularını Kullanarak Erişimin Engellemesi

Proxy sunucular kullanıcıların İnternet erişimini hızlandıran ve ayrıca İnternet trafiğini izleyip bunların günlüğünü tutan bir sunucudur (İnt.Kyn.26). Proxy sunucular ağda mevcut olan diğer bilgisayarlara İnternet erişimi sağlayan bilgisayardır. Büyük ağların kurulumda proxy, şirketin bilgisayarları ile İnternet arasında durur. Proxy sunucu sayesinde ağ yöneticileri İnternet erişimi üzerinde kontrol yetkisine sahip olur. Aynı

zamanda üstün bir güvenlik duvarı ve ön bellekleme sistemi olarak da son derece verimlidir (İnt.Kyn.27). Proxy sunucu içerik ve kullanıcı arasında filtreleme görevi üstlendiği için kullanıcının istenmeyen içerikle veya virüs gibi zararlı programlarla karşılaşma riski ortadan kaldırmaktadır (Kaya 2010). Proxy sunucusu aynı zamanda IP adresini de gizleyerek İnternette anonim dolaşma imkanı sağlar (İnt.Kyn.27). Devletler Proxy sunucularını İnternet bağlantı noktalarına konumlandırarak web içeriğini filtreleyebilmekte ve bireylerin hangi web sitesine veya hangi tür içeriğe erişeceğini belirleyebilmektedir. Bu şekilde Proxy sunucular erişim engelleme amacıyla da kullanılabilmektedir (Kaya 2010).

4.1.5 İçerik Engellemesi

İnternet ağının belirli kuralları tanıyarak otomatik engelleme yapması fikir ve sanat eserlerinin dijital ortamda korunması için kullanılmakta olan Dijital Hak Yönetimi (DRM) sistemiyle aynı prensiplerle çalışmaktadır (Kaya 2010). DRM yazılımları elektronik ortamdaki dosyaların değiştirilmesini, tamamen kopyalanmasını, içeriğinin kopyalanmasını, yazıcıdan çıktı alınması sırasında değişikliğe uğratılmasını, çıktı alınmasını, hatta ekran görüntüsünün alınmasını bile engelleyebilmektedir (Aşçıoğlu ve Şamlı 2008). Routerlar içerik katmanına müdahale etmeden veri paketlerinin üzerlerinde yer alan etiket katmanını esas alarak veri iletimi geçekleştirmektedir. Veriler parçalar halinde iletildiği için engellenecek içeriğin tespit edilebilmesi için paketlerin bir noktada birleştirilerek denetlenmesi gerekmektedir(Kaya 2010). Engellenmeyen içerik ise tekrar parçalara ayrılarak nihai iletim adreslerine iletilmesi gerekmektedir. Routerlar DRM sistemleri ile aynı prensibe göre programlanarak ağ üzerinde belirli kelimeleri içeren veri parçalarını denetlemeleri sağlanabilmektedir. Bu sayede, bir noktadan başka bir noktaya iletilen verilerin içerik katmanında, kelime, URL veya alan adı temelli olarak inceleme yapılması mümkün olmaktadır (Kaya 2010).

Diğer taraftan içerik engellemesi çoğu zaman aşırı engellemeye sebep olmaktadır. Örneğin, "İngiliz Essex ve Sussex Üniversitelerinin web siteleri erişim engelleme sistemine zararsız site olarak tanıtılmadıkları sürece alan adlarında bulunan sex kelimesi sebebiyle cinsel içerikli web sitesi olarak muamele göreceklerdir. Benzer bir şekilde

cinsel hastalıklar konusunda bilgi veren bir sağlık sitesi de aynı tür bir engellemeye takılacaktır. Diğer taraftan web sitelerinin içeriği şifreli olarak sunulduğu durumlarda içerik engelleme sistemleri çaresiz kalmaktadır" (Kaya 2010).

4.1.6 DDOS Atakları

Herhangi bir saldırgan tarafından önceden tasarladığı çok sayıdaki makine üzerinden saldırı yapılacak olan bilgisayara ataklar düzenleyerek hedef sistemin kullanıcılarına hizmet veremez hale gelmesini hedefleyen saldırı türüdür (İnt.Kyn.28). Bazen devletler, egemenlik alanları dışında kalan yabancı ağlarda barındırılan sitelerin erişimin tamamen engelleme ihtiyacı duyabilirler. Bu durum daha çok ülke genelinde erişim engellemenin gereken faydayı vermediği veya siyasi muhaliflerin veya terör örgütlerinin propagandalarını tamamen engelleme ihtiyacı duyulduğu zamanlarda gündeme gelebilmektedir (Kaya 2010). Örneğin devlet terör örgütü propagandası yapan sitelere erişimi engellemiş ve ülke genelinde web siteleri etkisiz hale getirmiştir. Ancak siteler dünya genelinde erişilir olduğu için devlet engelleme konusunda amacına ulaşamamıştır. Bu gibi durumlarda bazı otoriter devletler kullanımı hukuka aykırı olan DDOS ağ saldırı yöntemine başvurabilmektedir.

Koordineli olarak yapılan DDOS atakları saldırının boyutunu büyütür ve saldırganın gizlenmesini sağlar. Bu işlemleri yapan aracı kullanıcı bilgisayarlarına zombi denmektedir. Bu saldırı türünde saldırganı bulmak oldukça zordur. Çünkü saldırının merkezinde bulunan saldırgan, saldırıyı zombi kullanıcılar aracılığıyla gerçekleştirir ve asla saldırıya katılmaz. Sadece zombi bilgisayarları yönlendirir (İnt.Kyn.29). DDOS saldırılarında asıl failin bulunması zor olduğu için bazen devletler tarafından hukuka aykırı bir erişim engelleme metodu olarak kullanılabilmektedir. Örneğin Kırgızistan'da gerçekleştirilen Şubat 2005 seçimleri sırasında muhalif sitelerin web siteleri DDOS saldırısına uğramış ve erişilemez hale gelmiştir. Muhalif partiler bu saldırıdan dolayı iktidar partisini suçlamışlardır. Ancak belirtildiği üzere bu tür saldırılarda failleri tespit etmek zor olduğu için herhangi bir neticeye ulaşılamamıştır (Kaya 2010).

4.1.7 Fiziksel Sunuculara Müdahale Edilerek

Sunucu, herhangi bir ağ üzerinde bir programı veya bir veriyi çeşitli kullanıcılara / sistemlere dağıtan donanım veya yazılımlara verilen genel isimdir. Buradaki en temel nokta, sunucuların bir bilgisayar ağına bağlı olmasıdır. Donanımsal ve yazılımsal olarak sunucuların, sorun çıkarmadan çalışmak üzere kurulmuş, güvenilir, çoklu kullanıcıya hizmet veren bilgisayar sistemleri olduğu söylenebilir. Örnek verecek olursak, PC Labs'ın bulunduğu bilgisayar sistemi sunucudur ve bu bilgiler İnternet aracılığı ile siteyi ziyaret eden kullanıcılara dağıtılır (İnt.Kyn.30). İnternete bağlı her sunucunun fiziksel olarak bir yerde barındırılması gerekmektedir. Sunucu barındırma hizmetleri devletlerin denetimi altında gerçekleştirilmektedir. Bulunduğu ülkenin hukuk kurallarına aykırı bir web sunucusunun İnternet bağlantısı fiziksel olarak kesilerek içeriğe erişimin tamamen engellenmesi mümkündür (Kaya 2010).

4.1.8 Ağ Hataları

İnternet erişiminin engellemelerinde karşılaşılan diğer bir durum ise web sitesine erişilmeye çalışıldığında bağlantı hatası olduğunu gösteren mesajlarla karşılaşmaktır. Herhangi bir siteye ulaşmaya çalıştıklarında ağ hatası meydana geldi uyarısıyla karşılaşan kullanıcılar içerik ve hizmet sağlayıcılar İnternet sitesine teknik bir sorun sebebiyle ulaşamadığı yanılgısına düşmektedir. İnternet sitelerinin yönetici otorite tarafından engellendiğinin farkına varamamaktadır (Kaya 2010). Örnek verecek olursak, İngiliz Telekom şirketi, Cleanfeed adı verilen bir kontrol sistemiyle İnternet Denetim Kurulunun hazırlamış olduğu yasaklı listesine göre İnternet trafiğini filtrelemektedir. Yapılan bu filtreleme neticesine listede yer alan bir sayfa bulunduğunda sistem "Sayfa Bulunamadı" hatası vermektedir (Köse ve Özen 2010). Özellikle telekomünikasyon sektörünün devlet tekelinde olduğu dolayısıyla tüm İnternet ağının sadece devlet tarafından yönetildiği ülkelerde bu yöntem etkin bir erişim engelleme yöntemi olarak kullanılabilir. Nihayetinde devlet tekeli yüzünden içerik ve hizmet sağlayıcıların elinde hatanın kesin çözümlenmesini sağlayacak ve ağda ayrıntılı inceleme yetkiler olmadığı için devlet müdahalesi ispatlanamamaktadır (Kaya 2010).

4.2 Erişim Engellemesini Aşmak İçin Kullanılan Teknikler

4.2.1 VPN (Virtual Private Network) Kullanarak

VPN (Virtual Private Network) basit anlamıyla İnternete bir başka bilgisayar üzerinden şifreli (kriptolu) girme işlemidir. Bu yöntemde bilgisayarınız bağlanmak istediğiniz sitelere doğrudan değil, tanımladığınız VPN sunucusu üstünden erişir (İnt.Kyn.31). Böylece hem bütün veri akışınız şifrelenir (dışarıdan teknik takibi fayda etmez) hem de İnternet ile aranızda bir perde, koruma kalkanı yer almış olur. Karşıdaki hizmet sizin kim olduğunuzu bilemez, aradaki VPN sistemiyle muhatap olur (İnt.Kyn.32).

İki çeşit VPN bağlantısı vardır. Birincisi, evinde çalışan veya seyahat esnasında ofisinde olamayan kullanıcıların İnternet üzerinden özel ağ üzerindeki sunucuya erişime olanağı sunan uzaktan erişim VPN'dir. Uzaktan erişim VPN bağlantılı veriler, özel bir ağ üzerinden gönderiliyormuş gibi görünmektedir. Bu sebepten ortak ağın gerçek alt yapısı çokta önemli değildir. İkincisi ise siteden siteye VPN'dir. Siteden siteye VPN bağlantıları değişik ofisler arasında veya değişik kuruluşlar arasında ortaklaşa bir ağ üzerinden güvenlikli bir şekilde iletişimi sağlayamaz. VPN bağlantısı WAN (Wide Area Network) bağlantısı gibi çalışır. WAN bağlantısı kentler, kıtalar gibi uzun mesafeler arasında iletişimi sağlayabilen ağ türüdür. Ağlar, İnternet üzerinden verileri bir yönlendirici ile başka bir yönlendiriciye ulaştırır. Yönlendiricilere göre VPN bağlantısı, veri bağlantısı olarak vazife görmektedir (İnt.Kyn.33).

Örneğin, Eskişehir'de yaşıyorsunuz ve Paris'te bir VPN hizmetiniz var. Kullanıcı adı ve şifrenizi girip Paris'teki VPN'e bağlanıyorsunuz. O andan itibaren İnternet ile bütün iletişiminiz Eskişehir'den değil; bağlı olduğunuz Paris'teki sunucu üzerinden gerçekleşir. Youtube'a erişmek istediğinizde Paris'teki VPN bilgisayarı Youtube'dan istediğiniz içeriği talep eder. Gelen içeriği de şifreleyerek size; yani Eskişehir'e iletir. Youtube sizi Parisli bir kullanıcı zanneder. Sansür ve fişleme için teknik takip yapan devlet (ya da şirketiniz) sizin sadece Paris'te bir bilgisayarla bağlantı kurup şifreli (içeriğini anlayamadığı) bir şeyler alıp verdiğinizi zanneder. Aslında o bilgisayar üstünden Youtube'a bağlandığınızı bilemediği için sansür de uygulayamaz. Bu şekilde

sadece Parisli (Fransa'da yaşayan) kullanıcılara açık her hizmetlere de erişebilirsiniz. Sonucu tekrar edecek olursak; Eskişehir'den sizin İnternet bağlantınızı takip eden şirketiniz, devletiniz ya da başka bir kurum hattınızı dinlerken sadece Paris'te bir bilgisayarla kriptolu (anlaşılmaz) veri yığınları görür. Ne yaptığınızı, nereye bağlandığınızı bilemez, takip edemez, fişleyemez. Aynı sebeple sizi engelleyemez. Yani devletinizin ya da şirketinizin sansür duvarını da aşmış olursunuz. Ziyaret ettiğiniz site ve hizmetler de (VPN şirketiniz kimlik bilgilerinizi vermediği sürece) gerçek kimliğinize ulaşamaz. Farklı VPN sunucuları / hizmetleri kullanarak saniyeler içinde dünyanın dört bir yanına kendinizi taşıyabilirsiniz (İnt.Kyn.32). VPN kullanmanın dezavantajı ise firmalara göre değişik kullanım ücretlerinin olmasıdır.

4.2.2 DNS Değiştirme Yöntemi

İnternet kullanıcılarının engellenen sitelere erişmek için kullandıkları ve en basit yöntem DNS değiştirme yöntemidir. Bu yöntemde servis sağlayıcımızın bize sunduğu IP yerine farklı bir DNS üzerinden bağlantı sağlanır. DNS bir köprü vazifesi görür ve size sadece erişim imkânı sunar. Devlet sizin kim olduğunuzu ve hangi siteye girdiğinizi rahatlıkla bulabilir (İnt.Kyn.31). İnternet hizmeti aldığımız cep telefonu operatörleri ve evimize fiber ya da ADSL getiren İnternet servis sağlayıcıları, kendi DNS sunucularında yönlendirme yaparlar. Bu sunuculardaki bazı web sitelerinin IP adresleri yasaklı olur ve bu siteleri açmaya kalktığımızda karşımıza "Bu site engellenmiştir" yazısı çıkar. Bu şekilde bizi istediğimiz web sitesi yerine, site engellendi sayfasına yönlendirirler. Ancak, DNS sunucumuzu değiştirip, bu sitelerin IP adreslerini yönlendirme yapmadan doğrudan başka bir sunucuya bağlanarak istediğimiz siteye girebiliriz (İnt.Kyn.31). Şubat 2014 tarihinde 5651 sayılı kanunun 6 ncı madde ç bendinde yapılan düzenlemeyle erişim sağlayıcılar, erişimi engelleme kararı verilen yayınlarla ilgili olarak alternatif erişim yollarını engelleyici tedbirleri almakla yükümlü tutulmuştur.

4.2.3 Proxy Kullanımı

Proxy sunucular devletler tarafından erişim engelleme amacıyla kullanılabileceği gibi

İnternet kullanıcıları tarafından engellemelerin aşılması amacıyla da kullanılabilmektedir (Kaya 2010). Esasında içeriğe Proxy sunucu erişir ve eriştiği içeriği İnternet kullanıcısına aktarır. Proxy sunucu başka bir ülkede yer aldığı için içeriğe engelsiz bir şekilde erişmektedir. Ayrıca, içeriğe ilk elden Proxy sunucu eriştiği için İnternet kullanıcısı kimliğini gizleyebilmektedir. Proxy sunucular, hem engellemeleri aşmak için hem de çeşitli suçlarda aracı olarak kullanılabildikleri için devletlerin sıkı takibine tabidirler (Kaya 2010).

4.2.4 Tarayıcı Tabanlı Çözümler

Kullanılan İnternet tarayıcılarının özel eklentileri ile erişim engellemesi aşılabilmektedir. Örneğin Google Chrome tarayıcısı kullanıyorsanız eğer ZenMate eklentisi size bu konuda çözüm sunacaktır veya Mozilla Firefox kullanıyorsanız AnonymoX eklentisi ile aynı işlevi görebilirsiniz. Bir diğer tarayıcı tabanlı çözüm ise TOR Browser'dır. Windows işletim sistemine sahip kullanıcılar için tasarlanmış olan Tor Browser, İnternet gezintiniz sırasında kişisel bilgilerinizin başkaları tarafından görülmesini engelleyen bir güvenlik aracıdır. TOR tarayıcısını kullandığınız takdirde TOR ağına dahil olursunuz ve İnternete gönderdiğiniz ya da oradan çağırdığınız veriler parçalar halinde şifrelenerek diğer TOR kullanıcılarının bağlantılarının üzerinden gönderilir (İnt.Kyn.31).

4.2.5 Mobil Tabanlı Çözümler

Akıllı telefonların yaygınlaşmasıyla birlikte kullanıcılar artık her türlü İnternet işlemini telefonlar aracılığıyla yapabilmektedir. Ülkemizde en çok kullanılan işletim sistemi Android ve iPhone tarafından kullanılan i-OS'tur. Android işletim sistemi kullanan kullanıcılar arasında en çok tercih edilen uygulama VPN tabanlı HotSpot Shield uygulamasıdır. Kullanıcılar HotSpot Shield sayesinde Amerika sunucuları üzerinden bağlantı alarak engelli sitelere kolaylıkla erişebilmektedir. Android kullanıcılarının çok sık kullandığı diğer bir uygulama TunnelBear uygulamasıdır. TunnelBear uygulaması ile İnternet trafiği yönlendirebilir ve kimlik gizleyerek farklı bir ülkeden giriş yapıyormuş gibi ziyaret etmek istenen sitelere giriş yapabilmektedir. Bunun yanında

bilgisayar ile kurulan diğer uzak sunucular ile aradaki veri akışı şifrelenerek sistemde bulunan tüm verilerin gizliliği korunabilmektedir (İnt.Kyn.31). HotSpot Shield ve TunnelBear, Android kullanıcıları arasında çok yaygınken Onavo Extend, iPhone kullanıcıları arasında daha yaygın kullanılan bir uygulamadır. Bu uygulamayı mobil cihaza yükledikten sonra bütün veri akışı Onavo sunucuları üzerinden şifrelenerek sağlanmakta ve bu şekilde İnternette iz bırakmadan güvenli bir şekilde gezinilebilmektedir (İnt.Kyn.31).

5. TÜRKİYEDE İNTERNET ERİŞİMİNİN ENGELLENMESİ

İnternet erişiminin engellenmesi genel olarak bakıldığında yoğun eleştirilere maruz kalabilir ve hatta sansür olarak değerlendirilebilir. Fakat gerçek hayatta suç olduğu için cezalandırılan bir olgunun sanal ortamda cezasız kalması akıl ve mantık dışıdır. Dolayısıyla devletler vatandaşlarını suç unsuru teşkil eden yayınlardan korumakla görevlidir ve bunun için uluslararası yasaların yetersiz olmasından dolayı ülke bazında yasal düzenlemeler yapması gerekmektedir. (İnt.Kyn.34).

5.1 Yetkili Kurumlar:

5.1.1 Telekomünikasyon İletişim Başkalığı (TİB)

Teknolojik vasıtaların günden güne gelişmesi ve yeni buluşların ortaya çıkması, sosyal yaşantıyı kolaylaştırmasının yanı sıra kötü niyetli kullanılmaya da müsait olduğu için, bu araçların insan haklarına müdahale boyutu yasal düzenlemelerle belli birtakım devlet organlarına bırakılmak durumundadır (Gödekli 2013). Ülkemizde iletişimin denetlenebilmesi, yetkilerin kötüye kullanılmasının önüne geçmek ve dünya standartlarına uygun alınan tedbirlerinin uygulanması ve bütün iletişim denetlenmesinin bir tek merkezden yürütülmesi hedefiyle 5397 sayılı Kanunla Polis Vazife ve Salahiyet Kanunu, 2803 sayılı Jandarma Teşkilat, Görev ve Yetkileri Hakkında Kanunu ve 2937 sayılı Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanunu çerçevesinde yapılan değişiklikler sonrası yasal dayanağına kavuşan TİB kurulmuştur (Avşar Öngören 2010).

Kurumun çalışma usul ve esasları Telekomünikasyon Yoluyla Yapılan iletişimin Tespiti, Dinlenmesi, Sinyal Bilgilerinin Değerlendirilmesi ve Kayda Alınmasına Dair Usul ve Esaslar ile TİB'in Kuruluş, Görevce Yetkileri Hakkında Yönetmelikte (TİB Yönetmeliği) düzenlenmiştir (Avşar Öngören 2010). Başkanlığın kuruluşunun Anayasal dayanağını, 1982 Anayasasının "Haberleşme Hürriyeti" başlıklı 22. maddesi teşkil etmektedir (Gödekli 2013). 22 nci maddeye göre, "Herkes, haberleşme hürriyetine sahiptir. Haberleşmenin gizliliği esastır. Milli güvenlik, kamu düzeni, suç işlenmesinin

önlenmesi, genel sağlık ve genel ahlakın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak usulüne göre verilmiş hâkim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; haberleşme engellenemez ve gizliliğine dokunulamaz. Yetkili merciin kararı yirmi dört saat içinde görevli hâkimin onayına sunulur. Hâkim, kararını kırk sekiz saat içinde açıklar; aksi halde, karar kendiliğinden kalkar. İstisnaların uygulanacağı kamu kurum ve kuruluşları kanunda belirtilir."

TİB'in görevleri şunlardır:

1) TİB kuruluş aşamasında yetkilendirildiği ilgili kanunlara dayanarak telekomünikasyon yoluyla yapılan iletişim faaliyetinin tespit edilmesi, dinlenmesi, sinyal bilgilerinin değerlendirilmesi ve kayıt altına alınmasına yönelik iş ve işlemleri bir tek merkezden yürütmek,

2) 5271 sayılı Kanun kapsamında yapılacak iletişimin tespit edilmesi, dinlenmesi, kayıt altına alınması ve sinyal bilgilerinin değerlendirilmesine yönelik işlemleri bir tek merkezden yürütmek,

3) Yukarıda belirtilen iki madde kapsamındaki taleplerin TİB yönetmeliğine ve diğer konuyla ilgili yasal mevzuata uygunluğunu incelemek ve gerektiği takdirde yetkili makamlara başvurmak,

4) Yine yukarıda yer alan 1 ve 2 nci maddeler gereğince gerçekleştirilen faaliyetler neticesinde ele geçen verileri ve bilgileri ilgisine göre Milli İstihbarat Teşkilatı Müsteşarlığına, Emniyet Genel Müdürlüğüne ve Jandarma Genel Komutanlığına, talep edilmesi durumunda mahkemeye ve Cumhuriyet Başsavcılıklarına ulaştırmak,

5) TİB yönetmeliği kapsamında yapılacak tespit, dinleme, sinyal bilgilerinin değerlendirilmesi ve kayıt altına alınması işlemleri ile 5651 sayılı Kanunla ve diğer yasal mevzuatla verilen görevlerin icrasını olanaklı kılacak her türlü teknik alt yapının,

kamu kurum ve kuruluşları ile kamu görevi yapan kuruluşlar ve işletmeler tarafından kurulmasını sağlamak, sağlatmak, ihtiyaç duyulan alt yapıyı kurmayan işletmelerin cezalandırılması için girişimde bulunmak,

6) TİB faaliyetleriyle ilgili olarak kamu kurum ve kuruluşları, kamu hizmeti veren kuruluşlar ile işletmelerden gelen her türlü bilgi, belge ve kayıtların bilgi güvenliği kıstaslarına uygun şekilde arşivlenmesini sağlamak,

7) Görev sahasına giren konularla alakalı yerel ve uluslararası alanda ortaya çıkan gelişmeleri takip etmek, bu kapsamda uluslararası kurum ve kuruluşlarla işbirliği ve koordinasyonu sağlamak ve ortaya çıkan gelişmelerin TİB hizmetlerine katkı sağlaması için önlemler almak,

8) TİB faaliyetlerinin icrası için yurt içinden ve dışından gerekli olan her türlü malzeme, sistem, yazılım ve donanımı belirleyerek Telekomünikasyon İletişim Başkanına bildirmek,

9) TİB'in yapmış olduğu faaliyetleriyle ilgili olarak Başbakanın talep ettiği bilgileri Başbakana vermek,

10) 5651 sayılı kanun gereğince Ulaştırma Bakanlığı, kolluk kuvvetleri, ilgili kamu kurum ve kuruluşlarla içerik, yer ve erişim sağlayıcılar ve konuyla ilgisi olan sivil toplum kuruluşları arasında koordine kurarak İnternet ortamında yapılan ve 5651 sayılı kanun alanına giren suçları oluşturan içeriğe sahip faaliyet ve yayınları önlemek için çalışmalar yapmak; bu sebeple, gerektiği takdirde, her türlü giderleri kurumca karşılanacak çalışma kurulları oluşturmak,

11) İnternet ortamında yayınlanan içeriklerini takip ederek, 5651 sayılı kanun kapsamına giren suçların oluşması halinde, İnternet ortamında yapılan ilgili yayınlara erişimin engellenmesi şeklinde 5651 sayılı kanunla kendisine verilen tedbirleri almak,

12) İnternet ortamında yayınlanan içeriklerinin takibinin ne seviyede, ne zaman ve ne

şekilde yapılacağını belirlemek,

13) TİB'ce yetkilendirilen işletmeler ile mahalli mülki amirleri tarafından ticari amaçlı toplu kullanım sağlayıcılarına verilecek izin belgelerinde, filtreleme ve engellemede kullanılması gereken sistemlere ve yapılması gereken düzenlemelere yönelik esas ve usulleri belirlemek,

14) İnternet ortamında yayınlanan içeriğin izlenmesi suretiyle, 5651 sayılı kanunun 8 nci maddesinde yer alan katalog suçlar kapsamında olan ve 5237 sayılı Türk Ceza Kanununda yer alan; intihara yönlendirme suçu, çocukların cinsel istismarı suçu, uyuşturucu veya uyarıcı madde kullanılmasını kolaylaştırma suçu, sağlık için tehlikeli madde temin etme suçu, müstehcenlik suçu, fuhuş suçu, kumar oynanması için yer ve imkân sağlama suçları ve 5816 sayılı Atatürk Aleyhine İşlenen Suçlar Hakkında Kanunda yer alan suçların meydana gelmesinin önlemek amacıyla izleme ve bilgi ihbar merkezi dâhil, gerekli görülen her türlü teknik altyapıyı kurmak veya kurdurmak, kurulan bu altyapıyı işletmek veya işletilmesini sağlamak,

15) İnternet ortamında herkese açık olan değişik türdeki servislerde yapılması gereken filtreleme, perdeleme ve izleme esaslarına uygun olarak gerekli donanımın üretilmesi veya yazılım yapılmasına ilişkin asgari kıstasları belirlemek,

16) 14 ncü madde de belirtilen suçların, İnternet ortamında işlenmesini konu alan her çeşit temsili görüntü, yazı veya sesleri içeren yayınların tanıtımı, yurda sokulması, bulundurulması, kiraya verilmesi veya satışının önlenmesi için yetkili ve görevli kolluk kuvvetleri ile soruşturma makamlarına, teknik imkânlar dâhilinde gereken her çeşit yardımı ve koordineyi sağlamak,

17) İnternet Kuruluyla gereken işbirliğini ve koordinasyonu sağlayarak; İnternet Kurulu tarafından izleme, filtreleme ve erişim engelleme yapılacak içeriğe konu olan yayınların tespit edilmesi ve benzer konularda yapılacak görüş ve önerilerle ilgili olarak gerek gördüğü her çeşit tedbir veya kararları almak,

18) 5651 sayılı kanunun 8 inci maddesinde yer alan katalog suçlar ve 7258 sayılı Kanun kapsamında hâkim, mahkeme veya Cumhuriyet Savcısınca kendisine verilen İnternet erişiminin engellenmesi kararlarının uygulamasını sağlamak ve bununla ilgili iş ve işlemleri yürütmek,

19) 5651 sayılı kanunun 8 inci maddesinde yer alan katalog suçları oluşturan yayınların içerik veya yer sağlayıcısının ülke dışında bulunması durumunda veya içerik veya yer sağlayıcısı ülke içinde bulunması halinde bile, içeriğin çocukların cinsel istismarı suçunu ve müstehcenlik suçunu oluşturan İnternet yayınlarına ilişkin olarak re'sen İnternet erişiminin engellenmesi kararı vermek ve bu kararı, ilgili erişim sağlayıcısına bildirmek suretiyle gereğinin en kısa zamanda ve en geç kararın bildirilmesi anından itibaren yirmi dört saat içinde yerine getirilmesi gerektiğini bildirmek,

20) Konusu suç teşkil ettiği için erişim engellenmesi kararı verilen İnternet yayınını yapan kişi veya kişilerin kimliğinin tespit edilmesi halinde Cumhuriyet Başsavcılığına suç duyurusunda bulunmak,

21) Mevcut yasal mevzuatla veya düzenlenecek yeni kanunlarla kendisine verilen diğer görevleri yerine getirmek.

23 Temmuz 2006 tarihinden itibaren iletişimin tespiti, dinlenmesi, kaydedilmesi ve sinyal bilgilerinin değerlendirilmesi işlemlerini yapan tek kurum TİB olup; başka hiçbir kurum veya kuruluş ile gerçek veya tüzel kişilerin bu işlemleri yapma yetkisi bulunmamaktadır (Avşar Öngören 2010). TİB Yönetmeliği, Emniyet Genel Müdürlüğü, Jandarma Genel Komutanlığı ve Milli İstihbarat Teşkilatı Müsteşarlığı'nın mevzuat kapsamındaki faaliyetleri açısından teftiş olanağı getirerek denetleyici organları sıralamıştır. Buna göre, her üç kamu kuruluşunun telekomünikasyon yoluyla yapılan iletişimi dinleme ve tespit etme faaliyetleri, sıralı kurum amirleri tarafından gerçekleştirilir. Bunun yanında üç kurumun kendi denetçileri de yönetmelikte sırasıyla Emniyet Genel Müdürlüğü teftiş elemanları, Jandarma Genel Komutanlığı teftiş elemanları ve MİT Müsteşarlığı teftiş elamanları olarak belirtilmiştir (Gödekli 2013).

Başkanlığın, Yönetmelikte yer alan faaliyetlerle ilgili denetimi, Başbakanın özel olarak yetkilendireceği kişi veya komisyon tarafından yapılır (Avşar Öngören 2010). Başbakanın görev verdiği kişi veya komisyonun Emniyet Genel Müdürlüğü, Jandarma Genel Komutanlığı ve MİT Müsteşarlığı'nın Yönetmelikte belirtilen faaliyetlerini denetleme olanağına da sahip olduğu vurgulanmıştır (Gödekli 2013). Ancak 5397 sayılı yasanın Anayasaya aykırılık iddiasıyla Anayasa Mahkemesi önüne götürülmesi ve yüksek mahkemece hukuk devleti ilkesine aykırı olduğu gerekçesiyle iptal edilmiştir (İnt.Kyn.35). Bu kararla birlikte, Başkanlığın idari açıdan denetlenmesine ilişkin yasal bir mevzuat hükmü ve hiçbir hukuki dayanak kalmamış, adı geçen diğer kurumların faaliyetlerinin denetimi konusunda ise başbakanın tek başına kişi veya komisyon görevlendirme yetkileri elinden alınmıştır (Gödekli 2013).

5.1.2 Erişim Sağlayıcılar Birliği

Şubat 2014 tarihiyle 5651 sayılı Kanun'a eklenen 6/A maddesinde Erişim Sağlayıcıları Birliğinin amacı, niteliği tanımlanmıştır (Gönenç 2014). Erişim Sağlayıcılar Birliğinin çalışma şekil ve usulleri hazırlanacak olan Birlik Tüzüğüyle belinlenecek olup, Erişim Sağlayıcılar Birliğine 5809 sayılı Elektronik Haberleşme Kanunu kapsamında yetki verilen bütün İnternet servis sağlayıcılarıyla İnternet erişim hizmeti veren işletmelerin üye olması gerektiği, 5651 sayılı Kanunla düzenlenmiş bulunmaktadır. Üye olması gereklerden oluşması gereken Erişim Sağlayıcılar Birliğinin yönetimi de yine bu işletmelerin oluşturacağı Genel Kurul ve Yönetim Kurulu kanalıyla gerçekleştirilecektir (İnt.Kyn.36).

5651 sayılı kanun 8.maddede belirtilen katalog suçlar haricinde bir hak ihlali doğuran içeriğe erişimin engellenmesi kararlarını artık merkezi Ankara olan Erişim Sağlayıcıları Birliği uygulayacaktır (Gönenç 2014). Erişim Sağlayıcılar Birliği, Sulh Ceza Mahkemelerinin göndereceği gerçek ve tüzel kişiler ile kurum ve kuruluşlarla alakalı İnternet ortamında yapılan kişilik haklarının ihlaliyle ilgili İnternet erişim engellenmesi kararlarını uygulamaktan sorumludur (İnt.Kyn.37).

Erişim engellenmesi kararı verildiğinde bu karar uygulanması için birliğe

gönderilecektir. Bu sayede tüm erişim sağlayıcılarına tebliğ edilmiş sayılacak bir tebliğ kolaylığı sağlanmıştır. Bu, kararın uygulanması açısından zaman kazandıracaktır. Fakat bu kararların uygulanması için gerekli her türlü donanım ve yazılım erişim sağlayıcıların kendileri tarafından sağlanacaktır, bu da gerekli ama ek bir yükümlülüktür (Gönenç 2014). Birlik kendisine gönderilen kararın hukuka aykırı olduğunu düşünüyorsa karara itiraz edebilecektir (5651 S.K.). Bu konudaki en büyük mükellefiyet ise, birliğe üye olmanın zorunlu ve ücretli olmasıdır. Üye olamayan erişim sağlayıcı kesinlikle faaliyette bulunamayacaktır. Bu mükellefiyet erişim sağlayıcılar açısından rekabeti ve ekonomik dengeyi sarsabilecek, küçük çaplı şirketler açısından piyasadan çekilmeye sebep olabilecektir. Ayrıca erişim sağlayıcılar üzerindeki denetim kolaylaşacaktır. Gerekli donanımı sağlama koşulunun ve birliğe üyeliğin ücretli olmasının getirdiği ekonomik külfetin ise kullanıcıya yansıtılmaması gibi bir ihtimal çok düşüktür (Gönenç 2014).

5.2 Yükümlülükler

5.2.1 Kamuyu Bilgilendirme Yükümlülüğü

5651 sayılı kanunun 3 ncü maddesinde İçerik, yer ve erişim sağlayıcıları için, yönetmelikçe belirlenecek esas ve usuller kapsamında kendilerini tanıtmak için gereken bilgileri kendilerine ait İnternet sayfasında kullanıcıların istediklerinde ulaşabileceği şekilde ve her zaman güncel olarak bulundurulmasından sorumludur (5651 S.K. 2014) denilmektedir. Kanuna Şubat 2014 düzenlemesiyle İçerik, yer ve erişim sağlayıcıları için, faaliyetlerini yurt içinden veya yurt dışından yürütmekte olanlarla, İnternet ortamlarındaki iletişim kurma araçları, alan adı, IP adresi ve benzeri kaynaklarla elde edilen bilgiler üzerinden elektronik postayla ya da başka iletişim araçlarıyla bildirim yapılabilir şeklinde düzenlenmiştir (5651 S.K. 2014).

Telekomünikasyon Kurumu Tarafından Erişim Sağlayıcılara ve Yer Sağlayıcılara Faaliyet Belgesi Verilmesine İlişkin Usul ve Esaslar Hakkında Yönetmeliğin Madde:14/1'de kamuyu bilgilendirme yükümlülüğü içeriği olarak;

1. Gerçek kişilere verilecek faaliyet belgesiyle ilgili olarak; gerçek kişilerin adı ve soyadı, tüzel kişilerin ise unvanı ve sorumlu kişiler, vergi kimlik numarası veya ticaret sicil numarası,

b. Yerleşim yeri olarak, tüzel kişi ise faaliyet göstereceği merkezin bulunduğu yer,

c. E-posta adresi ve iletişim için telefon numarası,

d. Sunduğu hizmet bir makamın izniyle ya da denetimine ilişkin bir faaliyet kapsamında yapılıyorsa yetkili denetim makamına ilişkin bilgiler kullanılıcıların ulaşabileceği şekilde yayımlanmalıdır şeklinde düzenlenmiştir (İnt.Kyn.38).

5.2.2 İçerik Sağlayıcının Yükümlülüğü

5651 sayılı kanunun 4. maddesinin 1 ve 2. bendinde İçerik Sağlayıcının sorumlulukları ile ilgili olarak İçerik sağlayıcılar İnternet sayfalarında başkalarının kullanıma sunduğu bütün içeriklerinden sorumludur, eğer başkası adına bağlantı sağlıyor ise sağladığı bağlantının içeriğinden dolayı sorumlu değildir, fakat sunuş biçiminden dolayı, sağlamış olduğu bağlantıyı sahiplendiği ve kullanıcıların söz konusu içeriğe ulaşmasını hedeflediği açık olarak belliyse genel hükümlere göre sorumludur şeklinde düzenlenmiştir (5651 S.K. 2014). Şubat 2014'te yapılan düzenleme ile kanunun 4. maddesine yapılan eklemede İçerik sağlayıcının, TİB'in 5651 sayılı kanun ve konuyla ilgili kanunlar tarafından verilen görevlerinin icrası kapsamında; talep edeceği bilgileri talep ettiği şekilde TİB'e teslim edeceği ve TİB tarafından kendisine bildirilen tedbirleri alacağı hususu eklenmiştir (5651 S.K. 2014).

İçerik sağlayıcı, sulh ceza hâkiminin verdiği içeriğin yayından çıkartılması ve hazırlanan cevabı kullanıcıların ana sayfadan doğrudan ulaşabileceği şekilde, tekzip başlığı altında yayınlanması kararını uygulamak zorundadır (Durnagöl 2011).

İçerik sağlayıcı ile ilgili olarak kanunda "İnternet ortamı üzerinden kullanıcılara sunulan her türlü bilgi veya veriyi üreten, değiştiren ve sağlayan gerçek veya tüzel kişilerdir"

(5651 S.K.2014) şeklinde tanımlama yapılmıştır. Web 2.0 teknolojisinin kullanılmaya başlamasıyla beraber kullanıcılar da yaptıkları yorumlar nedeniyle artık birer içerik sağlayıcı konumundadır. Peki suç teşkil eden bir içerikten dolayı içeriğe yorumda bulunan kişiler de suça ortak olmuş mudur? Bu konuyla ilgili olarak karşılaşılacak başka bir önemli örnek de arama motorlarıyla alakalıdır. İçerik sağlayıcıların içeriği hukuka aykırı bağlantılarını ücret karşılığında sözleşmesi gereği üst sıralarda görünmesini sağlayan, bu bağlantıya ulaşılmasına aracılık eden arama motoru yöneticileri bu konudan dolayı sorumlu mudur? Bu tür sorunlarla listeyi uzatmak mümkündür (Dülger 2013).

5.2.3 Yer Sağlayıcının Yükümlülüğü

5651 sayılı kanunun 5. maddesinde yer sağlayıcıların sorumluluğu ile ilgili olarak "Yer sağlayıcı, yer sağladığı içeriği kontrol etmek veya hukuka aykırı bir faaliyetin söz konusu olup olmadığını araştırmakla yükümlü değildir." (5651 S.K. 2014) denmektedir. Yer sağlayıcı, sulh ceza hâkiminin verdiği içeriğin yayından çıkartılması ve hazırlanan cevabı kullanıcıların ana sayfadan doğrudan ulaşabileceği şekilde, tekzip başlığı altında yayınlanması kararını uygulamak zorundadır (Durnagöl 2011).

Şubat 2014'te 5651 sayılı kanununda yapılan düzenlemeyle yer sağlayıcılara ilgili yer sağladığı hukuka aykırı içeriğin 5651 sayılı kanunun 8. ve 9. maddelerine göre haber edilmesi durumunda yayından çıkarma sorumluluğu getirilmiştir. Aynı düzenleme kapsamında yer sağlayıcıların, sağlamış olduğu hizmetlere alakalı İnternet trafik bilgilerini bir yıldan az ve iki yıldan fazla olmayacak şekilde saklamakla ve sakladığı bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini korumakla yükümlüdür (5651 S.K. 2014). Yer sağlayıcıların, TİB'in 5651 sayılı kanun ve konuyla ilgili kanunlar tarafından verilen görevlerinin icrası kapsamında; talep edeceği bilgileri talep ettiği şekilde Başkanlığa teslim edeceği ve Başkanlıkça kendisine bildirilen tedbirleri alacağı kanuna eklenmiştir (5651 S.K. 2014).

5.2.4 Erişim Sağlayıcının Yükümlülüğü

5651 sayılı Kanunun 6. maddesine göre Erişim Sağlayıcılar, herhangi bir İnternet kullanıcısının yayınlamış olduğu hukuka aykırı içerikten dolayı sorumlu değildir. 5651 sayılı kanun hükümlerine uygun olarak hukuka aykırı içeriğin haberdar edilmesi durumunda İnternet erişimi engellemekten dolayı sorumludur. Erişim Sağlayıcılar sağladığı hizmetlerle alakalı olarak, TİB yönetmeliğinde belirtilen İnternet trafik bilgilerini altı aydan az ve iki yıldan fazla olmamak üzere ilgili yönetmelikle belirlenen süre kadar saklamakla ve bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini korumakla yükümlü tutulmuşlardır (5651 S.K. 2014).

Şubat 2014'te yapılan düzenlemeyle 5651 sayılı kanuna, İnternet erişim engellemesi kararı verilen İnternet sitesi ve İnternet yayınları ile alakalı alternatif İnternet erişim yollarını engellemek için tedbirler almak için sorumlu tutulmuşlardır (5651 S.K. 2014). TİB tarafından istenilen bilgileri TİB'e ulaştırmakla ve TİB tarafından kendilerine tevdi edilen tedbirleri almakla da yükümlüdürler (5651 S.K. 2014).

5651 sayılı kanun Yer Sağlayıcılarda olduğu gibi Erişim Sağlayıcılar için de erişim sağladıkları içerikle alakalı olarak içeriğin hukuka aykırı olup olmadığını kontrol etmekle ilgili bir sorumluluk yüklememiştir (5651 S.K. 2014).

5.2.5 Toplu Kullanım Sağlayıcının Yükümlülüğü

TİB'in 1/11/2007 tarihli Yönetmeliğine göre, İnternet toplu kullanım hizmeti veren kurum ve kuruluşların konusu suç teşkil eden yayınlara erişilmemesi için gerekli tedbirleri almak ve iç IP dağıtım loglarını elektronik ortamlarında sistemlerine kaydetme sorumluluğu vardır (İnt.Kyn.38). Toplu kullanım sağlayıcılar çocuklar dâhil toplumun her kesimi tarafından İnternete erişim için yoğun olarak kullanıldığından İnternet ortamında suçla mücadele alanında önlemler almayı zorunlu kılmaktadır. Avrupa Konseyi 1999/246 ve 2005/854 sayılı kararlarıyla konseye üye ülkeleri İnternetin doğru ve güvenli bir biçimde kullanılmasının sağlanması amacı ile filtreleme ve bloke etmek için gerekli programları geliştirmeye ve aynı amaçla eğitim ve tanıtım

faaliyetlerini yaygınlaştırmaya davet etmektedir (Kaya 2010).

5.2.6 Ticari Kullanım Sağlayıcının Yükümlülüğü

TİB'in 1/11/2007 tarihli Yönetmeliğine göre, Ticari amaçlı İnternet toplu kullanım sağlayıcılarının sorumlulukları; Mahalli Mülki idare amirlerinden izin belgesi almak, konusu suç teşkil eden içeriklere ilişkin erişim önleyici tedbirler almak, TİB tarafından onaylanan İnternet içerik filtreleme yazılımlarını kullanmak, erişim sağlayıcılardan sabit IP adresi almak ve kullanmak, iç IP dağıtım loglarını kendi elektronik ortamlarında saklamak ve Başkanlıkça verilen yazılım ile kaydedilen bilgileri ve bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini teyit eden değeri kendi sistemlerine günlük olarak kaydetmek ve bu verileri bir yıl süre ile saklamaktır (İnt.Kyn.38).

5.3 5651 Sayılı Kanun Kapsamında İnternet Erişiminin Engellenmesi

23.05.2007 tarihli Resmi Gazetede yayımlanan 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun Türkiye'de İnternet erişiminin engellenmesi ile ilgili yapılan ilk yasal düzenlemedir. 26.02.2014 tarihli torba yasayla 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun içeriğinde çeşitli düzenlemeler yapılmış ve kanun en son halini almıştır.

5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun içeriği incelendiği zaman 8 nci maddede belirtilen katalog suçlar sebebiyle ve 9 ncu maddede yer alan kişilik haklarının ihlali sebebiyle, 9/A maddesinde yer alan özel hayatın gizliliğinin ihlali sebebiyle TİB tarafından tedbir amaçlı İnternet erişim engellemesi yapılmaktadır. 5651 sayılı kanun haricinde 6362 sayılı Kanunun 109'uncu maddesinde yer alan suçlar, 7258 sayılı Futbol ve Diğer Spor Müsabakalarında Bahis ve Şans Oyunları Düzenlenmesi Hakkında Kanunda yer alan suçlar, 4733 sayılı Kanunun 8'inci maddesinin beşinci fıkrasının (k) bendinde yer alan ürünlerin İnternet ortamında satışının yapılması ve 1262

sayılı Kanunun 18'inci maddesinde yer alan ürünlerin İnternet ortamında satışının yapılması hallerinde ilgili mercilerce erişim engelleme kararı verilebilmektedir Ayrıca adli suça konu olan web sitelerinin İnternet erişimi mahkeme kararıyla engellenmektedir.

5.3.1. 5651 Sayılı Kanunun 8. Maddesinde Yer Alan Katalog Suçlar Kapsamında İnternet Erişiminin Engellenmesi

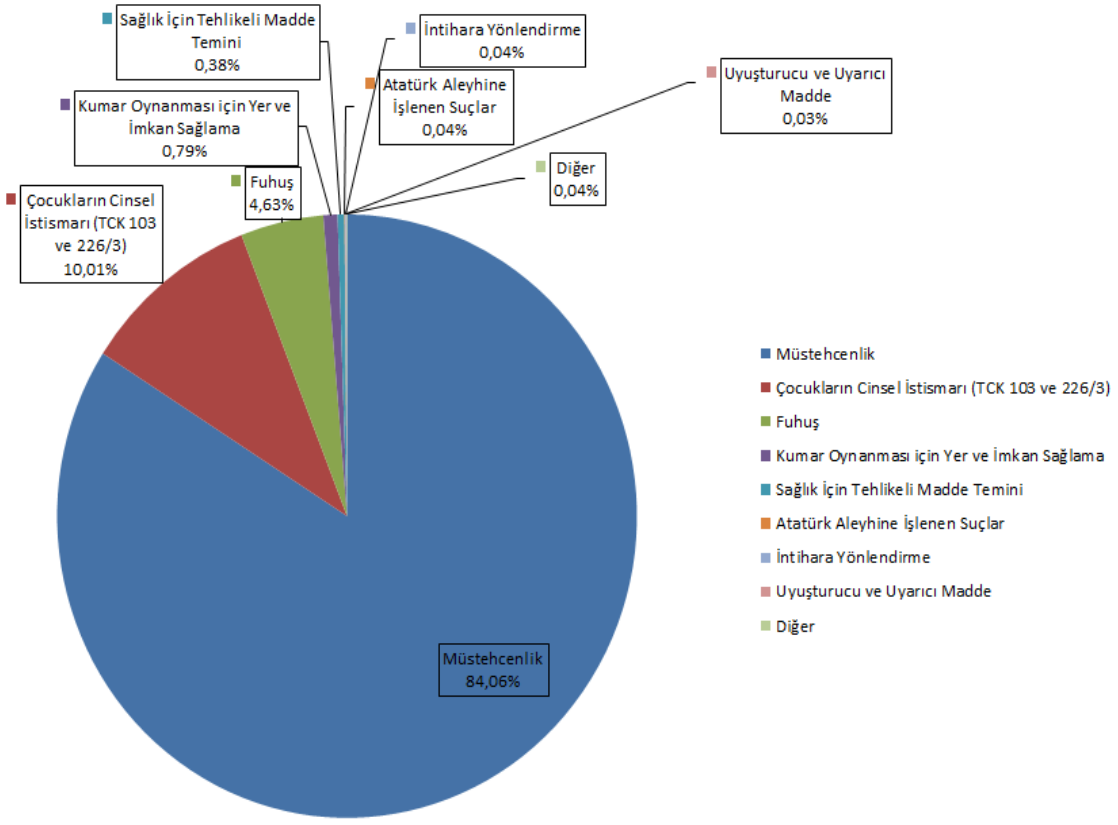
İnternet erişimin engellemeyle ilgili karar verilebilecek suçlar, 5651 sayılı kanunun 8. maddesinde ki katalog suçlar, 9 ncu maddesinde ve Şubat 2014'te yapılan düzenlemeyle kanuna eklenen 9/A maddesinde belirtilmiştir (5651 S.K.). İnternet erişim engelleme kararı verilen bu suçlardan Atatürk'ün hatırasına hakaret ve sövme suçu 5816 sayılı kanunda, diğer suçlar ise TCK'da düzenlenmiştir. Belirtilen bu suçlar haricinde 5651 sayılı kanun kapsamında İnternet erişimi engelleme kararı verilemeyecektir.

5651 sayılı kanunun 8 nci maddesinde yer alan katalog suçlar kapsamında İçerik veya yer sağlayıcı yurtdışında bulunuyorsa TİB, hâkim veya savcı kararına gerek duymadan kendiliğinden İnternet erişim engelleme kararı verebilmektedir. Barındırma hizmetini yurt dışından yürüten bir yer sağlayıcıdan almak, bir nevi mahkeme kararı olmadan İnternet sitesinin TİB tarafından erişme kapatılması için bir gerekçe sunmak anlamına gelmektedir (İnt.Kyn.34). İnternet erişimi engelleme kararının TİB tarafından alınabilmesi, içerik veya yer sağlayıcıdan herhangi birinin yurt dışında olması yeterli görülmektedir. Dolayısıyla içerik veya yer sağlayıcılardan birinin yurt içinde bulunması halinde TİB tarafından İnternet erişimi engelleme kararı alınabileceği bilinmelidir (5651 S.K.).

İçerik ve Yer Sağlayıcı Yurtiçinde Bulunması durumunda çocukların cinsel istismarı veya müstehcenlik suçlarının işlendiğine dair yeterli suç şüphesi bulunuyorsa, içerik veya yer sağlayıcının yerine bakılmaksızın ve hâkim, mahkeme veya cumhuriyet savcısının kararı olmadan TİB İnternet erişimi engelleme kararı verebilmektedir (İnt.Kyn.34). TİB yönetmeliği, kanunda bulunmamasına rağmen 14. maddesinde içerik veya yer sağlayıcının yurt içinde bulunması halinde TİB tarafından verilecek İnternet

erişimi engelleme kararlarına bir sınırlama getirmiştir. TİB tarafından engelleme yapılan bu hallerde engelleme kararını yirmi dört saat içinde hâkim onayına tâbi tutulması gerekmektedir. Hâkim, kararın kendisine sunulması anından itibaren yirmi dört saat içinde onay vermez ise, İnternet erişimi engelleme kararı TİB tarafından kendiliğinden kaldırılacaktır (İnt.Kyn.34).

5651 sayılı Kanunda sayılan katalog suçlar kapsamında, TİB tarafından idari tedbir olarak uygulanan erişimin engellenmesi tedbirlerinin suç türlerine göre oransal dağılımı:



Şekil 5.1 15 Eylül 2014 tarihi itibariyle TİB tarafından re'sen aktif olarak engellenen kararlar (İnt.Kyn.74).

5.3.1.1 İntihara Yönlendirme

İnternetin kolay ulaşılabilirliği ve giderek yaygınlaşması, ulaşılan bilgiler ve yayınların güvenilir olup olmadığının sorgulanmasını gündeme getirmektedir. Sağlık alanı için bu konu özellikle önemlidir. Çünkü İnternet ulaşımına sahip birçok kişinin sağlık sorunları ile ilgili olarak öncelikle İnternete başvuruyor olduğuna ilişkin giderek artan sayıda

yayın yapılmaktadır. İnternette kimliğin kolayca gizlenebilmesi, intiharın kültürel ve toplumsal olarak kabul gören bir davranış olmaması nedeniyle intihar konusunda İnterneti çekici hale getirmektedir (Sakarya *et al.* 2012). İntihara yönlendirdiği şeklinde yeterli şüphe bulunan İnternet siteleri TİB tarafından erişime engellenmektedir. İntihara yönlendirme suçu Türk Ceza Kanunu Madde-84'te cezalarıyla ele alınmıştır. 15 Eylül 2014 tarihi itibariyle TİB tarafından re'sen aktif olarak engellenen siteler içerisindeki intihara yönlendirme suçu oranı %0,04'tür (İnt.Kyn.74).

5.3.1.2 Çocukların Cinsel İstismarı

Avrupa Konseyinin Siber Suçlar Sözleşmesinde çocuk pornografisi suçunu şu şekildedir. "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 materyal" olarak tanımlanmıştır. Tanım kapsamında geçen küçük tabirinden kast edilmek istenen 18 yaşının altındaki herkestir. Taraf devletler buna karşın, 16 yaşından az olmamak şartıyla daha küçük bir yaş sınırı belirleyebilmektedir (Tulum 2006). Çocukların cinsel istismarına yönelik yayın yaptığı hakkında yeterli şüphe bulunan İnternet siteleri TİB tarafından erişime engellenmektedir.. Türk Ceza Kanun Madde-103'te Çocukların Cinsel İstismarı ile ilgili cezai düzenlemeler ele alınmıştır. 15 Eylül 2014 tarihi itibariyle TİB tarafından re'sen aktif olarak engellenen siteler içerisindeki çocukların cinsel istismarı suçu oranı %10,01'dir (İnt.Kyn.74).

5.3.1.3. Uyuşturucu ve Uyarıcı Madde Kullanımını Kolaylaştırma

5237 Sayılı Türk Ceza Kanununun 190. maddesi; uyuşturucu veya uyarıcı madde kullanılmasını kolaylaştırma başlığı altında düzenlenmiştir. 765 Sayılı Eski Türk Ceza Kanun'undaki düzenlemeden farklı olarak ayrı bir suç şeklinde tanımlanmış, artırım nedeni olarak değil de, doğrudan ceza verilen eylem olarak nitelendirilmiştir. Yine suçun yapısı geniş bir şekilde ele alınmıştır. Uyuşturucu veya uyarıcı madde kullanılmasını kolaylaştırmak için, özel yer, donanım veya malzeme sağlayan, kullananların yakalanmamaları için önlemler alan, kullanma metotları hususunda

başkalarına bilgi veren kişi veya kişilerin hapis cezasıyla cezalandırılacağı hükmü yer almaktadır. Aynı kanunda uyuşturucu veya uyarıcı madde kullanılmasını alenen özendiren veya bu nitelikte yayınlar yapan kişi ya da kişilerinde hapis cezası ile cezalandırılacağı belirtilmiştir. Suçun nitelikli hali olarak ise, tanımlanan suçların tabip, diş tabibi, eczacı, kimyager, veteriner, sağlık memuru, laborant, ebe, hemşire, diş teknisyeni, hastabakıcı, sağlık hizmeti veren, kimyacılıkla veya ecza ticareti ile iştigal eden kişi tarafından işlenmesi durumudur (Özmen 2009). Suç eğer İnternet ortamından işlenir ise ilgili site İnternet erişimine engellenmektedir. 15 Eylül 2014 tarihi itibariyle TİB tarafından re'sen aktif olarak engellenen siteler içerisindeki uyuşturucu ve uyarıcı madde kullanımını kolaylaştırma suçu oranı %0,03'tür (İnt.Kyn.74).

5.3.1.4. Sağlık İçin Tehlikeli Madde Temini

İnternet sitesi aracılığı ile, e-mail alıp verme yoluyla, chat yaparak, web sayfalarında tanıtım, pazarlama ve sipariş yöntemlerini kullanarak ya da İnternet üzerindeki sesli ve görsel iletişim metotları kullanılarak sağlık için tehlike oluşturabilecek maddelerin, nerelerden alınabileceği, ticaretinin yapılması, yönetilmesi ve planlanmasıdır (Tulum 2006). Türk Ceza Kanunu Madde-194'te suçun cezası belirtilmiştir. Suçun oluşması durumunda mahkeme kararı ile ilgili İnternet sitesi erişime engellenmektedir. 15 Eylül 2014 tarihi itibariyle TİB tarafından re'sen aktif olarak engellenen siteler içerisindeki sağlık için tehlikeli madde temini suçu oranı %0,58'tir (İnt.Kyn.74).

5.3.1.5. Müstehcenlik

Müstehcenlik tabirinin kökeni Arapça'daki hücnet kelimesinden türemiş ve "açık saçık, edepsizce olan, çirkin ve uygunsuz" anlamına gelmektedir (Beyaznar ve Karaca 2010). Müstehcenlik kavramının zamana, kişilere ve yere bağlı olarak değişen bir kavram olduğu ve müstehcenlik anlayışının bir toplumdan diğer bir topluma göre değiştiği gibi, aynı toplum içinde de kültürel değerlere bağlı olarak zaman içerisinde türlü değişikliklere uğradığı kabul edilmektedir. Müstehcenlik ayrıca "duygular açısından tiksindirici, nefret uyandıran, pis, açık-seçik, iğrendirici ve hoş olmayan şeyler" şeklinde de tanımlanmaktadır (Kaya 2010).

Müstehcenlik erotizm ve pornografi olmak üzere ikiye ayrılmaktadır. Müstehcenliğin tanımı ne kadar muğlâk ise, erotizm ve pornografinin de tanımı aynı derece muğlâktır (Kaya 2010). Erotizm şiddet içermeyen, aşağılayıcı olmayan ve rızaya dayalı cinsel aktivitelerin sözsel ya da görsel temsili şeklinde tanımlanmaktadır (Dülger 2013). Pornografi ise cinsel organların uyarılmış biçimleriyle dile getirilmesi ya da gösterilmesi olarak tanımlanmaktır. Pornografinin temel amacının salt cinsel uyarılmayı sağlamak olduğu kabul edilmektedir (Kaya 2010).

Müstehcenliğe devletin müdahalesinin gerekli olup olmadığı hususunun lehinde ve aleyhinde farklı görüşler bulunmaktadır. Aleyhe olan görüşlere ilk olarak; müstehcenliğin ahlak dışı olması nedeniyle toplumun kendi ahlak düzeyinin korunması için egemen ahlak değerlerine uymayan içeriğin sınırlandırılması gereği öne sürülmüştür. İkinci olarak; müstehcenliğin kişileri bazı toplum dışı davranışlara sürüklemesi iddiasıyla yapılan müdahale meşru gösterilmeye çalışılmıştır (Kaya 2010). Son olarak; müstehcenliğin yasaklanmasının çevresel nedenlerle isabetli olduğu ileri sürülmüştür. Lehe olan görüşlerde ise; müstehcenliğin bireyin iç dünyasına ait bir konu olduğu için bu alanda herhangi bir devlet müdahalesinin olmaması gerektiği karşı tez olarak belirtilmektedir. Bu görüş, nihayetinde müstehcen içeriğin kullanılmasının ya gizli ya da başkalarına zarar vermeden gerçekleştirilmesi sebebiyle devletin müdahaleyi haklı kılacak bir menfaatinin olmadığı savıyla desteklenmektedir. Bir başka deyişle; devletin hukuk sistemi aracılığıyla belirli bir ahlak anlayışını zorlamaması gerektiği düşünülmektedir (Dülger 2013).

Müstehcen yayın yaptığı hususunda yeterli şüphe bulunan İnternet siteleri TİB tarafından erişime engellenmektedir. Suçun cezai yaptırımları Türk Ceza Kanunu Madde-226'da düzenlenmiştir. 15 Eylül 2014 tarihi itibariyle TİB tarafından re'sen aktif olarak engellenen siteler içerisindeki müstehcenlik suçu oranı %84,06'dır (İnt.Kyn.74).

5.3.1.6 Fuhuş

Fuhuş, etimolojik anlamı çerçevesinde; insan bedeninin her türlü müstehcen ticareti olarak tanımlanabilir. Flexner'e göre fuhuş üç unsurdan oluşur. Bunları; ticaret (trafic),

düzensiz veya rastgele cinsel ilişki (la promiscuité) ve duygusal ilgisizlik (indifférence émotienelle) olarak adlandırmak olanaklıdır (Dursun 2011). Türkiye fuhuşun önlenmesine ilişkin çeşitli uluslararası sözleşmeye taraftır. Bu sözleşmelerden, 4 Mayıs 1910 tarihinde Paris'te imzalanan Beyaz Kadın Ticaretinin Zecren Men'ine Dair Milletlerarası Sözleşme ile 30 Eylül 1921 tarihli Kadın ve Çocuk Ticaretinin Men ve Zecrine Dair Beynelmilel Cenevre Mukavelesine Lozan Anlaşmasını kabul etmekle taraf olmuştur. 1910 tarihli sözleşme bir kişinin ihtiraslarını tatmin etmek amacıyla, rızası olsa dahi bir kadın veya küçük bir kızın fuhuş için hizmetlerinin taahhüt edilmesini, bu amaçla götürülmesini veya sevk edilmesini suçun kurucu unsurları farklı ülkelerde işlenmiş olsa da cezalandırmaktadır. 1921 tarihli sözleşme ise devletleri hangi cinsiyetten olursa olsun, çocuk ticareti yapan kişilerin tespiti ve cezalandırılması için gerekli tedbirleri alma hususunda yükümlü kılmıştır (Kaya 2010).

5651 sayılı kanun ailenin ve gençliğin korunması amacına uygun olarak kişilerin ve özellikle çocukların fuhşa teşvik edilmesini suç kabul eden 5237 sayılı Türk Ceza Kanununun 227. maddesini bir erişim engelleme sebebi olarak kabul etmiştir. 15 Eylül 2014 tarihi itibariyle TİB tarafından re'sen aktif olarak engellenen siteler içerisindeki fuhuş suçu oranı %4,63'tür (İnt.Kyn.74).

5.3.1.7 Kumar Oynanması İçin Yer Ve İmkân Sağlama

Kumar oynanması için yer ve imkân sağlama suçu, Türk Ceza Kanununun 228. maddesinde, genel ahlaka karşı suçlar başlıklı bölümde düzenleme altına alınmıştır. Kanun koyucu bu suç tipiyle, kumarın toplumda denetimsiz olarak yaygınlaşmasının önüne geçmek istemiştir. Suçun oluşabilmesi için yer ve imkân sağlama seklindeki unsur hareketlerin her ikisinin de birlikte gerçekleştirilmesi gereklidir. Bu hareketlerden sadece birisinin gerçekleştirilmesi durumunda suç oluşmayacaktır. Bunun dışında manevi unsur bakımından ise yer ve imkân sağlamanın kumar oynanmasına yönelik olması gereklidir. Bu nedenle söz konusu suç sadece bu şekilde ortaya çıkan özel kastla işlenebilir (Karakeyha 2013).

5651 sayılı kanun, 5237 sayılı Türk Ceza Kanununun 228. maddesinde yer alan kumar

oynanması için yer ve imkân sağlama suçunun İnternet ortamında yapılan yayınlarla oluşturduğu yönünde şüphe bulunması durumunda erişim engellenmesi kararı verilebilmesini kabul etmiştir (Kaya 2010). 15 Eylül 2014 tarihi itibariyle TİB tarafından re'sen aktif olarak engellenen siteler içerisindeki kumar oynanması için yer ve imkân sağlama suçu oranı %0,79'dur (İnt.Kyn.74).

5.3.1.8 5816 Sayılı Atatürk Aleyhine İşlenen Suçlar Hakkında Kanunda Yer Alan Suçlar

5816 sayılı Atatürk Aleyhine İşlenen Suçlar Hakkında Kanun'da yer alan suçların İnternet ortamında yapılan yayınlarla oluştuğu yönünde şüphe bulunması durumunda erişim engellenmesi kararı verilebilecektir. 5816 sayılı kanunda iki farklı suç yer almaktadır. Birinci suç, Atatürk'ün hatırasına alenen hakaret edilmesi veya sövülmesi suçudur. İkinci suç ise temsil eden heykel, büst veya abidelerin veya Atatürk'ün kabrinin tahrip edilmesi, kırılması, bozulması veya kirletilmesi suçudur. Kanun söz konusu suçların iki veya daha fazla kişi tarafından toplu olarak, aleni, umuma açık yerlerde veya basın vasıtasıyla işlenmesini ağırlaştırıcı neden olarak kabul etmiştir (Kaya 2010).

Bu suç bağlamında 5651 sayılı yasa yürürlüğe girdikten sonraki ilk erişim engelleme kararı Ankara 11. Sulh Ceza Mahkemesi tarafından verilmiştir. Bunun dışında da pek çok mahkeme tarafından benzer gerekçelerle Youtube web sitesine erişimin engellenmesi kararı verilmiştir. Söz konusu kararlar farklı zamanlarda kaldırılmış; ancak söz konusu site uzun süre erişime kapalı tutularak, dünya gündeminde dahi yer almıştır. Bu bağlamda Youtube'a erişimin engellenmesi AB'nin Türkiye hakkında yayınladığı 2008 ilerleme raporunda eleştiri konusu yapılmıştır. Buna rağmen, erişim engellemenin uzun süre kaldırılmamasının esas sebebinin yayıncı şirketin gereken ve beklenen alakayı göstermemesi olduğu ifade edilmiştir (Dülger 2013).
15 Eylül 2014 tarihi itibariyle TİB tarafından re'sen aktif olarak engellenen siteler içerisindeki Atatürk aleyhine işlenen suçlar oranı %0,04'tür (İnt.Kyn.74).

5.3.2 5651 Sayılı Kanunun 9. Maddesinde Yer Alan Kişilik Haklarının İhlali Sebebiyle İnternet Erişiminin Engellenmesi

5651 sayılı kanunun 9. maddesince, İnternet ortamında yapılan yayın içeriği sebebiyle, gerçek ve tüzel kişilerle kurum ve kuruluşlar, kişilik haklarının ihlal edildiğini gerekçe göstererek içerik sağlayıcısına, içerik sağlayıcısına ulaşılamaması durumunda yer sağlayıcısına başvurmak suretiyle ilgili içeriğin yayından çıkarılmasını talep edebilirler (İnt.Kyn.39). İnternet ortamında yapılan yayın içeriği sebebiyle kişilik haklarının ihlal edildiği iddiasında bulunan kişilerin talepleri, içerik ve/veya yer sağlayıcısınca en geç yirmi dört saat içinde cevaplandırılması gerekmektedir. İçerik ve/veya yer sağlayıcısından olumlu cevap veya hiç cevap alamayan gerçek veya tüzel kişiler içeriğin kişilik haklarını ihlal ettiği gerekçesiyle mahkemeye başvurup ilgili içeriğin yayından çıkarılmasını isteyebilirler. Hatta bu madde kapsamında hâkim tarafından ilgili siteye erişim engelleme kararı verilebilir (5651 S.K.).

Hâkim, bu madde kapsamında vereceği İnternet erişim engellenmesi kararına esas olarak, yalnızca kişilik haklarının ihlal edildiği yayın, kısım, bölümle ilgili olarak nesne tabanlı İnternet erişimi (URL, vb. şeklinde) engellenmesi yöntemiyle uygulanmasını ister. Çok zorunlu olmadığı sürece İnternet sitesinde yapılan yayının tamamına yönelik erişim engellenme kararı verilemez. Ancak, hâkim Nesne tabanlı erişim engellemenin (URL) belirtilen içeriğe erişimin engellenemeyeceği şeklinde kanaat getirirse, gerekçesini belirtecek şekilde, İnternet sitesindeki bütün yayını erişime engelleyecek bir karar verebilir (Dülger 2013). Hâkimin bu madde uyarınca verdiği İnternet erişim engellenme kararları doğrudan Erişim Sağlayıcılar Birliğine gönderilir. Hâkim bu maddeye dayanarak yapılan başvuruları en geç yirmi dört saat içinde duruşma yapmadan karara bağlar. Bu kararlara karşı 4/12/2004 tarihli ve 5271 sayılı Ceza Muhakemesi Kanunu hükümlerine göre itiraz edilebilmektedir. İnternet erişiminin engellenmesine konu içeriğin yayından çıkarılması halinde hâkim kararı kendiliğinden kalkar. Erişim Sağlayıcılar Birliği tarafından İnternet Servis Sağlayıcılara gönderilen İnternet içeriğine erişim engellenmesi kararı derhâl, en geç dört saati geçmeyecek şekilde yerine getirilir. Bu madde uyarınca hâkimin verdiği İnternet erişim engellenmesi kararına konu kişilik hakkının ihlaliyle alakalı yayının veya yayınların başka İnternet

adreslerinde de yayınlanması durumunda ilgili kişinin Erişim Sağlayıcılar Birliğine müracaat etmesi durumunda mevcut karar bu adresler için de uygulanır (5651 S.K. 2014).

5.3.3 5651 Sayılı Kanunun 9/A Maddesinde Yer Alan Özel Hayatın Gizliliğinin İhlali Sebebiyle İnternet Erişimin Engellenmesi

5651 sayılı kanuna Şubat 2014 düzenlemesiyle 9 uncu maddeden sonra gelmek üzere, özel hayatın gizliliği nedeniyle içeriğe erişimin engellenmesi başlıklı 9/A maddesi ilave edilmiştir. 9/A maddesi kapsamında, İnternet ortamındaki yayın içeriğinin özel hayatının gizliliğini ihlal ettiğini belirten kişi ya da kişiler, TİB'e başvurmak suretiyle ilgili içeriğe İnternet erişiminin engellenmesini isteyebilir (İnt.Kyn.39). Yapılan bu talepte, hakkının ihlal edildiğine sebep olan yayının tam adresi (URL), hangi açılardan hakkının ihlal edildiğiyle alakalı açıklaması ve kimlik bilgilerini ispatlayacak belgelere yer verilir. Bu bilgilerin eksik olması durumunda talep işleme alınmaz (5651 S.K.).

TİB, kendisine gelen talebin eksiksiz olduğunu görmesi üzerine uygulanmak üzere derhâl Erişim Sağlayıcılar Birliğine bildirir. Erişim sağlayıcılar Birliği tedbir talebini derhâl, en geç dört saat içinde yerine getirmekle yükümlüdür. İnternet erişiminin engellenmesi, özel hayatın gizliliğini ihlal eden yayın, kısım, bölüm, resim, video ile ilgili olarak nesne tabanlı (URL şeklinde) gerçekleştirilir. İnternet erişiminin engellenmesi talebinde bulunun kişiler talepte bulunduğu saatten itibaren yirmi dört saat içinde ilgili talebini sulh ceza hâkiminin kararına sunar. Hâkim konuyla ilgili kararını en geç kırk sekiz saat içinde açıklar ve doğrudan TİB'e gönderir. Bunun aksi olması halinde İnternet erişim engellenmesi tedbiri kendiliğinden ortadan kalkar. Hâkimin aksi bir karar vermesi durumunda verilen bu karara karşı TİB 5271 sayılı Kanun kapsamında itiraz edebilir. İnternet erişiminin engellenmesine konu olan içeriğin yayından çıkarılması durumunda hâkim kararı kendiliğinden hükümsüz kalır. Özel hayatın gizliliğinin ihlaline bağlı olarak gecikmesinde sakınca bulunan durumlarda doğrudan Telekomünikasyon İletişim Başkanının talimatı üzerine İnternet erişim engellenmesi gerçekleştirilir. Telekomünikasyon İletişim Başkanının talimatı üzerine verilen erişimin engellenmesi kararı, TİB tarafından, yirmi dört saat içinde sulh ceza hâkimine sunulur.

Hâkim, bu konudaki kararını en geç kırk sekiz saat içinde açıklar, eğer aksi bir karar verirse engelleme kendiliğinden kalkar (5651 S.K. 2014).

5.4 7258 Sayılı Futbol ve Diğer Spor Müsabakalarında Bahis ve Şans Oyunları Düzenlenmesi Hakkında Kanun Gereğince Erişimin Engellenmesi

7258 sayılı kanunun 5. maddesinde Spor müsabakalarına dayalı sabit ihtimalli ve müşterek bahis veya şans oyunlarını oynatanlar veya oynanmasına yer veya imkân sağlayanlar, yurt dışında oynatılan spor müsabakalarına dayalı sabit ihtimalli veya müşterek bahis ya da şans oyunlarının İnternet yoluyla veya değişik şekillerde erişim sağlamak suretiyle Türkiye'den oynanmasına imkân sağlaması durumunda ilgili yayını yapan İnternet sitesi erişime engellenir (7258 S.K.).

5.5 5846 Sayılı Fikir ve Sanat Eserleri Kanunu Kapsamında Yapılan Erişim Engellemeleri

5651 sayılı Kanun ile İnternetteki yayın faaliyetlerinde bulunma sürecindeki temel fonksiyonlar dikkate alınarak içerik sağlayıcının, yer sağlayıcının veya erişim sağlayıcının sorumluluklarını telif hakları ve tazminat gerektiren haksız fiiller konusu eksik bir şekilde belirlenmiştir (Oğuz 2008). Yer sağlayıcı ve erişim sağlayıcıya, aracılık ettikleri içerikleri kontrol etme sorumluluğu yüklenmemiştir. Fakat 5846 sayılı Fikir ve Sanat Eserleri Kanunu ek madde 4'ün değişik 3. fıkrasında "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 ihlali halinde, hak sahiplerinin başvuruları üzerine ihlale konu eserler içerikten çıkarılır" denilmektedir (Koç 2013). Açık bir şekilde hukuka aykırı içeriklerin doğrudan yayından kaldırılması konusunda yetki ve sorumluluk sınırlaması getirilmemiştir. Yer ve Erişim sağlayıcının sorumluluğu, hukuka aykırı içerikten uygun bir şekilde haberdar edilmelerinden sonra başlamaktadır (Oğuz 2008).

5846 sayılı Fikir ve Sanat Eserleri Kanunu ek madde 4 hükmündeki ifadelere yakın bir düzenlemeyle uyar-kaldır prensibi benimsenmiştir. Uyur-kaldır sistemi İnternet demokrasisi anlayışına ve İnternetin doğasına uygun ilk önce işletilmesi gereken ilke

olmalıdır (Koç 2013). Uygulama gelindiğinde uyar-kaldır yönteminin çok fazla kullanılmadığı görülmektedir. Şikâyeti olan taraflar, ihlali gerçekleştirdiğini düşündükleri içerik sağlayıcılara ya hiç uyarı göndermemekte veya içerik sağlayıcıların hiç bir iletişim bilgisi sitelerinde yer almaması sebebiyle kendileriyle iletişim kurulamamaktadır (Koç 2013).

Erişim ve yer sağlayıcılar tarafından içerikten çıkarılma işlemi yapılamaması neticesinde eser sahibinin Cumhuriyet savcısına başvurup durumu yargıya taşımasıyla İnternet sitesinin söz konusu içeriği sayfasından kaldırana kadar erişim engelleme kararları alınabilmektedir (Memiş 2009).

5.6 6362 Sayılı Kanunun 109'uncu Maddesi Gereğince Erişimin Engellenmesi

Sermaye Piyasası Kanunu m.115/5'te bilgi suiistimali (içeriden öğrenenlerin ticareti), piyasa dolandırıcılığı (bilgi yahut işleme dayalı manipülasyon) ile usule uygun olmayan halka arz ve izin alınmayan sermaye piyasası faaliyetinde bulunulması suç tipi yönünden İnternet ortamında yapılması durumunda ilgili site hakkında İnternet erişim engelleme kararı verilebilmektedir. (Canpolat ve Yenidünya 2014).

5.7 4733 Sayılı Kanunun 8'inci Maddesinin Beşinci Fıkrasının (k) Bendinde Yer Alan Suçlar Nedeniyle Erişimin Engellenmesi

4733 sayılı Tütün Ve Alkol Piyasası Düzenleme Kurumu Teşkilat Ve Görevleri Hakkında Kanunun 8. maddesi (k) bendince tütün mamulleri veya alkollü içeceklerin tüketicilere yapılacak satışının İnternet, televizyon, faks ve telefon gibi elektronik ticaret araçları ya da posta ile sipariş yöntemi kullanarak yapılmasını yasaklamıştır. Bu tür mamullerin İnternet ortamından satışının yapılması durumunda 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunda öngörülen usullere göre ilgili İnternet sitesine erişim engellenmesi kararı verilir (4733 S.K.).

5.8 1262 Sayılı Kanunun 18'inci Maddesinde Yer Alan Ürünlerin İnternet Ortamında Tanıtımının Yapılması Sebebiyle Erişimin Engellenmesi

1262 sayılı İspençiyari ve Tıbbi Müstahzarlar Kanununun 10. maddesinde "Üretim izni alınarak satılan yerli ürünlerin katışıksız olmasından ve formülüne uygun olarak imal edilip edilmemesinden üreten sorumludur. Yabancı ülkelerden ithal edilenler ürünler için ithal izin talep belgesi vermiş olanların vekilleri sorumludur. Gerektikçe ve bedel düzenlemesi yapılmak üzere ürünlerden gelişigüzel alınacak örneklerin tahlilini yaparak Sağlık Bakanlığı sürekli bir kontrol sağlar" denilmektedir. Yine aynı kanunun 18. maddesinde 10. maddede yazılı tahlil sonucunda ürünlerin birleşiminde bulunan maddelerin saf olmadığı veya ruhsat almak için verilmiş formüle uygun olmadığı ya da ilacın tedavi niteliklerini azaltacak veya kayıp edecek şekilde üretilmiş olduğunun anlaşılması durumunda ilaçların bu şekilde tanıtım veya satışların İnternet üzerinden yapılması durumunda TİB tarafından ilgili İnternet sitesine derhal erişimin engellenme kararı verileceği belirtilmiştir (1262 S.K.).

5.9 İnternet Erişiminin Adli Makamlarca Engellenmesi

İnternet ortamında suç işlendiğine dair bir ihbar alındığında veya suç işlendiği tespit edildiğinde Cumhuriyet savcılığınca Sulh Ceza Mahkemesine ilgili sitenin suç oluşturan eyleminden dolayı İnternet erişimine engellenmesi konusunda talepte bulunmaktadır (Dülger 2013). İnternet erişim engellenmesi kararı, soruşturma aşamasında hâkim tarafından, kovuşturma aşamasında ise mahkeme tarafından verilmektedir. Soruşturma aşamasında, gecikmesinde sakınca bulunan bir hal mevcut ise Cumhuriyet savcısı tarafından da İnternet erişim engellenmesi kararı verilebilmektedir. Böyle bir durumda Cumhuriyet savcısı ilgili kararını yirmi dört saat içinde hâkimin onayına sunması gerekmektedir. Hâkim ise kararını en geç yirmi dört saat içinde vermelidir. Bu süre zarfında onaylanmayan erişim engelleme kararı Cumhuriyet savcısı tarafından derhal kaldırılır. İnternet erişim engellenmesi kararı, amacı gerçekleştirecek nitelikte görüldüğü takdirde belirli bir süre ile sınırlı olarak da verilebilir. Hâkim, mahkeme veya Cumhuriyet savcısı tarafından verilen İnternet erişim engellenmesi kararının bir sureti gereği yapılmak üzere TİB'e gönderilir (5651 S.K.2014).

5.10 Erişim Engelleme Kararının Kaldırılması

5651 sayılı kanunun 9. maddesinin 7. fıkrasında suç oluşturan bir içeriğin yayından kaldırılması durumunda İnternet erişimi engelleme kararının kaldırılabileceği hususu düzenlenmiştir (5651 S.K. 2014). Eğer, İnternet erişimi engelleme kararı soruşturma aşamasında alındaysa kararı Cumhuriyet Savcısı, kovuşturma aşamasında alındıysa kararı veren mahkemece kaldırılacağı belirtilmektedir (5651 S.K. 2014). İnternet erişimini engellemenin kaldırıldığını gösterir kararın bir sureti TİB'e gönderilir. TİB'de İnternet Servis Sağlayıcılara elektronik ortamdan bilgi vererek erişim engelleme işleminin sona erdirilmesi sağlar (5651 S.K. 2014).

Koruma tedbiri amacıyla, Cumhuriyet Savcısı, Hâkim veya Mahkemece verilen İnternet erişim engellenmesi kararlarına TİB tarafından ceza muhakemeleri kanunu hükümlerine göre itiraz edilebilir (5651 S.K. 2014). Hakkında İnternet erişimi engelleme kararı verilen bir İnternet sitesinin kullanıcıları da dâhil olmak üzere itiraz hakkına sahiptir. İnternet erişimi engelleme kararına karşı, kararın öğrenildiği tarihten itibaren 7 gün içerisinde itiraz edilebilir (5651 S.K. 2014).

Ceza muhakemeleri kanunu gereği, İnternet erişimi engelleme kararı soruşturma evresinde verildi ise ve karar veren makam Cumhuriyet Savcısıysa Sulh Ceza Hâkimine itiraz edilecektir. İnternet erişimi engelleme kararını Sulh Ceza Hâkimi veya mahkeme verdiyse, kararı veren hâkime veya mahkemeye itiraz edilecektir. Eğer hâkim veya mahkeme, itirazı haklı bulursa kararı düzeltecektir. Kararında ısrar etmesi durumunda itirazı incelemeye yetkili olan makama gönderecektir (5651 S.K. 2014). Ceza Muhakemeleri kanunu madde 268'de yapılacak itirazları incelemeye yetkili makamlar belirtilmiştir. Bu maddeye göre, Sulh Ceza Mahkemesinin vermiş olduğu kararlarda itirazı incelemeye yetkili makam, yargı kapsamında bulunan Asliye Ceza Mahkemesidir. Eğer İnternet erişimi engelleme kararını Asliye Ceza Mahkemesi verdiyse, kararı incelemeye yetkili makam, yargı kapsamında bulunan Ağır Ceza Mahkemesidir (5651 S.K. 2014). İnternet erişimi engelleme kararını Ağır Ceza Mahkemesi verildiyse itirazı incelemeye yetkili makam o yerde Ağır Ceza Mahkemesinin birden fazla dairesi bulunması hâlinde, numara olarak kendisini izleyen

daireye, en son numaralı daire için ise birinci daireye, o yerde Ağır Ceza Mahkemesinin bir tek dairesi var ise, en yakın Ağır Ceza Mahkemesine itiraz edilebilecektir (5651 S.K. 2014).

5651 sayılı kanunda, TİB tarafından alınan İnternet erişimi engelleme kararlarına karşı bir itiraz yoluna yer verilmemektedir. Hâkim onayına sunulan TİB kararları için onay kararını veren adli makama itiraz edilebilecektir. Ancak TİB'in 5651 sayılı kanun 8 nci maddesinde bulunan ve içerik veya yer sağlayıcısı yurt dışında bulunan İnternet siteleri ile ilgili hâkim onayına sunmaksızın erişime engelleme kararları için Kanunda ve Yönetmelikte konuyla ilgili bir hüküm bulunmamaktadır (5651 S.K. 2014). Bu sebepten, İnternet erişimi engelleme kararının TİB tarafından kanuna aykırı olarak alındığını düşünen kişi ya da kişiler ilgili idari işlemin iptali için idare mahkemesinde dava açabilir ve ayrıca uğramış olduğu zarar varsa tam yargı davası ile de tazminat isteyebilir (5651 S.K. 2014).

6. ULUSLARARASI BOYUTTA ERİŞİM ENGELLEME

İnternet iletişiminin düzenlenme sebepleri, uygulamada olan metotlar, kültürel sebepler nedeniyle İnternete yaklaşımdaki farklılıklar, hukuksal yapılar ve bunların işleyişiyle alakalı hususlar ülkeler arasında çeşitlilik göstermektedir. Vatandaşlarının güvenli bir şekilde İnterneti kullanabilmesi için ülkeler bir taraftan siber suçlarla mücadele ederken diğer taraftan da İnternet içeriğini yasa dışı unsurlardan arındırmak için önlemler almakta ve gerektiğinde içeriklere müdahalede bulunacak yasal düzenlemeler yapmaktadırlar. Yapılan düzenlemeler yöntem ve kapsam açısından bakıldığında eleştirilere neden olmaktadır. Dünya örneklerinde İnternet iletişim yöntemlerine ilişkin fikir ayrılıklarının genel sebebi içerik düzenlemelerinin doğrudan devlet tarafından mı, yoksa sivil inisiyatif tarafından mı veya her ikisinin ortaklaşa yapmasının ve uygulamasının mı uygun olacağı noktasında ortaya çıkmaktadır. İnternet içerik düzenlemesi kapsamında konusu zararlı ve yasadışı olarak kabul gören unsurlarla mücadele edilmesi ülkelerin hem fikir olduğu konudur. Fakat bu zararlı ve yasadışı unsurları önlemek için kullanılacak erişim engelleme ve filtreleme hususlarının sınırları tartışılmaktadır.

6.1 İnternet Yönetiminde Yetkili Kurumlar

6.1.1 Kök Sunucular

DNS ağacının en üstünde bulunan ve altındaki tüm alt alanların alan adı sunucularının adreslerini tutan, yetkili alan adı sunucularını öğrenmek için gelen sorguları cevaplayan DNS sunucularıdır (İnt.Kyn.40). Host isimleri-IP dönüşümü ilk olarak kök sunucularında başlar. Kök sunucuları Top-Level Domain (Üst Düzey Alan) sunucularının adresini bilirler ve gelen istekleri gerekli TLD(Top Level Domain-Üst Düzey Etki Alanı) sunucularına yönlendirirler. İnternet üzerindeki isim çözümlemesinin doğru, güvenli ve devamlı olması için kök sunucular gereklidir. Dünya üzerinde isim bazında 13 tane kök sunucu bulunmaktadır (İnt.Kyn.41). Her bir sunucu ICANN tarafından akredite edilmiş farklı kurumlar tarafından yönetilmektedir.

6.1.2 ICANN (İnternet Corporation for Assigned Names and Numbers)

İnternetin küresel ağ niteliğinin korunabilmesi için İnternetin yönetimine ilişkin bazı politikaların merkezi bir şekilde belirlenmesi ve uygulanması gerekmektedir. Temel İnternet mekanizmalarının yönetimi ve politikalarının belirlenmesi görevi çeşitli kurumlar tarafından gerçekleşmektedir. Bunlardan en çok bilineni kısaca ICANN olarak adlandırılan "İnternet Corporation for Assigned Names and Numbers" isimli kuruluştur (Dülger 2013). ICANN, İnternetin iş dünyası, teknik, akademik ve kullanıcı gruplarının geniş katılımlarını içeren, kâr amacı gütmeyen ve özel sektör alanında faaliyet gösteren bir kuruluştur (Bal 2013). ICANN İnternet ağının yaygınlaşmasıyla birlikte alan adı sisteminin özelleştirilmesi için özerk olarak faaliyet göstermek üzere 1998 yılında ABD tarafından yetkilendirilmiştir. ICANN, alan adları sisteminin teknik yönetimi, protokol parametrelerinin belinlenmesi ve kök sunucu sistemi yönetimi işlevlerini koordine etmekle görevlendirilmiştir. Bu yetkileri nedeniyle İnternetin tamamını ICANN'ın yönettiği şeklinde yanlış bir algı bulunmaktadır. Buna bağlı olarak bu kurum oluşturulduğu ve yetkilendirildiği günden beri her zaman çeşitli eleştirilere ve menfaat çekişmelerine hedef olmuştur. İnternet kullanımının yaygınlaşması ve alan adlarının ekonomik değerlerinin artması nedeniyle bu eleştiriler artarak ICANN'ın tüm yetkilerinin bağımsız uluslararası bir kuruluş tarafından devralınması ve görevlerinin bu bağımsız kuruluş tarafından yerine getirilmesi önerilmektedir (Dülger 2013). ABD özellikle ICANN'ı özelleştirme ve uluslararası katılıma açma konusunda çeşitli denemelerde bulunsa da sahip olduğu yetkileri devretme konusunda fazla istekli davranmamıştır. ABD İnternet üzerindeki egemen konumunu korumayı ekonomik ve ulusal güvenlik çıkarları gereğince sürdürmektedir (Dülger 2013).

İnternetin yoğun ticari işlemler ve kritik iletişim alanlarında kullanılması, devletlerin gizlilik politikalarının farklı olması, ulusal güvenlik tehditleri ve İnternet altyapı yatırımları nedeniyle başta AB olmak üzere uluslararası toplum İnternet üzerindeki ABD etkisinin kırılması için çeşitli girişimlerde bulunmuştur (Dülger 2013). Ayrıca ICANN'ın kök sunucularının güvenliğini sağlayamaması ve devletlerin bu yöndeki taleplerini geri çevirmesi de bu yöndeki girişimleri hızlandırmıştır (Kaya 2010). Bu girişimlerin en önemlisi 2005 yılında Tunus'ta gerçekleştirilen Dünya Bilgi Toplumu

Zirvesinde gerçekleştirilmiştir. Zirvede, AB radikal bir teklifte bulunarak, alan adı yönetiminin ICANN ve Amerikan Ticaret Bakanlığından alınarak Birleşmiş Milletler çatısı altında faaliyet gösterecek bir uzmanlık kurumuna aktarılmasını önermiştir. ABD bu teklifi kabul etmemiş ve mevcut tepkileri dindirmek için devletlerin İnternetle ilgili görüşlerini doğrudan beyan edebilecekleri İnternet Governance Forum adlı uluslararası platformu faaliyete sokacağını belirtmekle yetinmiştir (Dülger 2013).

6.1.3 IANA (İnternet Assigned Numbers Authority)

İnternet Assigned Numbers Authority (IANA) ICANN ile koordinasyon içerisinde IP adreslerinin yönetimini gerçekleştirmek amacıyla ve ICANN gibi bağımsız olarak faaliyet göstermek üzere ABD Ticaret Bakanlığı tarafından yetkilendirilmiş kurumdur (İnt.Kyn.42). IANA'nın yetkisi, IP yönetimi için politikalar belirlemekten ziyade önceden belirlenmiş politikaları tarafsız bir şekilde uygulamaktan ibarettir. ICANN için yöneltilen uluslararası kalıtım sorunu IANA için de geçerlidir (Kaya 2010).

ICANN ve IANA'nın mevcut yetkilerine rağmen, İnternetin işlerliği için tüm devletlerin aktif katılımı zorunludur. İnternet trafiğinin aktarıldığı hatlar ve web sitelerini barındıran sunucular dünyanın her tarafına yayılmıştır. İnternet trafiği farklı ülkeleri saniyeler içerisinde geçerek akmaktadır. Bu karmaşık yapı sebebiyle bir noktadaki kesinti dünyanın çok uzak bir noktasındaki İnternet trafiğini olumsuz etkileyebilmektedir. Ayrıca, genel veya bölgesel İnternet noktalarının kontrolü, bakımı, hatların sayısının artırılması içinde devletlerarası işbirliği gerekmektedir (Kaya 2010). Devletlerin katılımı İnternetin yönetiminde önemli bir yer tutsa da ICANN ve IANA'nın mevcut yapılanma şekilleri İnternet politikalarının taraflı olmasına yol açmaktadır. ICANN ve IANA devlet müdahalesi olmaksızın İnterneti düzenleyecek ve İnternetin tüm aktörleri arasında etkileşimi sağlayacak bağımsız kurumlar olarak düşünülmüşlerdir (Kaya 2010). Ancak ne ICANN ne de IANA düşünüldükleri gibi bağımsız olamamışlardır. Aynı şekilde, tüm kök sunucular üzerinde ve özellikle verileri tüm kök sunucular tarafından temel değer olarak alınan A kök sunucusu üzerindeki ABD'nin mutlak hâkimiyeti, devletlerin kendi üst düzey ülke alan adları üzerinde bile egemen

olmalarına veya bu alan adları üzerinde hak iddia etmelerine imkân vermemektedir (Kaya 2010).

6.1.4 Echelon (AUSCANZUKUS)

İnternetin merkezi bir yönetiminin olmaması, bilginin alternatif akım yollarının bulunması ve bir ağdan değil içinde barındırdığı sayısız ağdan oluşması nedeniyle İnternete müdahale çok kolay olmamakla birlikte teknoloji sadece İnternetin lehine olarak gelişmemektedir (Tümerdem 2013). Pek çok ülke elektronik iletişimi denetim altına almak için yeni teknolojilerini geliştirmek çabasındadır. Gelişmemiş ülkelerin bu amaca hizmet eden ilk tepkisi yasaklamak olurken, gelişmiş ülkeler ise iletişimi serbest bırakmakla birlikte teknolojik gizli denetim altında tutmayı tercih etmektedirler (Tümerdem 2013). Gelişmemiş bazı ülkelerde faks cihazlarının devlet kontrolünde kullanılmasını zorunlu tutma veya GSM şirketlerinin faaliyetine izin verilmemesi gibi tedbirler söz konusu iken gelişmiş ve demokratik ülkelerde "Echelon" gibi takip teknolojisi sonrasında müdahale imkânı bulunmaktadır (Tümerdem 2013).

Echelon, Avustralya, Kanada, Yeni Zelanda, Birleşik Krallık ve Amerika Birleşik Devletleri tarafından imzalanan AUSCANZUKUS olarak bilinen UKUSA anlaşmasına dayalı, istihbarat sinyalleri toplama ve analiz ağı işletimini açıklarken kullandıkları isimdir (İnt.Kyn.43). Echelon projesine 1947'de UKUSA Anlaşmasıyla başlanmış ve 1971'de kullanılmaya başlanmıştır. 1971'den bugüne kadar Echelon'un kullandığı teknolojiler ve kapsamı sürekli sürekli olarak genişletilmiş, güncellenmiştir (İnt.Kyn.44). Echelon hakkında kara hatları, yüksek frekanslı radyo, telefon, faks, telsiz iletişimi, Radyo röle, haberleşme uyduları, denizaltı kabloları ve İnternet üzerinde sinyaller toplayıp bu sinyalleri işlemek suretiyle istihbarat toplandığı iddiası dile getirilmektedir (Sloan 2001). Dünyada İnternet üzerinden yapılan tüm yazışmalar Echelon sistemi içinde yer alan 'root server' denilen 13 tane kök sunucu bilgisayardan geçmektedir. Echelon dakikada 8 milyon, günde ise tam 12 milyar telefon görüşmesini izlemekte ve dinlemektedir (Şenkaya, Adar 2014). İlk kez 1988 yılında bir makalede bahsedilmiş 2001 yılında ise AB Parlamentosu Komitesi tarafından soruşturulmuştur. Bu soruşturma sonucu yayınlanan rapora göre "Echelon", telefon, faks, e-mail ve diğer

veri trafiğini uydu iletimi, “public swiched telephone networks (PSTN)” ve mikrodalga bağlantılarının denetimi suretiyle “interception ve “content inspection” yeteneklerini taşımaktadır (Tümerdem 2013). Diğer bir deyişle yapılan iletişimlere denetim ve müdahale etme imkânı tanımaktadır. Echelon’la ilgili olarak iki iddia bulunmaktadır. Bunlardan ilki sistem kullanılarak Amerikan şirketleri için ticari alanda casusluk faaliyetinde kullanıldığıdır. ikinci iddia ise Amerika Birleşik Devletleri vatandaşlarının güvenliği sağlanması amacıyla istihbarat topladığıdır (Sloan 2001).

MERCURY ve ORION isimli uyduların Echelon için iletişimi takip ederek istihbarat topladığı iddiası bulunmaktadır (Sloan 2001). Sistem bu işlemi yaparken sadece kayıt etmekle kalmayıp diğer yandan da konuşmanın yapıldığı çıkış noktasını tespit etmeye çalışmakta ve dünya üzerindeki net koordinatlarını ele geçirmektedir. ABD’de bu amaçla kullanılan ve “Carnivore” adı verilen izleme sistemi, 2000 yılında FBI tarafından geliştirilmiş, servis sağlayıcının bilgisayarına yüklenen bir program sayesinde şüphelilerin e-mail trafiğini ve web üzerindeki her türlü faaliyetini izlemeye yarayan bir sistemdir. FBI’ın bu sistemi kullanarak delil toplayabilmesi için yetkili merciden izin alması gerekmekte olmasına karşın bu sistemin kullanımı, kişilerin özel hayatlarına müdahale edildiğinden bahisle bazı eleştirilere maruz kalmıştır (Tümerdem 2013).

ECHELON programı Amerika birleşik devletlerinde Ulusal Güvenlik Kuruluşu tarafından koordine edilmekte, anlaşma ortaklarında ise İngiltere’de Devlet İletişim Karargah (GCHQ), Kanada’da Kanada İletişim Güvenlik Kurumu (CSE), Avustralya’da Savunma Sinyalleri Yönetimi (DSD) ve Yeni Zelanda’da Devlet İletişim Güvenlik Bürosu (GCSB) tarafından koordine edilmektedir (Sloan 2001). Amerika Birleşik Devletleri, Echelon sisteminin yasadışı faaliyetlerini inkar etmektedir. İnkar etmesinin sebebi ise Echelon faaliyetlerinin birçok ülke kanununda yasadışı olarak düzenlenmiş olmasıdır. Echelon faaliyetleri Amerika Birleşik Devletlerinde yasadışı değildir, çünkü ülkede 1978 yılında çıkarılmış dış istihbaratı gözetleme yasası bulunmaktadır (Sloan 2001).

6.2 Uluslararası Sözleşmeler ve Kurumlar

Siber suç olgusuyla mücadele etmek bakımından en önemli husus uluslararası adli yardımlaşmadır. Bunun bilincinde olan devletler, uluslararası örgütler ve sivil toplum kuruluşları, yeknesak bir mücadeleyi mümkün kılmayı amaçlayan sayısız girişimlerde bulunmuşlardır. Bu sayede ortaya çıkan hukuki enstrümanlardan en önemlisi, Avrupa Konseyi bünyesinde kabul edilen 2001 tarihli Siber Suç Budapeşte Sözleşmesi'dir (Önok 2013). Sözleşmeyle bilişim suçlarının uluslararası özelliğinden kaynaklandığı düşünülen sorunların giderilmesine çalışılmış, bununla ilişkili olarak sanal ortamın düzenlenmesiyle alakalı bir takım kurallar getirilmiştir. Bu konuda yapılan başka bir düzenleme ise yine Avrupa Konseyi tarafından oluşturulan Bilişim Sistemleri Aracılığıyla İşlenen Irkçı ve Yabancı Düşmanı Eylemlerin Suç Haline Getirilmesi İçin Avrupa Siber Suç Sözleşmesi'ne Ek Protokol'dür (Dülger 2013). Ayrıca konuyla alakalı olarak Avrupa Birliği, Birleşmiş Milletler, G 8 ve O.E.C.D. tarafından oluşturulan belgeler de bulunmaktadır. Bilişim suçlarıyla mücadele etmek adına özellikle çocuk pornografisi hususunda Avrupa Konseyi ve Avrupa Birliği tarafından yapılan düzenlemeler de bulunmaktadır (Dülger 2013).

6.2.1 Avrupa Konseyi Siber Suç Sözleşmesi

Avrupa Konseyi (AK) bünyesinde hazırlanarak 23 Kasım 2001 tarihinde Budapeşte'de imzaya açılan ve 1 Temmuz 2004 tarihinde yürürlüğe giren "Sanal Ortamda İşlenen Suçlar Sözleşmesi"ne AK dışındaki ülkelerin de taraf olma imkânı bulunmaktadır (Önok 2013). Bugüne kadar 32'si AK üyesi ve AK dışından ABD olmak üzere toplam 33 ülke sözleşmeye taraf olmuştur. 14 ülke ise sözleşmeyi imzalamış; ancak henüz onaylamamıştır (Anonim 2012).

Anılan sözleşmenin ülkemizce imzalanması konusunda ilgili makamlardan alınan görüşler ışığında, sözleşmeye iç hukuk düzenlemelerinin tamamlanmasının ardından taraf olunmasının uygun olacağı sonucu çıkmış ve ilgili bakanlıkların sözleşmeyle ilgili iç hukuk gereklerinin yerine getirildiğini bildirmeleri üzerine sözleşme, Türkiye tarafından 10 Kasım 2010 tarihinde Strazburg'da imzalanmıştır (Anonim 2012).

İnternet ve bilgisayar ağları aracılığıyla işlenen suçlara ilişkin ilk uluslararası sözleşme olan belge, özellikle telif haklarının ihlali, bilgisayarla bağlantılı sahtecilik, çocuk pornografisi ve güvenlik ağlarının ihlali konuları üzerine odaklanmaktadır (Anonim 2012).

Sanal dünyada işlenen suçların ortak tanımlarının yapılmasını, bu alanda ülkelerin maddi ceza hukuku unsurlarını bu sözleşmeyle uyumlu hale getirmeyi, suçların soruşturulması ve kovuşturulması için gereken yerel ceza usul hukuku yetkilerini sağlamayı ve etkili bir uluslararası işbirliği ortamı oluşturmayı amaçlayan söz konusu sözleşme, küresel düzeyde etkilere sahip olabilecek bir hukuki belgedir (İnt.Kyn.45). Budapeşte Sözleşmesi adıyla da anılan ve siber ortamda özgürlüklerin, insan haklarının ve güvenliğin korunması ile risklerin azaltılmasına ilişkin kabul edilmiş tek uluslararası rehber olan belge, hükümetlerin vatandaşlarını korumasına yönelik önemli bir araç niteliğindedir (Anonim 2012).

Siber Suç Sözleşmesi çok önemli bir adım olmakla birlikte, henüz sadece bir başlangıçtır. Sözleşme Avrupa Konseyi üyesi olmayan devletlere açık olsa da, Sözleşme bölgesel bir araç olup, kendi bölgesinde bile henüz genel kabul görmüş değildir (Önok 2013). Uzun vadede de, global katılım beklenmemektedir; zaten taraf olma süreci de hızlı işlememektedir (Önok 2013). Rusya ve Çin gibi, birçok siber saldırının kaynağı olan ülkelerin sözleşmeye taraf olmaması da endişe sebebidir (Önok 2013). Taraf olan devletlerin de sözleşme gereklerini ne ölçüde iç hukuklarına aktardıkları, tartışmaya açıktır.

2003 tarihli ek protokolünde, sözleşmeyi imzalayan devletlerin bilişim sistemleri aracılığıyla ırkçı ve yabancı düşmanlığı oluşturan içeriğin yayılmasını ve propagandasının suç saymalarını gerektirirken protokolde ayrıca ırkçılık ve yabancı düşmanlığı suçunun tanımı da yapılmaktadır. (İnt.Kyn.45). Özellikle antisemitizmi ve 1940-45 yılları arasında gerçekleşen soykırım veya insanlığa karşı işlenen suçların inkârı, aşırı derecede küçümsenmesi, onaylanması veya meşru görülmesi dâhil ırkçılık ve yabancı düşmanlığını içeren tehdit ve aşağılamaları da cezalandırılması gereken içerikler arasında görmektedir (İnt.Kyn.45). Ancak bu protokol Türkiye tarafından

imzalanmamıştır.

6.2.2 Dünya Fikri Mülkiyet Örgütü (WIPO (World Intellectual Property Organization))

Birleşmiş Milletlerin özelleşmiş 17 örgütünden birisidir. WIPO, Dünyada fikri mülkiyet haklarının korunmasını ve yaratıcı etkinliği teşvik etmek amacıyla kurulmuştur (İnt.Kyn.46). Birleşmiş Milletler Enformasyon Merkezi tarafından Dünya Fikri Mülkiyet Örgütü şeklinde Türkçeleştirilen WIPO (World Intellectual Property Organization), ilk olarak 1883 yılında düzenlenen Paris Fuarı'nda endüstriyel mülkiyet haklarını korumak için 14 ülkenin katılımıyla oluşturulmuştur (İnt.Kyn.47). İlk kuruluşunda marka tescil etmek, patentler ve endüstriyel tasarımlar içeren bir anlaşmadır. 1886 yılında sanat eserlerini ve telif hakkı yasalarını da kapsamı içine almıştır. 1960 yılına gelindiğinde WIPO ismini alan kuruluş, 1974 yılında Birleşmiş Milletlerin bütün üyelerinin tanıdığı bir organizasyona dönüşmüştür (İnt.Kyn.47). Uluslararası anlamda fikri mülkiyet haklarını korumaya ve düzenlemeye yönelik çalışmalar yapan Fikri Mülkiyet Örgütü, aynı zamanda gelişmekte olan ülkelere fikri mülkiyet haklarını korumaya ve düzenlemeye yönelik finansal ve bilimsel destekte de bulunmaktadır (İnt.Kyn.48). Birleşmiş Milletlerin bütün üyelerine açılan anlaşmalarla, ulusların kendi içerisinde fikri mülkiyet hukukunu belirginleştirmeye yönelik çalışmalar yapmaktadır. Bulunduğumuz zaman itibarıyla 24 anlaşma düzenlemiş olan organizasyon, 184 üye ülkeye sahiptir (İnt.Kyn.47). Fikri mülkiyet çevresinde akademik çalışmalar da yapan Fikri Mülkiyet Örgütü, bireysel anlamda da insanların yaratılarını hukuksal bir düzleme yerleştirip fikri mülkiyete saygıyı güçlendirme ve bilinçlendirme görevini sürdürmektedir (İnt.Kyn.47). Fikri Mülkiyet Örgütü ayrıca uluslararası sahada İnternet alan adlarının nasıl oluşturulması gerektiği ve nasıl dağıtılması gerektiği konularında da düzenleme yaptığı gibi alan adlarıyla alakalı ortaya çıkan uyuşmazlıkların çözüm aşamasında da yer almaktadır (Dülger 2013).

Avrupa Konseyi Siber Suç Sözleşmesi, 2003 tarihli ırkçılıkla ilgili Ek Protokolü ve Dünya Fikri Mülkiyet Örgütü ile ilgili bilgilerin ismen bakıldığında İnternet erişiminin engellenmesi ile ilgili bağlantısı görülmese de, Ülkelerin İnternet erişim politikalarını

belirlemekte çok önemli kaynaklar olduğu bilinmelidir.

6.3 Bazı Ülkelerde Erişim Engelleme Uygulamaları

Ülkeler ulusal güvenlikleri hususunda duydukları endişeler, kendi gelenek, tarih, kültür, siyasi, dini ve ahlaki değerleriyle alakalı kaygılanmaları ve uluslararası toplum tarafından yasaklanan ve konusu suç teşkil eden unsurlardan yurttaşlarını korumak adına bir takım düzenlemeler yapmaktadırlar (Kaya 2008). Genel olarak bakıldığında ülkelerin üzerinde ortaklaşa durduğu üç konu göze çarpmaktadır. Bunlar çocuk pornografisi ve cinsel istismarı, telif haklarına ait içerikler ve çocukları pornografik içerikten korunmaktır. Bunların dışında en çok düzenleme konusu olan hususlar extrem pornografi, ırkçılık ve ayrımcılık, nefret ve şiddet içerikleri, online kumar, intihara ve uyuşturucu kullanmaya teşvik gibi konulardır (Dülger 2013).

6.3.1 Almanya

Almanya da İnternet kullanımın gelişmişlik seviyesine oranla oldukça yoğundur. Bu yoğun kullanım oranına rağmen İnternet içeriği Almanya'da devlet eliyle yapılan sıkı bir denetime tabi tutulmaktadır (Kaya 2008). Yapılan denetimin ana başlıklarını ırkçılık, müstehcenlik ve fikri mülkiyet ihlalleri oluşturmaktadır. İnternet içeriğinin kontrolü Jugendschutz isimli kuruluş tarafından yapılmaktadır (Berber ve Kaya 2010). Bunun yanı sıra mahkemeler ve kamu kuruluşları tarafından da bazı içeriklerin bloke edilmesine yönelik kararlar alınabilmektedir (İnt.Kyn.48).

İnternet ortamındaki bütün yetişkin pornografisi kapsamında yer alan yayınların içeriğinin görüntülenmesi için yaş doğrulama sistemi zorunludur (İnt.Kyn.48). Bu kapsamda, yaş doğrulama sistemlerini kullanmayan pornografik içerikli İnternet sitelerini engellemediği için Google neredeyse engellemeye tabi tutulacaktı (Berber ve Kaya 2010). Alınan mahkeme kararları genellikle Almanya'da kamu oyuna açıktır, fakat ilgili kurumlara gelen ihbarlarla yapılan İnternet erişimi engelleme ve içerikten listeleri gizli tutulmaktadır (İnt.Kyn.48).

İnternet şirketlerini tarafından Almanya'da oluşturulan öz düzenleme kuruluşu Multi Medya Servis Sağlayıcısı (FSM) tarafından geliştirilen filtreleme yazılımları ile özellikle ülke dışında hatalı bulunan her türlü içerik kara listeye alınmakta, Almanya'daki İnternet sağlayıcılar tarafından da bu kara listelere uyulması istenmektedir (İnt.Kyn.48). Tarihi nedenlerle Almanya her türlü Nazi propagandasını, ırkçılık söylemlerini ve aşırı sağ görüşleri etkin bir şekilde erişime engellemektedir. Yasal olmayan bir içeriğe müdahale etmek için yurt içi veya yurt dışında barındırılmasını bir koşul olarak aramamaktadır. Yapmış olduğu İnternet erişim engellemelerin etkinliğini artırmak için İnternet Servis Sağlayıcıları ve bilişim şirketlerini sıkı bir kontrole tabi tutmaktadır (Berber ve Kaya 2010). Alman hükümetinin baskıları neticesinde 2005 yılında Google Almanya, Lycos Avrupa, MSN Almanya, AOL Almanya, Yahoo ve T-Online arama sonuçlarıyla alakalı özdenetim uygulayacaklarını ve bu doğrultuda koordineli bir şekilde hareket etmek için Multi Medya Servis Sağlayıcısı ortak veritabanını kullanacaklarını duyurmuşlardır. Bu kapsamda Multi Medya Servis Sağlayıcısı veritabanında engellenen bir içeriğin otomatik olarak bütün arama motorlarında engellenmesi sağlanmıştır (Berber ve Kaya 2010).

Almanya, kamu güvenliğine ciddi tehlike oluşturan durumlarda ve kriminal suçların kovuşturulmasında kullanılmak üzere yapmış olduğu yasal düzenleme ile e-postalarla ilgili olarak; bir e-posta gönderildi ise gönderenin e-posta ve IP adresini, e-posta alınırsa gönderenin, e-posta adresini, gönderme sunucunun IP adresini, gönderilen veya alınan e-postanın tarih, saat dilimi, İnternet servis sağlayıcılarınca 6 ay boyunca muhafaza edilmesini zorunlu kılmıştır (Palfrey *et al.* 2011).

Diğer büyük içerik ve yer sağlayıcılar gibi Youtube medya paylaşım sitesi de Almanya ile yoğun bir işbirliği içerisindedir. Alman politikacılar ve Merkezi Yahudi Konseyi Ağustos 2007'de Youtube medya paylaşım sitesinde barındırılan aşırı söylemli içeriğe sahip videoların kaldırılmasını ve böyle videolara karşı Youtube medya paylaşım sitesinin özel önlemler almasını içeren isteklerini iletmişlerdir. Youtube, bu isteği kabul etmiş, Alman hukukuna aykırılık oluşturan içeriklerin en hızlı şekilde kaldıracaklarını duyurmuştur (Berber ve Kaya 2010).

Kişilik haklarının ihlal edilmesi ve fikri mülkiyet ihlalleri nedeniyle de Almanya'da birçok engelleme gerçekleştirilmektedir (Berber ve Kaya 2010). Örneğin, Alman Sol Parti Federal milletvekili Lutz Heilmann, eski Doğu Almanya'nın iç istihbaratı STASİ'deki göreviyle alakalı bilgilerin yer alması sebebiyle açmış olduğu dava sonucu Lübeck Bölgesel Mahkemesi, www.wikipedia.de İnternet sitesini geçici olarak 2008 yılında kullanıma kapattırmıştır (İnt.Kyn.49). Ücretsiz İnternet ansiklopedisi olan www.wikipedia.de sitesindeki hukuka aykırı veya zararlı sayılan sadece bir sayfa içerik için bütün ansiklopediye İnternet erişimi engellenmiştir. Fikri mülkiyet ihlalleri sebebiyle dünyanın en büyük dosya paylaşım sitelerinden birisi olan rapidshare.com İnternet sitesi 2007 senesinde Alman müzik telif hakkı sahipleri ittifakı GEMA tarafından erişme engellenmiştir. Rapidshare isimli İnternet sitesi yöneticileri kullanıcılar tarafından yüklenen içerikle ilgili olarak sorumlu tutulamayacaklarını belirtmelerine rağmen, telif haklarını ihlal edilen dokümanların Rapidshare isimli İnternet sitesinin sunucularından silininceye kadar erişim yasağı kaldırılmamıştır (Berber ve Kaya 2010).

6.3.2 Amerika Birleşik Devletleri

Amerika Birleşik Devletleri İnternetin anavatanı olması nedeniyle, aynı zamanda İnternet kullanımının ortaya çıkardığı çeşitli hukuki sorunların çözümüne ilişkin ilk hukuki düzenlemelerin de yapıldığı ülke olmuştur (Mahmutoğlu 2002). Amerika Birleşik Devletleri İnternet içeriğini denetlemek amacıyla bir takım yasal düzenlemeleri yürürlüğe koymuştur. Bu düzenlemelerden en önemlileri 1996 tarihli Communications Decency Act (CDA) ve 1998 tarihli Child Online Protection Act (COPA) ve 2001 tarihli Children's İnternet Protection Act (CIPA)'dır. Yapılan düzenlemelerin temel amacı çocukları İnternet üzerindeki yer alan müstehcen yayınlardan korumak ve çocuk pornografisiyle mücadele etmektir. Düzenlemelerin her biri yürürlüğe girdiği dönemlerde Amerika Birleşik Devletlerinde geniş çaplı tartışmalara neden olmuş ve sansür düzenlemeleri olarak bahsedilmişlerdir. Kamuoyundan gelen aşırı tepkiler neticesinde Amerika Birleşik Devletleri Yüksek Mahkemesince CDA ve COPA iptal edilmiştir. Bir takım düzenlemelere tabi tutulan CIPA halen yürürlüktedir (Berber ve Kaya 2010).

Amerika Birleşik Devletleri kongresi, Şubat 1996 da imzalanan Telekomünikasyon Edep Kanununa (Communications Decency Act (CDA)) göre 18 yaşın altı bireylere, "edepsiz" sayılan materyalin iletişiminin ulaştırılmasını yasaklamıştır. CDA, bu materyalin hem sahibini hem de bunu ileten servis sağlayıcısını hedef almıştır. Ancak, CDA daha etkisini bile göstermeden, sivil toplum örgütleri tarafından yargıya taşınmıştır. Yargı, yasada geçen "edepsiz" gibi kavramların muğlâk olduğunu belirterek bunun anayasal haklardan olan ifade hürriyetini zedeleyebileceğini ifade etmiş ve bu görüş Amerikan Yüksek Mahkemesi tarafından da söz konusu muğlâk tanımlamaların geçerli olamayacağına karar verilerek gösterilmiştir (Kılınç 2010). Ayrıca, sakıncalı içeriklerin çocuklarca erişilebilecek şekilde yayınının yasaklaması kanunun uygulama sahasını belirsiz bir hale getirdiğine hükmetmiştir. İnternet ortamının sadece yetişkinler için bir alan olarak uygun değildir. Bunun neticesinde İnternet ortamı yakınlık ve uzaklık kavramının belirtilmeyeceği bir alandır. Dünyanın herhangi bir yerinden hizmet veren İnternet siteleri kullanıcılarına karşı her zaman aynı mesafede kabul edilmektedir. Amerika Birleşik Devletleri Yüksek mahkemesi, bu gerçekliği göz ardı etmeyerek, erotik ve pornografik filmler gösteren sinema salonlarının sadece yerleşim alanlarının dışında gösterim yapabileceği ilkesinden yola çıkarak düzenlenen CDA yasasını mevcut hükümlerin İnternet ortamı için geçerli olmayacağını varsayarak iptal etmiştir. Yüksek Mahkemeye göre bilgisayar karşısındaki kullanıcının yetişkin veya çocuk olduğunun kesin olarak tespit edilmesinin olanaksız olduğundan bu yasanın İnternet yayınları için uygulanamayacağını öngörmüştür (Berber ve Kaya 2010).

Amerikan yasa koyucular da buna, içerik sahibini hedef alan ikinci bir girişim olan Çevrimiçi Çocuk Koruma Kanunu (COPA-Child Online Protection Act) ile karşılık vermişlerdir. "Küçükler için Zararlı" diye bir kavram oluşturarak, bu tür materyallerin ticari dağıtımını düzenlemek istemişler ancak COPA'nın akıbeti de CDA gibi olmuştur. Bunun üzerine bakış açısı tersine dönmüş ve kullanıcıya odaklanılmıştır. 2000 yılında, Çocuk Koruma Kanunu (Children İnternet Protection Act - CIPA) ilan edilmiş ve okullar ile kütüphanelere İnternet filtresi kullanma zorunluluğu getirilmiştir. Bu defa Amerikan Yüksek Mahkemesi kanun tarafında olmuş ve açılan davaları reddetmiştir (Kılınç 2010).

Çocuk Koruma Kanunu (Children İnternet Protection Act - CIPA)'nun etkin bir şekilde uygulamasını temin etmek amacıyla, bu tür filtreleme sistemlerin kurulmaması durumunda okul ve kütüphanelerin almış olduğu federal yardımların kesilmesi öngörülmektedir. Bu sebeple CDA ve COPA gibi CIPA da ifade hürriyetini anayasaya aykırı bir şekilde kısıtladığı gerekçesiyle eleştirilere maruz kalmıştır. Tüm bu eleştirilere rağmen CIPA yürürlüğünü korumaktadır. Mevcut yasa dışında çocukların korunması için ayrıca Amerikan Ceza ve Ceza Usul Kanunu'nun çocukların istismarının önlenmesine ilişkin 2256 numaralı maddesinde yer alan hüküm gereğince içerik sağlayıcılar tarafından erotik ve pornografik yayınlarla ilgili olarak yaş doğrulama benzeri sistemlerin kullanması gerektiğine dair zorunluluk getirilmiştir (Kaya 2010).

Amerika Birleşik Devletlerinde İnternetin içeriğine müdahale etmek için çocuk pornografisi yayını yapan siteler ve fikri mülkiyet ihlalleri mevzu bahis olduğunda engellemeden söz edilmektedir. Çocuk pornografisiyle ilgili suçlar her daim güncelliğini korumakta olan ve evrensel ölçüde bir sorundur (Berber ve Kaya 2010). Çocuk pornografisinin ortaya çıkardığı zarar sadece istismar edilen çocuklarla sınırlı kalmamaktadır. Olayın başka bir boyutu ise çocuk satışının ve çocuk kaçırılma olaylarında görülen artıştır. Birleşmiş Milletlerce kabul edilen Çocuk Haklarına Dair Sözleşme'ye taraf olan ülkelerden olan Amerika Birleşik Devletleri ulular arası büyük bir sorun teşkil eden çocuk pornografisi suçuyla diğer gelişmiş ülkeler gibi etkin bir şekilde mücadele etmektedir (Berber ve Kaya 2010).

Amerika Birleşik Devletleri hukukunda İnternete ilişkin olarak yapılan diğer bir federal yasa ise, İnternet Kumarının Yasaklanması Yasasıdır. Amerika Birleşik Devletlerinde açıklanan bu federal nitelikli düzenlemelerin yani sıra, konu ile ilgili olarak eyaletlerde de çeşitli yasal düzenlemelere gidilmiştir (Mahmutoğlu 2002).

Amerika Birleşik Devletlerinde İnternet içeriğine müdahaledeki diğer bir önemli konu başlığı uluslararası terörizmle mücadeledir. Amerika Birleşik Devletleri 11 Eylül saldırısından bu yana terörle etkin bir mücadele hedefiyle İnternet politikalarında radikal değişikliklere gitmiştir. 2003 yılında Information Operations Roadmap isimli bir düzenlemeyi yürürlüğe koyarak başta İnternet olacak şekilde bütün iletişim araçlarının

askeri amaçla kullanımını, yasa dışı ağların çökertilmesi ve her çeşit ortamda propaganda faaliyetlerine karşı mücadele edilmesini amaçlamıştır (Kaya 2010). Yapılan bu düzenlemede İnternet içeriğine keyfi olarak müdahale edilebileceği ve Amerika Birleşik Devletlerinin İnternet yönetimi konusunda sahip olduğu yetkileri kötüye kullanacağı sebebiyle eleştirilere maruz kalmıştır. Diğer taraftan bu düzenleme kaldırılmamasına rağmen, Amerika Birleşik Devletleri ulusal bilgi ağını siber saldırılardan korumak ve siber güvenliğe yapılacak yatırımları ve araştırmaları teşvik edici yeni stratejiler dile getirilmektedir (Kaya 2010).

6.3.3 Çin

Çin, İnternet hususunda her zaman temkinli davranmıştır. İnternet ağlarına 1990 yılında katılan Çin, gerekli kontrol sistemlerini kuruncaya kadar İnterneti ortamını kamusal alanda kullanıma sunmamıştır (Köse ve Özen 2010). Çin'in kullanmış olduğu İnternet takip ve İnternet erişimi engelleme teknolojisi kendi alanında dünyanın en iyisidir. İnternet takibi için kurmuş olduğu sistem tüm ülkeyi kapsadığı için büyük Çin Seddi'ni andıran Büyük Çin İnternet duvarı şeklinde isimlendirilmiştir (Berber ve Kaya 2010). Engelleme sadece müstehcenlik veya pornografik değil, sosyal, siyasi, diplomatik, dini ve eğitim konularını kapsayacak ve endişe verici boyutlardadır (Köse ve Özen 2010).

Çin'de İnternet filtrelemesi anahtar kelime tabanlı olarak bilinen bir yöntemle omurga düzeyinde uygulanmaktadır. Bu engelleme yöntemi Çin'e özgü ve spesifik bir sistemdir. Sistem, hassas anahtar kelimeler mevcut olup olmadığını belirlemek için IP paketlerinin içeriğini inceleyerek çalışır. Bu anahtar kelimeler tarihsel olaylar, yasaklı gruplar ve Çin hükümeti tarafından sakıncalı olduğu düşünülen konularla ilgilidir. Başlığına veya iletinin içeriğine ilişkin tespit edilen bir anahtar kelime engelleme mekanizmasını tetikler ve hemen kaynak sıfırlama paketleri gönderir (Palfrey *et al.* 2011).

Çin İnternet ortamını yaşamsal gerçek alanların bir uzvu gibi görmekte ve İnternetin kullanılmaya başlandığı ilk dönemlerden beri kullanıcıların aktivitelerini takip etmekte ve gerek gördüğünde de engellemektedir. Kalabalık bir nüfusa sahip olmasına rağmen İnternet bağlantı noktalarında kullandığı gelişmiş sistemler sayesinde tüm Çin'i

kapsayacak şekilde takip, filtreleme ve erişim engellemeyi başarıyla sürdürmektedir (Berber ve Kaya 2010). Çin'in genelinde aşağı yukarı 40.000 civarı İnternet polisi devamlı bir şekilde İnterneti izlemekte ve yakaladıkları herhangi bir kendilerince yasa dışı içeriği en kısa zamanda erişimden kaldırmaktadır. Uygulama öyle bir boyuta ulaşmıştır ki fikir ve görüşlerini yazdığı için 30'u gazeteci olmak üzere 80 kişi hakkında tutuklama kararı verilmiştir. Denetimin sağlanması için İnternet'in en fazla kullanıldığı İnternet kafelerde kullanıcılar gerçek kimliklerini kullanmadan işlem yapamamaktadır (Köse ve Özen 2010). Durumun vahametini gösteren bir diğer önemli konu ise Çin haber siteleri gerçek kimlik bilgileri ile üye olmayan kullanıcılara yorum yaptırmamaktadır (Köse ve Özen 2010).

Ekonomik olarak gelişmek için güçlü bir altyapı gerekliliğinin farkında olan Çin, komünist devlet sistemini benimsemiş olmasına rağmen İnternet ortamının ekonomik kalkınmaya olan katkısı sebebiyle İnterneti tamamen yasaklanmamakta ve dünya ile kıyaslandığında gelişmiş bir ağ altyapısına sahip olmak amacıyla büyük yatırımlar yapmaktadır (Berber ve Kaya 2010). Fakat Çin İnternetin tüm ülke genelinde artarak yaygınlaşmasının denetimi zor olan büyük bir bilgi akışını da beraberinde getireceğini bilmektedir. Bir taraftan hızla gelişen ekonomisine katkıda bulunan İnternetin yaygınlaşması için çalışırken öte taraftan da mevcut komünist düzeni koruma gayretindedir (Berber ve Kaya 2010).

Çin, yasaklar konusunda kartlarını çok kurnazca oynamaktadır. Ülkede tüm bu sosyal paylaşım sitelerinin alternatifleri bulunmaktadır. Twitter yerine Weibo, Facebook yerine adını Çince de insan manasına gelen "ren" sözcüğünden türeyen RenRen, sohbet programları yerine kendi sohbet programı Tengxun kullanılmaktadır. Bugün gençliğin yeni çılgınlığı Weibo'nun 250–300 milyon civarında kullanıcısı vardır (İnt.Kyn.50). Çin'de İnternetten erişimi yasaklanan bazı site isimleri şunlardır: "Chinese Wikipedia, YouTube, Flickr, Blogspot, Blogger, Facebook, Yahoo, Twitter, DailyMotion, Huffington Post, ImageShack, Amnesty International, Human Rights Watch, Reporters Without Borders, Taiwan tarafından barındırılan web siteleri, Dalai Lama hakkındaki web siteleri, pornografi içeren web siteleri" Çin'de kullanılan arama motorları tarafından filtrelenen bazı kelimelerse şu şekildedir: "Demokrasi, İnsan Hakları,

Diktatörlük, Zulüm, 4 Haziran (Tiananmen olayları nedeniyle), Tibet Bağımsızlığı, Dalai Lama, Falun Gong" (Köse ve Özen 2010).

6.3.4 Fransa

Fransa, Almanya'da olduğu gibi aşırı sağ içeriklere ve fikri mülkiyet haklarının ihlalleri gerekçesiyle yoğun bir şekilde İnternet ortamına müdahale etmektedir. Fransa'nın içeriğe müdahalesi hususundaki en önemli girişimini International League Against Racism and Anti-Semitism ("LICRA") isimi örgütün 2000 yılında Yahoo aleyhine Nazi ürünlerinin Yahoo sitesinin açık artırma sayfasında satılması sebebiyle açmış olduğu dava oluşturmaktadır (Berber ve Kaya 2010). Yahudi Öğrenciler Birliği ve Irkçılık karşıtı LICRA'nın (League Against Racism and Anti-Semitism) Nazi hatıraları koleksiyonu ile ilgili Yahoo açık arttırma sitesine ilişkin başvurusu üzerine, Fransız mahkemesi, Yahoo'nun Fransa'dan bağlanan kullanıcıların %90'ının IP'lerini analiz ederek tespit edebileceğine, Fransa'dan bağlanan kullanıcılarının, yasaklı içeriğe erişimini engellemesi için tedbir almasına, aksi takdirde cezai müeyyide uygulanması ve Fransa'daki Yahoo ofisinin gelirlerine el konmasına karar vermiştir. 2000 yılındaki bu olay üzerine Yahoo Ocak 2001 tarihinde açık arttırma sitelerinden Nazi hatıralarının satışını engellemiştir (Kılınç 2010). Fransa'nın bu tutumu karşısında Fransız İnternet kullanıcılara yönelik hizmet veren bazı İnternet sitelerinin mevcut anlaşmalar gereği özdenetim mekanizmalarının çalışmasına sağlamaktadır. Örnek verecek olursak eğer, Google arama motorunun Fransa'da hizmet veren versiyonu Fransız yasalarınca sakıncalı gördüğü içerikleri otomatik olarak filtrelemektedir (Kaya 2010).

Fransa'da İnternet içeriğine ilişkin ikinci temel müdahale nedeni fikri mülkiyet ihlalleridir. Fransa'da telif hakları, Fransız Fikri Haklar Kanunu ve ilgili uluslararası antlaşmalarla düzenlenmektedir. Örneğin Fransa, Edebi ve Sanatsal Eserlerin Korunmasına Dair Bern Sözleşmesini, Telif Haklarının Korunmasına İlişkin Cenevre Sözleşmesini ve WIPO (Dünya Fikri Mülkiyet Teşkilatı) telif hakkı antlaşmasını imzalamıştır (Kılınç 2010). Fransız yasaları ülke genelinde caydırıcılığı sağlamak için içerik sağlayıcılara ağır cezalar öngörmektedir. Fransa, bu amacı öne sürerek İnternet ağını devamlı takip ve kontrol etmektedir. Bazı insan hakları kuruluşları fikri mülkiyet

ihlallerini kullanarak Fransa'nın İnternet trafiğini istihbari amaçla kullanmakta olduğunu iddia etmektedir (Berber ve Kaya 2010).

Aşırı sağ içerikle ve fikri mülkiyet ihlalleri dışında ayrıca online kumar oynatılmasıyla ilgili olarak 10 Şubat 2010 tarihinde; Fransa'da, çevrimiçi kumarla ilgili bir yasada değişiklik taslağı Fransız Senatosu Kültür ve Haberleşme Komisyonuna sunulmuştur. Söz konusu değişiklik; Fransız İdari Kurumu ARJEL'e (Çevrimiçi Oyunları Düzenleme İdaresi) mahkeme kararı olmaksızın erişim engellemeye yönelik önlemler alma yetkisi vermektedir. Bu düzenleme, 5651 sayılı kanunla TİB'e verilen yetkileri çağrıştırmaktadır (Kılınç 2010).

Fransa da, diğer batı ülkelerinde olduğu gibi, çevrimiçi fikri mülkiyet konusunda hassas davranmaktadır. Ülke terörizm, ırkçı nefreti teşvik ve çocuk pornografisi sebebiyle internet erişimini engellemektedir. Yapmış olduğu sınırlı filtreleme sebebiyle nispeten özgür ülkeler arasındadır (Palfrey *et al.* 2011).

6.3.5 Güney Kore

Güney Kore, İnternet bağlantısı ve hızında dünya lideri olmasına, dünyanın en gelişmiş bilgi iletişim teknolojisi sektörlerine sahip olmasına rağmen, İnternet erişimi hükümetin sıkı yasal ve teknolojik kontrolü altındadır (Palfrey *et al.* 2011). İnternet erişimi kısıtlaması yakın zamanlarda meydana gelen feribot kazası sebebiyle Cumhurbaşkanı Park Geun-hye'e yapılan kamu baskıları sebebiyle ve siyasi muhalifleri yıldırma adına giderek artmaktadır (İnt.Kyn.51).

Güney Kore İnternet kullanımında dünyanın en önde gelen ülkelerinden biridir. Ülkenin %81'inin İnternet bağlantısı bulunmaktadır. Ülkede kullanılan ulusal ağ ile vatandaşlar 17 Mbps hız ile dünya ortalamasının üzerinde İnternete erişebilmektedir. Ülke nüfusunun dörtte üçü her gün İnternete girmektedir. Ülkede 126 tane İnternet Servis Sağlayıcısı bulunmakta ve bunlardan geniş bant hizmeti veren Kornet aynı zamanda dünyanın en büyük ADSL tedarikçisidir (Palfrey *et al.* 2011).

Güney Kore'de 1991 yılında çıkarılan Telekomünikasyon İş Yasası ilk dijital ve analog düzenleme olmuştur. Yasada yer alan zararlı ve yaşa dışı içerik kapsamı dâhilinde İnternet sitelerine erişim engellenebilmekteydi, fakat 2002 yılındaki Yargıtay kararları nedeniyle telekomünikasyon hükümlerinin geçerliliği azalmıştır (Palfrey *et al.* 2011). Halen ülkede İnternet erişimini engelleme müstehcenlik, hakaret, şiddet veya zulüm ve tahrik başlıkları altında devam etmektedir (İnt.kyn.52).

Ülkede diğer erişim engelleme sebeplerden biri de ulusal güvenliği korumak içindir. Ulusal güvenliği tehdit eden, devlet tarafından filtrelenmiş içerikleri yaymak veya yayanlarla işbirliği içinde olmak suçtur ve 7 yıl hapis cezası vardır. Ülke gençliğini korumak adına ahlaksız, şiddet, müstehcen, spekülatif olarak tanımlanan anti sosyal bilgilerin filtrelenmesi ülkenin prensiplerinden biri olmuştur (Palfrey *et al.* 2011). Çocuk Koruma Yasası uyarınca, 19 yaşından küçüklerin uygunsuz içeriğe ulaşmaması için alınacak tedbirlerden İnternet Servis Sağlayıcılar sorumludur (İnt.kyn.52).

Güney Kore'de Sosyal Medya da takip altındadır. Bunu örneklendirecek olursak eğer yakın bir zamanda devlet başkanına sosyal paylaşım sitesi Twitter üzerinden hakaret eden bir muhalifin ilgili hesabı kapatılmıştır. Bir başka kullanıcı içinse, yetkilileri tartışmalı bir deniz üssüyle alakalı kararları sebebiyle korsana benzettiği için hakkında dava açılmıştır. Ve son olarak devlet başkanının İnternet iletişim politikasını eleştiren bir yargıç görevden alınmıştır (İnt.Kyn.53). Geçen sene olduğu gibi bu senede Güney Kore Sınır Tanımayan Gazeteciler tarafından İnternet Düşmanları ülkeler raporunda takibe alınmıştır. Raporda, Güney Kore'nin özellikle Kuzey'i destekleyen İnternet içerikleri karşısındaki baskıcı tutumunu artırdığı ve İnternet üzerinde görüşlerine belirten kullanıcılar üzerinde sansürün yoğunlaştığı belirtilmektedir (İnt.Kyn.54).

6.3.6 İngiltere

İngiltere, monarşiyle yönetilmektedir ve dünyanın önde gelen sömürgeci devletlerinden biridir. Aynı zamanda küresel bir finans merkezidir. İngiltere'nin, Galler, İskoçya, Kuzey İrlanda ve kendi ülkesini kapsayan bir anayasası vardır (Palfrey *et al.* 2011). İngiltere, British Broadcasting Corporation (BBC) liderliğindeki geniş bir medya ağına

sahiptir (İnt.Kyn.55). İngiltere şu anda dünyada beşinci büyük geniş bant abone nüfusunu oluşturmaktadır. İnternet konusunda da dünyanın önde gelen ülkelerinden olan İngiltere'de 2007 yılında konutların %61'inde İnternet erişimi vardı ve bunların %84'ü geniş bant bağlantıdan oluşmaktaydı (Palfrey *et al.* 2011).

Politika arenasının en eski üyelerinden biri olan İngiltere, İnternet ağına bütünleşmiş ülkelerden biridir. Bu denli büyük bir entegrasyon ise haliyle daha güçlü kontrol mekanizması getirmektedir. Ülkede sanal yasakların denetimi İnternet Watch Foundation (İnternet İzleme Vakfı) tarafından üstlenilmiştir. Bu vakıf, ülkenin büyük İnternet servis sağlayıcılarıyla da ortaklaşa çalışmaktadır (İnt.Kyn.55). Yapılacak bir İnternet erişimi engellemesinde İngiltere hukuka aykırı veya zararlı içeriğe Nesne tabanlı (URL) erişim engelleme metodunu kullanarak müdahalede bulunmaktadır. Kullanılan bu yöntemin erişim engelleme metotlarında bahsettiğimiz gibi en önemli avantajının sadece hukuka aykırı veya zararlı içeriği engellemesi ve tüm İnternet sitesine erişimin engellenmesinin önlemesidir. Nesne tabanlı (URL) erişim engelleme metodu ceza sorumluluğunun şahsiliği ilkesiyle uyumludur (Berber ve Kaya 2010). İngiliz Telekom şirketi, Cleanfeed adı verilen bir sistem ile İnternet Denetim Kurulunun hazırlamış olduğu kara listeye göre İnternet trafiğini filtrelemektedir (Palfrey *et al.* 2011). Kullanılan filtreleme neticesinde kara listede bulunan bir İnternet sayfasına bağlanılmak istendiğinde sistem uyarı veya bilgi vermek yerine Sayfa Bulunamadı hatası vermektedir (Köse ve Özen 2010).

İngiltere'nin en büyük sanal derdi, çocuk pornografisidir. Uluslararası arenada en ağır suçlardan biri sayılan bu porno dalı Britanya adasında fazlasıyla yaygındır (İnt.Kyn.58). Çocukları Koruma Kanunu (Protectıon Of Children Act 1978) İngiltere'de Çocuk pornografisiyle ilgili erişim engelleme düzenlemesidir (Kılınç 2010). Çocuk pornografisine yönelik her türlü içerik, içerik veya yer sağlayıcının İngiltere'de bulunmasına bakılmaksızın engellenmektedir (Berber ve Kaya 2010). Ülke bu konuda o kadar ciddidir ki, IWD geçtiğimiz yıl Scorpions adlı müzik grubunun üzerinde çıplak bir kız çocuğu resmi bulunan albüm kapağını yayınladığı için Wikipedia'yı bile kara listesine almıştır (İnt.Kyn.58). İngiltere'de, Ocak 2009'da yürürlüğe giren bir düzenlemeyle (Criminal Justice and Immigration Act 2008) halihazırda suç olmayan

bazı ekstrem yetişkin pornografisi bulundurmak da suç haline getirilmiştir (Kılınç 2010).

İngiltere'de 2010'da kabul edilen tasarı ile telif hakları ihlalleri, İnternet alan adları yönetimi, radyo ve televizyon hizmetleri, spektrum gibi konular düzenlenmektedir. Tasarı, Çalışma Bakanlığı'na yasa dışı dosya paylaşan İnternet abonesinin aboneliğini "geçici olarak askıya alma yetkisi" vermektedir. Bu kanun, Fransa'da başlayan daha sonra dalga dalga Avrupa'ya yayılan telif hakkı ihlallerinde "Three Strikes" modelini tercih etmektedir. Bu modele göre; ilk olarak abone elektronik posta ile uyarılır, ikincisinde mektup gönderilir ve son olarak eğer üçüncü kez yakalanırsa bir yıla kadar İnternet hesabı kesilebilir. Kanuna göre; İSS'ler telif hakkı ihlali yapan abonenin erişimini engellemekle yükümlüdür (Kılınç 2010).

İngiliz hükümeti ayrıca, Suriye'den Birleşik Krallık topraklarına dönen kişilerin, gençleri radikalleştirerek "terör eylemlerine" yönlendirmesinden endişe etmektedir. Mevcut uygulamaya göre, polis ve Kraliyet Savcılığı İnternete yüklenmiş videoların kaldırılmasını talep edebilmektedir. Bu çerçevede Şubat 2010'dan bu yana, "terörizm içerikli" olduğu belirtilen 21 binden fazla içerik yayından kaldırılmıştır (İnt.Kyn.56).

İngiliz kanunları yukarıda bahsettiğimiz hususlar haricinde kalan ve konusu veya içeriği suç teşkil eden yayınlarla ilgili değişik bir kanun hazırlamak yerine gerçek hayatta suç teşkil eden unsurlar sanal ortamda işlendiğinde de suçtur ilkesini benimsemiştir. Bir başka deyişle Ceza Kanununda belirtilmiş olan tüm suçlar kapsamında İnternet sitelerine erişim engellenme kararı verilmesi mümkündür (Kılınç 2010).

6.3.7 İran

İnternet erişim engellemeleri konusunda dünya bazında yapılacak bir değerlendirme de İran'ın İnternet düşmanları listesinde yer aldığını görebiliriz. Yapılan erişim engellemede en katı yaklaşım mevcut hükümeti eleştiren yayınlar hususunda görülmektedir. İran halkının siyasi otoriteyi eleştiren yayınlara ulaşması engellenmektedir (Bulut 2009). İran'da mevcut olan baskı rejiminin yurttaşlarının

istediği içeriğe değil de devlet kontrolünden geçen yayınlara erişilmesine izin vardır. Kullanılmakta olan pek çok İnternet filtrelemesini ve yasağını delerek istediği bilgilere erişen kullanıcıların engellenmesi için tedbirler artırmıştır. Uygulanan katı filtreleme ve bloke işleminin farkında olan İran vatandaşları uygulanan engellemeyi aşmak için VPN kullanmak suretiyle yasaklı yurtdışı sitelere giriş yapılabilmekteydi. Fakat İran Parlamentosu Bilgi ve İletişim Teknolojileri Komitesi Başkanı Ramezanali Sobhani-Fard'ın yaptığı açıklamayla yasadışı olan VPN'lere olan erişim tamamen engellenmiş durumdadır. Yani kullanıcılar artık VPN kullanarak özgür İnternete erişim gerçekleştiremeyeceklerdir (İnt.Kyn.57).

Batı kaynaklı olan ve kadın haklarını savunan İnternet siteleri de yaptığı propagandanın İranlı kadınları etki altına almaması için erişim engellemesine tabi tutulmuşlardır. Esasen bakıldığında ülkede uygulanan şeriat kuralları gereği kadınların korunması İran'da izlenen politikalardandır. İnsan hakları ihlallerini önlemek için, bu tür uygulamaları sonlandırmak ve hakkı ihlal edilenlerin haklarını aramak için araştırma faaliyetleri yürüten, çalışmalar yapan, İnternet sitesinde veri ve bilgi yayınlayan uluslararası bir sivil toplum örgütü olan Londra merkezli Uluslararası Af Örgütü'nün İnternet sitesine de erişim engellenmiş durumdadır. (Bulut 2009).

İran İslami rejimle yönetilmektedir ve şeriat kuralları uygulanmaktadır. Ülkede mevcut İnternet erişim engelleme uygulamalarının büyük çoğunluğu dini sebeplere dayanmaktadır (Köse ve Özen 2010) Dolayısıyla, ülke içerisinde diğer dini inanışların yayılmasına müsaade etmemektedir. Diğer dinleri anlatan, yayan, cazip gösteren İnternet sitelerine erişim engellenmiştir (Köse ve Özen 2010).

İnternet erişim engellemesine tabi tutulan sitelerin bazıları da değişik cinsel tercihlere yönelik, yani gay, lezbiyen, biseksüel, transseksüel yayın yapan İnternet siteleridir. İran cinsel tercihlerden dolayı da katı tedbirler almış durumdadır. Cinsel tercihleri nedeniyle suçlu bulduğu kişileri idam cezasıyla cezalandırmaktadır ve dolayısıyla bu tür yayın yapan İnternet siteleri de erişime engellenmektedir (Bulut 2009). Örnek verecek olursak 1990 yılında eşcinsel ilişki yaşadığı tespit edilen üçü erkek, ikisi kadın beş kişi idam edilmiştir. Halkın bu tür aşırılıklara teşvik eden eğilimlerin önüne geçmek için şeriat

kurallarıyla çakışan içeriklerin yer aldığı İnternet siteleri erişime engellenmektedir. Eşcinsel tercihlerin yanında her tür müstehcen ve pornografik yayın yapan İnternet siteleri de yine engellemeye tabi tutmaktadır. Çocuk pornografisi ya da erişkin pornografisi içeren sitelerin haricinde İranlı vatandaşı kızların da yüzlerini gösteren İnternet siteleri de erişime engellenmektedir (Bulut 2009).

YouTube medya paylaşım sitesi ve Facebook sosyal paylaşım sitesi İran'da İnternet erişimi engellemesine tabi tutulmuşlardır. Erişim engelleme sebebi dini sebeplere dayandırılsa da arka planda yatan amaç muhalif yayınların engellenmek istenmesidir (Köse ve Özen 2010).

İran'ın İnternet üzerine uyguladığı yasaklara Eylül 2014 tarihi itibarıyla yenileri eklenmiştir. İslam ahlakına, genel güvenliğe ve İran İslam Devrimi Lideri Ayetullah Humeyni'ye hakaret içeren mesajların yaygınlaştığı gerekçesiyle sosyal içerikli whatsapp, viber ve tango gibi mobil uygulamaların yasaklandığı açıklamış ve İletişim Bakanlığı'na mobil uygulamalara erişimin engellenmesi için 30 gün süre tanınmıştır (İnt.Kyn.57).

Tüm bu yasaklamalara rağmen İran Gençlik ve Spor Bakanlığı Stratejik Araştırma Merkezi tarafından yapılan on beş bin İranlı gencin katılımıyla yapılan anket sonuçlarına göre ülkede gençlerin %67,4'ü İnternet kullanmaktadır. Gençlerin %19,1'i İnternetten sohbet, %15,3'ü sosyal ağlar, %15,2'si oyun oynamak, %10,4'ü ise bilimsel araştırmalar için İnterneti kullanmaktadır. İnternet kullanan gençlerin %69'u ülkede sınırları içerisinde yasaklı olan sitelere girmek için alternatif filtre kırıcı programları kullanmaktadırlar (İnt.Kyn.58).

İran, İnternet üzerinde 2000 yılından beri yasalaştırdığı yasakları uygulamaktadır. Vatandaşlar ile devlet arasında süren yoğun mücadelenin ardından İran şu anda farklı bir yaklaşım geliştirmeye odaklanmış durumdadır. Ülke, 2005'ten beri sadece ülke içinde erişebilecek, dış dünyaya kapalı teknik olarak intranet diyebileceğimiz İran İnternetini geliştirmektedir. İran, fazla kurnaz davranmış ve fişini çekemediği İnterneti, kendi amaçları doğrultusunda kırpıp biçeceği bir platforma dönüştürmeye karar

vermiştir. Eğer İran bu sistemi başarılı bir şekilde uygulamaya başlarsa bu geleceğin İnternetini değiştirecektir (İnt.Kyn.59).

İran İnternet filtreleme sistemleri, hukuki, idari ve teknik yönlerini güçlendirmeye devam etmektedir. İran'ın İnternet filtreleme sistemi, dünyanın en kapsamlı ve karmaşık sistemlerinden biridir. Batı teknolojilerini güvensiz bulduğu için kendi oluşturduğu filtreleme sistemini kullanmaktadır (Palfrey *et al.* 2011).

6.3.8 İtalya

İtalya İnternet suçlarıyla mücadele etmek amacıyla 30 Mart 1998 tarihinde İtalya Emniyet Genel Müdürlüğü bünyesinde Posta ve İletişim Güvenliği Daire Başkanlığını oluşturmuştur. Bünyesinde personel-lojistik ve teknik olmak üzere iki bölüm bulunan bu başkanlığa bağlı olarak 20 ilde de ofisler bulunmaktadır. Dijital ortamda işlenen her suç bu başkanlığın görev alanına girmektedir (İnt.Kyn.60). İtalya özellikle çocuk pornografisi, çocukların korunması ve suistimal edilmelerini önlemeye çok büyük önem vermektedir (Köse ve Özen 2010). İtalya'da 03.08.1998 tarih ve 269 sayılı Kanunla küçüklerin pornografik yayınlarda kullanılması suçunun İnternet ortamı aracılığıyla işlenmesi durumunu özel olarak düzenleme altına almıştır (Nacar 2010). Ülkenin diğer bir düşmanı ise korsan siteleridir. İtalya her fırsatta korsan içerik sunan web sitelerinin erişimini engellemektedir.

İnternet erişimini engelleme konusunda farklı kurumlara da yetkiler verilmiştir. Italian Monopoly Administration Authority (AAMS) kurumu yaklaşık 1750 adet siteyi çeşitli kumar hizmetleri vermesinden dolayı kara listeye almıştır (İnt.Kyn.61). İtalyan polisi yargı kararı olmaksızın 600-900 arası siteyi çocukların istismarı sebebiyle kara listeye almıştır. Ayrıca mahkeme kararları da kara listeye alınmakta ve kara listede bulunan siteleri ISS erişime engellemekle yükümlüdür (İnt.Kyn.61). İtalya'da engellenen sitelere örnek verecek olursak; anti-mafya web sitesi (accadeinsicilia.net10) basın yayın yoluyla karalama yaptığı gerekçesiyle (aduc.it), fuhuş kolaylaştırmak gerekçesiyle online reklam sitesi (bakeca.it) ve dosya paylaşım sitesi (thepiratebay.com) (İnt.Kyn.61). İtalya da 2005 yılında kabul edilen anti terör yasası gereğince WİFİ noktalarından

faydalanmak için kimlik belgeleri veya pasaport numaraları belirtmek gerekmektedir (İnt.Kyn.62).

İtalya İnternet erişimini çocuk pornografisi ve kumar siteleri üzerine yoğunlaştırmıştır. İnternet erişimi hususunda nispeten özgür ülkeler arasındadır (Palfrey *et al.* 2011).

6.3.9 Kuzey Kore

Kuzey Kore'de halkın kullandığı yurt dışına erişmek için İnternet bağlantısı yoktur. Bunun yerine Kuzey Kore yönetimince 2000 yılında kurulan Kwangmyong isimli ülke içi kullanımı olan ulusal intranet ağı bulunmaktadır. Kwangmyong içerisinde e-posta hizmetleri, haber grupları ve bir iç web arama motoru mevcuttur (İnt.Kyn.63) Kwangmyong kamu kullanımı için ücretsiz bir hizmettir. Kwangmyong intranet ağına Kuzey Kore içinde büyük şehirler ve ilçelerin yanı sıra üniversiteler ve büyük sanayi ve ticari kuruluşlar ulaşabilmektedir.

Kwangmyong intranet ağı içerisinde denetimi Kuzey Kore hükümeti tarafından gerçekleştirilen siyasi, ekonomik, bilimsel, kültürel ve diğer bilgi alanları gibi web siteleri, yurtiçi haber servisi, bir e-posta hizmeti, bir sosyal ağ (İnt.Kyn.64) üniversite bilimsel araştırmaları için web tabanlı akademik değişim ve bilgi paylaşımı sağlayan akademik ve bilimsel çalışma alanları, çeşitli devlet kurumları, eyalet hükümeti, kültürel kurumlar, üniversiteler, bir elektronik kütüphanenin yanı sıra bazı önemli sanayi ve ticari kuruluşların web siteleri bulunmaktadır. 2014 yılı itibariyle, Kwangmyong bünyesinde 1 000 ila 5 500 web sitesi olduğu tahmin edilmektedir (İnt.Kyn.63).

6.3.10 Küba

Küba, Kuzey Amerika kıtasında kişi başına en az İnternet kullanım oranına sahip ülkedir. (İnt.Kyn.65). Küba'da Amerika Birleşik Devletleri tarafından uygulanan ticaret ambargosu, hükümet politikaları, ekonomik ve kişisel sınırlamalar sebebiyle İnternet erişiminde büyük sıkıntılar mevcuttur (Palfrey *et al.* 2011). 1998 yılında devlet onaylı

ve sadece bilim insanlarının kullanımında olan İnternet bağlantılı 200 masaüstü bilgisayar vardı ve ülke genelinde 2 000 e-posta adresi mevcuttu. 2000 yılına gelindiğinde ise İnternet bağlantılı 6 000 bilgisayar ve ülke genelinde alınmış 80 000 e-posta adresi vardı fakat bu adreslerden yarısına yakını kullanılmamaktaydı. Küba' da şu anda 190 000 düzenli İnternet kullanıcısı ve 480 000 e-posta adresi bulunmaktadır (İnt.Kyn.66). İnternet erişiminin bu denli az olmasındaki en önemli faktörlerden biri İnternet erişim ücretinden kaynaklanmaktadır. Öyle ki ekonomik ambargo sebebiyle maaşların düşük olduğu ülkede saat başı uluslararası kullanılan İnternet erişiminin ücreti 4,5 dolar, ulusal intranet erişiminin kullanılması için ödenen saat başı ücret ise 1,5 dolardır (Palfrey *et al.* 2011).

Küba hükümeti, ulusal bir intranet ve küresel İnternet ile bir ikili sistem kullanmaktadır. Çoğu Kübalı için sadece ülke içi e-posta sistemi, bir Küba ansiklopedisi ve hükümetin destekleyici web sitelerinden oluşan ulusal intranet erişimi vardır (İnt.Kyn.66). İnternet kullanımının kişi başı oranının düşük olmasının bir sebebi de kullanılan teknolojinin çok eski olmasıdır (İnt.Kyn.66). İnternet üzerinden yayımlanacak her türlü materyal National Registry of Serial Publications kuruluşu tarafından onaylandıktan sonra yayınlanmaktadır ve servis sağlayıcılar hükümet tarafından alınan izinle kişilere erişim sağlamaktadır (İnt.Kyn.66). Ülkede bazı sitlerin alternatifleri mevcuttur. Örneğin "wikipedia" alternatifi "ecured" "facebook" alternatifi "Social Red" siteleridir (İnt.Kyn.67).

6.3.11 Rusya

Rusya'daki İnternet yasakları ABD ve Avrupa'daki uygulamalardan farklıdır ve kararların çoğu siyasidir (Bulut 2009). Rusya'da 2012 yılında yapılan seçimler öncesinde Facebook gibi sosyal paylaşım siteleri üzerinden yapılan protesto çağrıları sebebiyle yeni hükümet seçim sonrası ilk iş olarak İnternet kontrollerini sertleştirmeye başlamıştır. 1 Şubat 2014 tarihinde yürürlüğe giren İnternet kullanımının kısıtlanmasını getiren yasayla güvenlik görevlilerinin İnternet sayfalarını sunucu üzerinden engelleme yetkisini genişletilmiştir. İnternet servis sağlayıcılarından radikal görüşler ya da çocuk pornografisi içeren sitelerin yanı sıra kitle gösterilerine katılım çağrısı yapan İnternet

sitesi ya da sosyal paylaşım sitelerinin de engellenmesini talep edebilmektedir (İnt.Kyn.68).

Rusya'da engellenen tüm İnternet sitelerinin tam listesine erişilememektedir, fakat http://zapret-info.gov.ru/sitesi kullanıcılara verilen IP, URL ve domain isimlerinin listede olup olmadığını belirlemeye imkân tanımaktadır. 21 Eylül 2012'de kanunlaşan yasaya göre alternatif yollardan İnternete giriş yapan kullanıcılara (Proxy, VPN vs.) İnternet erişimi engellenmesinden ağır para cezalarına kadar değişen cezalar verilebilecektir (İnt.Kyn.69).

Rusya'da dünya genelinde kullanılan sosyal paylaşım sitelerinin alternatifi olarak ülke genelinde kullanılan değişik sosyal paylaşım siteleri bulunmaktadır. Bu sitelerden 2006'da kurulan Vkontakte Rusya, Belarus ve Ukrayna'da çok kısa zaman zarfında en popüler sosyal paylaşım sitesi konumuna gelmiştir. Rusya'da İnternet kullanıcılarının %75'inin Vkontakte üyeliği bulunmaktadır. Vkontakte'yi %69'luk kullanım oranıyla Odnoklassniki takip etmektedir. Rusya'da Facebook üyeliği bulunan İnternet kullanıcılarının oranı ise %68'dir (İnt.Kyn.70).

Rusya Devlet Başkanı Vladimir Putin "İnternet CIA'in bir projesi" söyleminin üzerine sadece Rusya içinde çalışacak kapalı devre yeni Rus ağı oluşturulması önerisi getirilmiştir ve Rus İnternetine ülkede sevilen çizgi film kahramanı "Çeburaşka" adı konması düşünülmüştür (İnt.Kyn.71). Uygulama geçip geçmeyeceği ilerideki günlerde görülecektir.

Medyanın kontrolü Rusya'da köklü bir geçmişe sahiptir. Diğer ülkelerle karşılaştırıldığında, İnternet erişimini kontrol etmek için Çin tarzı filtreleme kullanmaktadır. Rus hükümetinin İnterneti filtrelemedeki amacı muhalif yayınları engellemek üzerinedir (Palfrey *et al.* 2011).

6.3.12 Suudi Arabistan

Suudi Arabistan diğer ülkelerle kıyaslandığında İnterneti daha geç kullanmaya

başlamıştır. Ülkede ilk İnternet servis sağlayıcısı 1999 yılında faaliyet göstermeye başlamıştır. İnternet yayınlarında daha çok İslami geleneklere uygun sitelere izin verildiği görülmektedir (Aydın 2008). Engelleme boyutuna bakıldığı zaman ise İslami geleneklere ve ulusal düzenlemelere karşı çıkan yayınlar yapan İnternet sitelerinin yanında politik ve İslam harici dini içerikli olan İnternet siteleri, İsrail İnternet siteleri, şiddet içeren yayınlar yapan İnternet siteler ile pornografik yayın yapan siteler filtrelemeye veya erişim engellemesine tabi tutulmaktadırlar (Köse ve Özen 2010). Suudi Arabistan hükümetinin İnternet ortamında ki kısıtlamalarının yumuşayacağı ya da ortadan kalkması pek mümkün görünmemektedir. Tam tersine ülkedeki İnternet kullanım oranı arttıkça kontroller ve bunun beraberinde engellemeler yoğunlaşarak devam etmektedir (Aydın 2008).

Suudi Arabistan'ın tüm İnternet trafiği Kral Abdulaziz Bilim ve Teknoloji Şehri'nde konuşlu proxy sunuculardan geçmektedir. Mevcut sunucular üzerinde yapılan içerik filtrelemesi iki listeye göre yapılmaktadır. Listelerin ilkini çoğunlukla pornografik yayın yapan İnternet siteleri, diğerini ise Suudi Arabistan hükümetinin muhalif olarak gördüğü İnternet siteleri içermektedir (Köse ve Özen 2010). Suudi Arabistan'ın uygulamakta olduğu filtreleme yazılımı pornografi, uyuşturucu kullanımı, kumar, din değişimi konularında dünya çapında uygulanan en saldırgan filtreleme sistemidir. Diğer taraftan bakıldığında ise Suudi Arabistan vatandaşlarının uygulanan erişim engelleme sisteminin en büyük parçası olduğu görülmektedir. Çünkü Suudi Arabistan vatandaşları tarafından bir günde ortalama 1200 İnternet sitesinin erişime engellenmesi için ihbarda bulunmaktadırlar. Gelen yoğun ihbarlara yetişemeyen Suudi Arabistan İletişim ve Bilgi Teknolojileri Komisyonu (CITC) bu isteklerin sadece yarısı kadarına karşı işlem yapabilmektedir (Köse ve Özen 2010).

Suudi Arabistan birçok batılı devletin aksine İnternet erişim politikasını gizlememekte ve kamuyla paylaşmaktadır. Suudi Arabistan'da İnternet içeriğine temelde sosyal ve siyasal iki sebeple müdahale edilmektedir. 2001 yılında Suudi Bakanlar Kurulu İnternet kullanıcılarının erişmesi ve yayınlanması yasak olan içeriğe ilişkin bir direktif yayınlamıştır. Direktif, ulusal birliği ihlal eden, İslam aleyhtarı olan ve kamu düzenine aykırılığı teşkil eden her türlü içeriğe erişimi ve bu tür içeriğin her türlü ortamda

yayınlanmasını yasaklamıştır. Ayrıca 2006 yılında yapılan başkaca bir düzenleme ile vatandaşların kişilik haklarını ihlal eden, Suudi hukuku ve İslami değerlere aykırı olan ve terör örgütlerine hizmet veren her türlü içerik sebebiyle cezai sorumluluğun doğacağı kabul edilmiştir (Kaya 2010).

Ulusal güvenlik ve kamu düzeninin ihlal edilmesi gibi muğlâk sebeplerin erişim engellemesi için esas kabul edilmesi düzenlemenin siyasal iktidarlar tarafından istismarına yol açmıştır (Kaya 2010). Yapılan düzenlemenin ifade hürriyetini aşırı sınırladığı ve muhalif görüşleri susturmak için kullanıldığı iddia edilmektedir. Benzer bir şekilde İnternet kafeler gibi İnternet toplu kullanım sağlayıcıları da sıkı denetime tabidir. Bu tür yerler devlet tarafından öngörülen filtreleme yazılımlarını kullanmakla yükümlü tutulmuştur (Kaya 2010).

Ülkede İnternet üzerinde yapılan filtreleme sistemleri ve yasaklamalar haricinde kişilere çok ağır bireysel cezalarda verilmektedir. Örneğin, Suudi blog yazarı Raif Bedevi, Cidde Ceza Mahkemesince "Özgür Suudi Liberaller" adlı siteyi kurarak ülkedeki bilgi teknolojisi kanunlarını ihlal etmekten suçlu bulunmuş, 10 yıl hapis ve kırbaç cezası ile cezalandırılmıştır (İnt.Kyn.72). Suudi Arabistan'da Şeyh Sadd El-Gamdi adlı bir din adamı, erkek vasileri olmadan kadınların İnternete girmesini yasaklayan bir fetva vermiştir (İnt.Kyn.73).

Suudi Arabistan ahlaken uygunsuz gördüğü ve dine duyarlı erişim engellemesi yanında, muhalif siyasi siteler ve insan hakları konuları üzerine yayın yapan siteleri filtrelemektedir. Buna ek olarak, devlet İnternet kafeleri sıkı takip altında tutmaktadır. Genel olarak, Suudi Arabistan İnternet filtrelemesini muhalefeti bastırmak ve tek bir dini inanç teşvik etmek amacıyla artırarak devam ettirmektedir (Palfrey *et al.* 2011).

7. SONUÇ

Türkiye'de İnternet kullanımı hızla artmakta ve olumsuz kullanımlardan doğan sorunlar baş göstermektedir. İnternet ortamının her istenenin veya her akla gelenin paylaşılabileceği ve kontrol edilmeyen bir alan olması düşünülmemelidir. Ortaya çıkan sorunların en aza indirgenmesi veya yok edilmesi için teknik ve hukuki yollarla bir takım önlemler almak kaçınılmazdır. Hukukumuzda İnternet ortamının düzenlenmesiyle ilgili olarak çıkarılan 5651 sayılı kanun bireysel özgürlükler açısından bakıldığında olumsuz eleştirilere maruz kalsa da kanunun, Türkiye'deki genç nüfus potansiyeli düşünüldüğünde toplumsal ve kültürel yönüyle ne kadar önemli bir düzenleme olduğu görülmektedir.

5651 sayılı kanunun 8. maddesi kapsamında yer alan intihara yönlendirme, çocukların cinsel istismarı, uyuşturucu ve uyarıcı madde kullanılmasını kolaylaştırma, sağlık için tehlikeli madde temini, müstehcenlik, fuhuş, kumar oynanması için yer ve imkân sağlama, 5816 sayılı Atatürk Aleyhine İşlenen Suçlar Hakkında Kanununda yer alan suçların oluştuğunu gösterir yeterli şüphe bulunması durumunda ilgili yayınlar İnternet erişimine engellenmektedir. Yukarıda sayılan katalog suçların kapsamı tekrar incelendiği zaman önemli eksiklikler göze çarpmaktadır. Terör örgütü propagandası yapan, çocukları ve gençleri üye ve sempatizanlığa teşvik eden İnternet sitelerinin yeterli şüphe olsa bile suç duyurusunda bulunup mahkemelerce erişime engellenmesi beklenmektedir. Katalog suçlar kapsamının genişletilerek dünya çapında terör örgütü olarak kabul edilmiş oluşumların reklâmının yapılması, bu oluşumlara İnternet üzerinden üye temin edilmesi amacıyla oluşturulan sitelerin de erişime engellenmesi düzenlemeye eklenmelidir. Türkiye'de yaşayan genç nüfusun yoğunluğu ve sokak olaylarındaki artış göz önüne alındığında 5651 sayılı yasanın 8. maddesinde belirlenen katalog suçlar kapsamına patlayıcı madde yapımını öğreten ve anlatan İnternet sitelerinin de eklenmesi gerekmektedir.

Katalog suçlar kapsamında tartışmaya konu olan ve Başkanlıkça Re'sen aktif olarak engellenen siteler içerisindeki oranı %84,06 oranla en çok erişimi engellenen müstehcenlik suçunun tekrar gözden geçirilmesi gerektir. İlk başta dikkat edildiğinde

müstehcen kavramının geniş bir anlama sahip olduğu görülmektedir. Neyin müstehcen, neyin erotik ve neyin pornografik olduğunun tanımlanması son derece zordur. Müstehcen tabiri kültürel farlılıklarından dolayı ülkeden ülkeye değişiklik göstermektedir (Dülger 2013). Bunun yanında, tıbbi, sanatsal, bilimsel veya benzeri materyaller, pornografik olmayan nesneler şeklinde değerlendirilmesi gerekmektedir. Bu sebeple 5237 sayılı TCK'nın 226. maddesinde ve 5651 sayılı kanunda müstehcenlik kavramı yerine pornografi kavramı kullanılması çok daha uygundur. Avrupa Konseyi tarafından oluşturulan Avrupa Siber Suç Sözleşmesi içerisinde müstehcen tabiri yerine pornografik eylem tabiri kullanılmıştır. Ayrıca ne tür eylemlerin pornografik olarak değerlendirilebileceği sözleşme içeriğinde açıkça belirtilmiştir (Dülger 2011). Türkiye'nin de sözleşmeye taraf olan ülkeler içinde bulunduğunu göz önüne alacak olursak ilgili kanunlarda gerekli düzenlemeler yapılarak müstehcenlik tanımının anlamı tam olarak belirtilecek şekilde düzenlenmesi uygun olacaktır.

5651 sayılı kanunun 8. maddesi kapsamında yer alan katalog suçlar kapsamında yapılan erişim engelleme uygulamasında eğer içerik veya yer sağlayıcısı yurt dışında ise TİB yeterli şüphe bulunduğu gerekçesiyle mahkeme kararı olmaksızın İnternet sitelerine erişimi engelleyebilmektedir. İçerik Sağlayıcısı yurt dışında bulunan zararlı içerik barındıran İnternet sitelerinin erişime engellemesi ile ilgili olarak sadece zararlı kısmın yayından kaldırılması şeklinde yapılacak bir engelleme daha doğru bir çözüm olacaktır (Henkoğlu ve Yılmaz 2013). Aynı İnternet sitesine diğer ülkelerdeki İnternet kullanıcıları erişirken tüm sitenin İnternet erişimine engellenmesi nedeniyle Türkiye'deki kullanıcılar cezalandırmakta ve alternatif erişim aşma yöntemlerinin kullanılmasına kullanıcılar teşvik edilmektedir.

İnternet erişiminin engellenmesi veya kısıtlanmasıyla ilgili olarak ülkeden ülkeye yönetim biçimleri, kültürel, dini ve siyasal sebepler nedeniyle farklılıklar söz konusudur. Kuzey Kore İnternet erişimini sadece kendi ülkesini kapsayacak şekilde (Kwangmyong) intranet olarak halkın kullanımına sunarken Çin, İran ve Rusya siyasal nedenlerle İnterneti sıkı takip altında tutmaktadırlar. Diğer ülkelere bakıldığında ise çocuk pornosu, çocukları ve gençleri olumsuz etkileyecek sitelerin sıkı denetime tabi tutulduğu görülmektedir. İnternet erişimine müdahale etmeyen ülke yoktur. Almanya,

Fransa, İngiltere gibi ülkeler büyük erişim ve içerik sağlayıcı İnternet siteleri (Google, Youtube, Facebook, Twitter vs.) ile erişim ve içerik sağlamaları ile ilgili bağlayıcı sözleşmeler yapmakta ve ülke kendisi filtreleme yapmasa bile İnternet siteleri o ülkede hizmet veren alt alan adlarında ülkenin istemediği içerikleri filtrelemektedir. Türkiye'de de büyük erişim sağlayıcı veya içerik sağlayıcı şirketlerle bağlayıcı sözleşmeler yapılması ile İnternet erişiminin engellenmesinin, kişisel özgürlüklere müdahale edilmesinin ve ülke imajının zedelenmesinin önüne geçerek uygunsuz içeriğin şirketler tarafından filtrelenmesi sağlanmalıdır.

Türkiye genelinde İnternet üzerinden işlenen suçlar sebebiyle İnternet sitelerine erişim engelleme kararları Sulh Ceza Mahkemelerince verilmektedir. Daha önce verilen bir karar emsal teşkil etmekte ve suçun tekerrür ettiğinin ispatı durumunda aynı gerekçeyle Sulh Ceza Mahkemelerince İnternet sitelerine erişim engellenmektedir. Herhangi bir ildeki herhangi bir Sulh Ceza Mahkemesine başvurup istediğini alamayan kişiler mahkeme mahkeme dolaşmak suretiyle istedikleri kararın çıkması için çeşitli uğraş vermektedirler. Adalet Bakanlığı bünyesinde bölge bazında veya il bazında sadece İnternet ve bilişim hukuku kararları alabilmek üzere İnternet ve Bilişim Mahkemeleri kurulmalı, bu mahkemelerde teknik yönden donanımlı Hakim ve Savcılar görevlendirilmelidir. Örneğin; Youtube medya paylaşım sitesi üzerinden yayınlanan ve suç unsuru teşkil eden bir yayınla ilgili olarak sitenin komple kapatılmasının kişisel özgürlükleri kısıtlayacağı bilinmelidir. Onun yerine 5651 sayılı kanuna Şubat 2014 değişiklikleriyle giren Nesne Tabanlı Erişim Engelleme (URL adresinden erişim engelleme) yöntemine başvurulması durumunda ilgili sitedeki sadece suç unsuru teşkil eden içeriğin engellenmesinin Uluslararası hukuk kurallarına uygun olduğu ve kişisel özgürlükler bakımından herhangi bir hak ihlaline sebep olmayacağı bilinmelidir.

İnternetin hızla yaygınlaşması, ülkemizdeki genç nüfusun fazlalığı ve bunun paralelinde İnternet kullanımındaki artış nedeniyle İnternetin devlet kontrolü altına alınması şarttır. Demokratik toplumlarda devletler, toplumu, aile yapısını ve çocukları korumak ve kollamakla yükümlüdür. Türkiye'deki dini ve kültürel yapı bizi diğer ülkelerden ayıran en önemli etkenlerdendir. Diğer ülkelerde hoşgörü ile karşılanan bazı içerik ve yayınlar toplum yapımız ve ahlaki yargılarımızla bağdaşmamakta ve bunun sonucunda da olağan

olarak İnternet erişimi engellenebilmektedir. Fakat bu engellemenin sınırı aşırıya kaçmamalıdır. Bu görevin hakkıyla yerine getirilebilmesi için toplumdaki bireylerin eğitilmesi ve oto kontrol yeteneklerinin geliştirilmesi önemlidir.

İnternet özgürlüğü konusunda birçok medya organı tarafından dünyada örnek gösterilen Amerika Birleşik Devletleri İnterneti ilk defa kullanan ve kullanıma sokan ülke olarak çeşitli önceliklere sahiptir. İnternet adreslerinin kontrolü ve denetiminden sorumlu iki kurum olan ICANN ve IANA bağımsız olarak görünse de Amerika Birleşik Devletleri bünyesinde faaliyet gösteren kurumlardır. Tüm İnternet sayfalarının çözümlendiği 13 sunucudan en önemlisi olan A kök sunucusu gene Amerika Birleşik Devletleri kontrolündedir. 1975 yılında İngiltere, Kanada, Avustralya, Yeni Zelanda ve Amerika Birleşik Devletlerinin ortaklaşa imzaladığı, AUSCANZUKUS anlaşması olarak bilinen Echelon projesi her ne kadar Amerika Birleşik Devletleri tarafından inkar edilse de İnternetin gözü ve kulağı olarak faaliyetlerine devam ettiği birçok otorite tarafından kabul görmektedir. Bunların yanında bugün dünyanın en büyük sosyal ağ siteleri (facebook, youtube, twitter vb.) Amerika Birleşik Devletleri ülke sınırları içerisinde bulunmakta ve mevcut Amerikan yasalarına uygun olarak yayın yapmaktadırlar.

İnternet erişimini ağır engellemelere ve sınırlamalara tabi tutan ve çalışma içerisinde yer alan ülkeler değerlendirildiğinde öne çıkan ortak husus bu ülkeleri yöneten siyasi otoritelerin Amerika Birleşik Devletleri karşıtlığı öne çıkmaktadır. 2009 yılındaki seçim öncesinde meydana gelen olayların sorumluluğunu sosyal ağ sitelerine yıkan İran, 2012 seçimlerinden önce ülkede meydana gelen protesto gösterilerini bahane ederek İnternet iletişiminde radikal kararlar alan Rusya'nın yanı sıra Amerikan ambargosuna maruz kalan Küba ve yönetim biçimleri sebebiyle Amerika Birleşik Devletleriyle ters düşen Çin ve Kuzey Kore İnternet iletişimini kontrol altına alma çabasındadır. Çalışma içerisinde yer alan ve İnternet erişimini engellemede katı bir politika izleyen Suudi Arabistan ise engellemeyi dini sebeplere dayandırmaktadır. Keza Suudi Arabistan bu engellemelerin büyük çoğunluğunu Suudi halkı tarafından yapılan şikâyetlerin oluşturduğunu dile getirmektedir.

Avrupa ülkelerini ele aldığımızda her ne kadar baskıcı bir politika uygulamasalar da

bunun asıl sebebi büyük yer ve erişim sağlayıcı firmalarla yaptıkları anlaşmalardan dolayıdır. Özellikle ırkçı yayınlar konusunda Almanya ve Fransa'nın katı politikaları bulunmaktadır.

8. KAYNAKLAR

Anonim, (2014). 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun

Anonim, (2012). Türkiye Büyük Millet Meclisi, Yasama Dönemi: 24, Yasama Yılı:3 Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun Tasarısı Ve Dışişleri Komisyonu Raporu, Ankara

Anonim, (2011). T.C. Millî Eğitim Bakanlığı, Bilişim Teknolojileri, İnternet Ve E-Posta Yönetimi, Ankara.

Anonim, (2008) T.C. Milli Eğitim Bakanlığı, Mesleki Eğitim ve Öğretim Sisteminin Güçlendirilmesi Projesi, Bilişim Teknolojileri, Tcp/Ip Taşıma Ve Uygulama Katmanı, Ankara

Anonim, 1262 sayılı İspençiyari ve Tıbbi Müstahzarlar Kanunu

Anonim, 4733 sayılı Tütün ve Alkol Piyasası Düzenleme Kurumu Teşkilat ve Görevleri Hakkında Kanun

Anonim, 7258 Sayılı Futbol ve Diğer Spor Müsabakalarında Bahis Ve Şans Oyunları Düzenlenmesi Hakkında Kanun

Aşçıoğlu, C. ve Şamlı, R. (2008). Dijital Hak Yönetimi ve Hukuksal Düzenlemeler, 3. Uluslar arası Katılımlı Bilgi Güvenliği ve Kriptoloji Konferansı, Bildiriler Kitabı, 101-105

Avşar, Z. ve Öngören, G. (2010). Bilişim Hukuku, Türkiye Bankalar Birliği Yayını, Yayın No:270, İstanbul.

Aydın, İ .S. (2008). Suudi Arabistan Ülke Raporu, T.C. Başbakanlık Dış Ticaret Müsteşarlığı İhracatı Geliştirme Etüd Merkezi.

Bal, N. (2013). İnternet Alan Adları ve İnternet Alan Adı Uyuşmazlıklarının Tahkim Yoluyla Çözümlenmesi, *Gazi Üniversitesi Hukuk Fakültesi Dergisi* C. **XVII**, Sa. 1-2

Birsen, H. (2014) İnternet Yayıncılığı, T.C. Anadolu Üniversitesi, Açıköğretim fakültesi yayını, Yayını No: 2661, Eskişehir

Bulut, E.A. (2009). Türkiye'de İnternet Yasakları, *Bilgi Dünyası*, Cilt **10**, Sayı 2, 163-186

Deilbert R., Maclay C., Palfrey J. and Roberts H. (2010) Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace, Cambridge, USA

Demir, E.P. (2014). İnternet Aracılığı İle Kişilik Haklarına Saldırı, Yüksek Lisans Tezi, T.C. İstanbul Kültür Üniversitesi, Sosyal Bilimler Enstitüsü, İstanbul.

Durnagöl, Y. (2011). 5651 Sayılı Kanun Kapsamında İnternet Aktörlerine Getirilen Yükümlülükler İle İdari Ve Cezai Yaptırımlar, *TAAD*, Cilt:**2**, Yıl:2, Sayı:4

Dursun, H. (2011). Fuhşa ve Fuhuş Hakkındaki Temel Türk Hukuk Normlarına Genel Bir Bakış, *TBB Dergisi*, **11:** 405-406

Dülger, M. V. (2013). Bilişim Suçları ve İnternet İletişim Hukuku, Seçkin Yayıncılık, Ankara.715-823

Dülger, M. V. (2011). 5651 Sayılı Yasada Yapılması Düşünülen Değişiklikler Hakkında Görüşler, 5651 Sayılı Yasa Hakkında Arama Toplantısı, Bahçeşehir Üniversitesi Hukuk Fakültesi – İstanbul Barosu Bilişim Hukuku Merkezi, İstanbul

Gödekli, M. (2013). Telekomünikasyon İletişim Başkanlığı, İstanbul Üniversitesi *Hukuk Fakültesi Mecmuası*, Cilt:**71**, Sayı:1, 511-546

Gönenç, E. (2014). 5651 Sayılı İnternet Kanunu'nda Yapılan Değişiklikler Üzerine Değerlendirme, *Adli Bilişim Dergisi*, Sayı:**1**, 8-12

Güngör, M. ve Evren, G. (2002). İnternet Sektörü ve Türkiye İncelemeleri, T.C. Telekomünikasyon Kurumu, Tarifeler Dairesi Başkanlığı Yayını, Ankara.

Henkoğlu, T. ve Yılmaz, B. (2013). İnternet Erişim Özgürlüğünün Kısıtlanması: Türkiye Üzerine Bir Değerlendirme, *Bilgi Dünyası*, **14 (2)**, 215-239

Karaca, A. ve Beyaznar, B. (2010). İnternette Müstehcenlik: Nerede Başlar ve Nerede , Biter?, Akademik Bilişim 10 - XII. Akademik Bilişim Konferansı Bildirileri, 63-70

Karakeyha, H. (2013). Kumar Oynanması İçin Yer ve İmkan Sağlama Suçu, Marmara Üniversitesi Hukuk Fakültesi, *Hukuk Araştırmaları Dergisi*, **C.19**, 699-713

Kaya, M. B. (2010). Teknik ve Hukuki Boyutlarıyla İnternet Erişiminin Engellenmesi 5651 Sayılı Kanun ve Dünya Uygulamaları, On İki Levha Yayınevi, İstanbul

Keser, L. Ve Kaya, M. B. (2010). 5651 Sayılı Kanunun Teknik ve Hukuki Açıdan Değerlendirilmesi, *TÜSİAD Görüş Dergisi*, **74,** Sayfa: 4-27

Kılınç, D. (2010). Türk Hukukunda ve Mukayeseli Hukukta İnternet Sitelerine Erişimin Engellenmesi ve İfade Hürriyeti , *Gazi Üniversitesi Hukuk Fakültesi Dergisi*

C.**XIV**, 2

Koç, S. (2013) Hukuksal Bağlamda Sosyal Medya Analizi ve Kıyaslamalı Mevzuat Önerileri, Yüksek Lisans Tezi, İstanbul Bilgi Üniversitesi. Sosyal Bilimler Enstitüsü, İstanbul

Köse, G. ve Özen, K. (2010). İnternet'te Sansür Üzerine Bir Değerlendirme, Hacettepe Üniversitesi Bilgi ve Belge Yönetimi Bölümü, *Elektronik Haber Bülteni*, Sayı:**3**, 113-122

Mahmutoğlu, F. S. (2002). Karşılaştırmalı Hukuk Bakımından İnternet Süjelerinin Ceza Sorumluluğu, *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası*, **C.59**, 39-49

Memiş, T. (2009). Erişimin Engellenmesi, Hukuki Sorunlar ve Çözüm Önerileri, *EÜHFD*, C. **XIII**, 3–4

Nacar, F.B. (2010). Avrupa Birliği Ülkeleri ve Türkiye'de Bilişim Suçlarının Ceza Hukukundaki Uygulamaları, Yüksek Lisans Tezi, Atılım Üniversitesi, Sosyal Bilimler Enstitüsü, Ankara

Oğuz, S. (2008). Telif Hakkı İhlallerinden İnternet Servis Sağlayıcıların Sorumluluklar, *Gazi Üniversitesi Hukuk Fakültesi Dergisi* C. **XII**, 149-182

Osman, M., Sultana, R., Slthana, S. (2013), Enhancement of Public Transportation Services Using Wireless Technologies , *International Journal of Engineering Trends and Technology (IJETT)* – Volume **6** Number 7

Önok, M. (2013). Avrupa Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliği, Marmara Üniversitesi Hukuk Fakültesi, *Hukuk Araştırmaları Dergisi,* Cilt:**19**, Sayı:2, 1229-1270

Özmen, Ö. (2009). Uyuşturucu ve Uyarıcı Madde Suçları, Yüksek Lisans Tezi, Bahçeşehir Üniversitesi, İstanbul

Palfrey J., Zittrain J., Deibert R. and Rohozinski R. (2011) Access Contested: Security, Identity, and Resistance in Asian Cyberspace, Cambridge, USA

Sakarya, D. - Güneş, C. ve Sakarya, A. (2012). İnternette İntiharı Aramak: İnternet Sitelerinin İntihar ile İlişkili İçeriklerine Göre Değerlendirilmesi, *Türk Psikiyat -ri Dergisi***, 24(1)**: 44-48

Şenkaya, Y., Adar, U. G., (2014) Siber Savunmada Yapay Zeka Sistemleri Üzerine İnceleme, Mersin Üniversitesi, *Akademik Bilişim Dergisi*, **22**: 13-17

Tulum, İ. (2006). Bilişim Suçlarıyla Mücadele, Yüksek Lisans Tezi, Süleyman Demirel Üniversitesi, Sosyal Bilimler Enstitüsü, Isparta.

Tümerdem, M. (2013). İnternette Kişilik Hakkı İhlâlinden Kaynaklanan Manevi Tazminat, Yüksek Lisans Tezi, Ankara Üniversitesi, Sosyal Bilimler Enstitüsü, Ankara.

Yenidünya, A. C. ve Canpolat, C. (2014) Sermaye Piyasası Kanunu'nda Düzenlenen Güveni Kötüye Kullanma Suçu, *BFHD* - Cilt: 3, Sayı: 9, 110-159

Yılmaz, S. (2007). Hukuki Açıdan İnternet Bankacılığı, Yetkin Yayınevi, Ankara

Zittrain J., Palfrey J., Deibert R. and Rohozinski R. (2008) Access Denied: The Practice and Policy of Global Internet Filtering, Cambridge, USA

Warf, B. (2011). Geographies of Global İnternet Censorship, University of Kansas, *GeoJournal* **76:**1–23, USA

İnternet Kaynakları:

1- http://tr.wikipedia.org/wiki/Web_2.0, Erişim Tarihi:04.01.2015

2- http://www.teknolojide.com/bilgisayar-nedir_4881.aspx, Erişim Tarihi: 21.12. 2014

3- http://seset.ceit.metu.edu.tr/2011/10/İnternetin-tarihcesi/ Erişim Tarihi: 29.11. 2014

4- http://www.İnternetarsivi.metu.edu.tr/10yil.php, Erişim Tarihi: 21.12.2014

5- http://tr.wikipedia.org/wiki/HTTP Erişim Tarihi:06.05.2015

6- http://www.ipadres.com/yazilar/tcpipprotokolleri Erişim Tarihi:06.05.2015

7- http://tr.wikipedia.org/wiki/Dosya_aktarım_iletisim_kuralı Erişim Tarihi:06.05.2015

8- http://tr.wikipedia.org/wiki/Web_tarayıcı/ Erişim Tarihi: 15.03.2015

9- http://www.tr.wikipedia.org/wiki/IP_adresi, Erişim Tarihi: 21.12.2014

10- http://www.ipadresi.org/website.php, Erişim Tarihi: 21.12.2014

11- http://www.tr.wikipedia.org/wiki/DNS, Erişim Tarihi: 21.12.2014

12- http://www.bilisimterimleri.com/bilgisayar_bilgisi/bilgi/4.html, Erişim Tarihi: 21.12.2014

13- http://www.daha.net/blog/alan-adi-uzantilarinin-anlamlari-ve-alan-adlarinin-yapisi/, Erişim Tarihi: 21.12.2014
14- http://windows.microsoft.com/tr-tr/windows-vista/what-is-a-proxy-server, Erişim Tarihi: 01.01.2015
15- http://proxy.nedir.com/, Erişim Tarihi: 01.01.2015
16- http://www.ersanyildirim.com/index.php/server/ pfsense/37-proxy-server-vekil-sunucu. html, Erişim Tarihi: 24.01.2015
17- http://router.nedir.com/, Erişim Tarihi: 01.01.2015
18- http://www.hukuksokagi.com/kaynak/5651-sayili-yasaya-gore-erisim-engellemeleri / Erişim Tarihi: 15.03.2015
19- https://opennet.net/about-filtering, Erişim Tarihi:14.04.2015
20- http://www.doublesolution.com/tr-blog--36-Yer_Saglayici_Erisim_saglayici_ ve _Toplu_Kullanim Saglayici _Kimdir_#.VEU8MPl_vtw, Erişim Tarihi: 23.10.2014
21- http://www.cnnturk.com/bilim-teknoloji/İnternet/her-İnternet-kullanicisinin-bilmesi-gereken-kavramlar, Erişim Tarihi: 24.10.2014
22- http://www.mgencer.com/files/BilgisayarKitabi.pdf, Erişim Tarihi:14.05.2015
23- http://www.tib.gov.tr/tr/tr-menu-47-İnternet_icerik_duzenlenmesi_hakkindaki_ sorular.html, Erişim Tarihi: 06.12.2014
24- http://www.esquire.com.tr/Teknoloji/2014/02/05/url-tabanli-erisim-engelleme-nedir, Erişim Tarihi: 24.01.2015
25- https://yenimedya.wordpress.com/2014/03/23/ozlu-bilgi-dns-ve-ip-tabanli-engelleme-nedir/, Erişim Tarihi:24.01.2015
26- http://www.ersanyildirim.com/index.php/server/ pfsense/37-proxy-server-vekil-sunucu.html, Erişim Tarihi: 24.01.2015
27- http://www.daha.net/blog/proxy-sunucular-nedir-ve-ne-ise-yarar/, Erişim Tarihi: 24.01.2015
28- http://www.cozumpark.com/forums/thread/1795.aspx, Erişim Tarihi: 01.01.2015
29- http://www.mustafakaya.com.tr/ddos-ataklari-nedir.html, Erişim Tarihi: 01.01. 2015
30- http://www.kaynet.net/index.php/coezuemlerimiz/sunucu/item/48-sunucu, Erişim Tarihi: 01.01.2015

31- http://www.melihguney.com/yasak-niteleri-nasil-girilir.html, Erişim Tarihi: 21. 12.2014
32- http://bilimsol.org/bilimsol/bilisim/İnternet-yasaklari-ile-mucadele-kilavuzu, Erişim Tarihi:21.12.2014
33- http://tr.wikipedia.org/wiki/Virtual_Private_Network, Erişim Tarihi: 21.12.2014
34- http://www.turkhukuksitesi. com/makale_ 1447.htm, Erişim Tarihi: 29.11.2014
35- http://www.anayasa.gov.tr/index.php?l=manage_karar&ref=show&action=karar &id=2679 &content= Erişim Tarihi:07.05 2015
36- http://www.esb.org.tr/biz-kimiz, Erişim Tarihi: 01.01.2015
37- http://www.tib.gov.tr/tr/tr-duyuru-56-erisim_saglayicilar_birligi_kuruldu..html, Erişim Tarihi:18.10.2014
38- http://www.ulakbim.gov.tr/ulaknet/calistay/08/5651.pdf, Erişim Tarihi: 15.03. 2015
39- http://www.erdem-erdem.com/articles/İnternet-ortamindaki-yayinlarin-duzen-lenmesi-hakkindaki-kanuna-getirilen-degisiklikler/ Erişim Tarihi:15.03.2015
40- http://www.isc.org/sw/bind/docs/turkish_guide_bind_ile_dns_sunucu_kurulumu .pdf, Erişim Tarihi: 29.11.2014
41- http://blog.btrisk.com/2014/07/dnsdomain-name-system-nedir.html, Erişim Tarihi: 29.11.2014
42- https://www.iana.org/about, Erişim Tarihi: 17.01.2015
43- http://tr.wikipedia.org/wiki/ECHELON Erişim Tarihi: 29.04.2015
44- https://erkete.wordpress.com/2014/07/17/echelonnedirnasilcalisir/ Erişim Tarihi: 25.04.2015
45- http://www.bilisimdergisi.org/s127, Erişim Tarihi : 17.01.2015
46- http://www.wipo.int,Erişim Tarihi:15.03.2015
47- http://tr.wikipedia.org/wiki/ Dünya_Fikri_Mülkiyet_Örgütü, Erişim Tarihi: 17.01.2015
48- http://www.aa.com.tr/tr/bilim-teknoloji/291242--dunyada-İnternet-uygulamalari, Erişim Tarihi : 10.01.2014
49- http://www.milliyet.com.tr/iran-da-dev-İnternet-yasagi-aktiflestirildi-İnternet-16 79441/ Erişim Tarihi: 15.12.2014
50- http://www.hurriyet.com.tr/ planet/18859506.asp, Erişim Tarihi:12.12.2014

51- https://freedomhouse.org/sites/default/files/01152015_FIW_2015_final.pdf, Erişim Tarihi: 14.04.2015
52- https://opennet.net/research/profiles/south-korea, Erişim Tarihi: 14.04.2015
53- http://www.hurriyet.com.tr/planet/21218635.asp. Erişim Tarihi: 17.04.2015
54- http://en.rsf.org/south-korea.html, Erişim Tarihi: 17.04.2015
55- http://shiftdelete.net/devletler-web-sitelerini-neden-yasakliyor-20104?p=2, Erişim Tarihi: 21.12.2014
56- http://www.aa.com.tr/tr/dunya/286112--ingilterede-İnternete-kisitlama-tartisiliyor, Erişim Tarihi: 21.12.2014
57- http://www.hurriyet.com.tr/dunya/27248287.asp, Erişim Tarihi: 15.12.2014
58- http://www.ntvmsnbc.com/id/25536979/, Erişim Tarihi: 15.12.2014
59- https://www.tumblr.com/search/İnternet+yasakları Erişim Tarihi: 15. 12.2014
60- http://www.academia.edu/2333087/Siber_Suclar_ve_Terorizm, Erişim Tarihi: 15.03.2015
61- https://edri.org/files/blocking_booklet.pdf, Erişim tarihi: 03.02.2015
62- http://www.reidsitaly.com/planning/comm/wifi.html, Erişim Tarihi: 03.02.2015
63- http://en.wikipedia.org/wiki/Kwangmyong_(network), Erişim Tarihi : 10.01.2015
64- http://www.washingtonpost.com/blogs/worldviews/wp/2013/03/13/a-rare-glimpse-of north-koreas-version-of-facebook/, Erişim Tarihi : 10.01.2015
65- http://12mars.rsf.org/2014-en/. Erişim Tarihi : 03.02.2015
66- http://www.cubademocraciayvida.org/web/article.asp?artID=13302, Erişim Tarihi: 03.02.2015
67- http://mashable.com/2014/04/03/İnternet-freedom-cuba/, Erişim Tarihi: 03.02. 2015
68- http://www.aktuel.com.tr/dunya/2014/01/17/İnternet-ozgurlugunu-kaybediyor, Erişim Tarihi: 21.12.2014
69- http://www.digitalage.com.tr/rusyada-İnternet-sansuru/, Erişim Tarihi: 21.12.2014
70- http://www.dijitalajanslar.com/İnternet-ve-sosyal-medya-kullanici-istatistikleri 2014/, Erişim Tarihi : 21.12.2014
71- http://www.hurriyet.com.tr/ dunya/26311769.asp, Erişim Tarihi: 21.12.2014

72- http://www.mynet.com/haber/dunya/suudi-blog-yazarina-10-yil-hapis-ve-kirbac-cezasi-1225963-1, Erişim Tarihi:15.12.2014

73- http://www.milliyet.com.tr/ -kadinlar-İnternete-yalniz-girmemeli-/ gundem/ gun-dem detay/ 18.09.2012/ 1597951/default.htm, Erişim Tarihi:15.12.2014

74- http://www.guvenliweb.org.tr/istatistikler/files/ISTATISTIK.pdf Erişim Tarihi: 04.06.2015

ÖZGEÇMİŞ

Adı Soyadı : Mehmet ERYILMAZ

Doğum Yeri ve Tarihi : Aksu / 18.05.1980

Yabancı Dili : İngilizce

İletişim (Telefon/e-posta) : 0530 691 15 34 / mhmtrylmz80@gmail.com

Eğitim Durumu (Kurum ve Yıl)

Lise : Gazi Lisesi – Isparta (1994-1996)

: Yakaavşar Lisesi – Isparta (1996-1997)

Önlisans : Jandarma Meslek Yüksek Okulu (2003-2005)

Lisans : AÖF İşletme Bölümü (2008-2010)

Çalıştığı Kurum / Kurumlar ve Yıl aralığı

Pazarcık İlçe J.K.lığı / Kahramanmaraş (2001-2005)

İl Jandarma Komutanlığı / Iğdır (2005-2008)

İl Jandarma Komutanlığı / Kocaeli (2008-2010)

Ovacık Jandarma Komando Tabur Komutanlığı / Tunceli (2010-2012)

İl Jandarma Komutanlığı / Kırşehir (2012-…….)

Yayınları (SCI ve diğer) : -