

T.C.
SELÇUK ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
KAMU YÖNETİMİ ANABİLİM DALI

DEVLET ELİ İLE İNTERNET İÇERİK DÜZENLEMESİ
SORUNU: TİB ÖRNEĞİ

Ahmet KILIÇ

DOKTORA TEZİ

Danışman
Prof. Dr. ÖNDER KUTLU

Konya – 2013

T.C.
SELÇUK ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
KAMU YÖNETİMİ ANABİLİM DALI

DEVLET ELİ İLE İNTERNET İÇERİK DÜZENLEMESİ
SORUNU: TİB ÖRNEĞİ

Ahmet KILIÇ

DOKTORA TEZİ

Danışman
Prof. Dr. ÖNDER KUTLU

Konya - 2013



T.C.
SELÇUK ÜNİVERSİTESİ
Sosyal Bilimler Enstitüsü Müdürlüğü



BİLİMSEL ETİK SAYFASI

Öğrencinin	Adı Soyadı	Ahmet KILIÇ
	Numarası	114128002001
	Ana Bilim / Bilim Dalı	Kamu Yönetimi / Kamu Yönetimi
	Programı	Tezli Yüksek Lisans ☐ Doktora ☒
	Tezin Adı	Devlet Eli İle İnternet İçerik Düzenlemesi Sorunu: TİB Örneği

Bu tezin proje safhasından sonuçlanmasına kadarki bütün süreçlerde bilimsel etiğe ve akademik kurallara özenle riayet edildiğini, tez içindeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edilerek sunulduğunu, ayrıca tez yazım kurallarına uygun olarak hazırlanan bu çalışmada başkalarının eserlerinden yararlanılması durumunda bilimsel kurallara uygun olarak atıf yapıldığını bildiririm.

Ahmet KILIÇ



T.C.
SELÇUK ÜNİVERSİTESİ
Sosyal Bilimler Enstitüsü Müdürlüğü



DOKTORA TEZİ KABUL FORMU

Öğrencinin	Adı Soyadı	Ahmet KILIÇ
	Numarası	114128002001
	Ana Bilim / Bilim Dalı	Kamu Yönetimi / Kamu Yönetimi
	Programı	Tezli Yüksek Lisans ☐ Doktora ☒
	Tez Danışmanı	Prof. Dr. Önder KUTLU
	Tezin Adı	Devlet Eli İle İnternet İçerik Düzenlemesi Sorunu: TİB Örneği

Yukarıda adı geçen öğrenci tarafından hazırlanan **Devlet Eli İle İnternet İçerik Düzenlemesi Sorunu: TİB Örneği** başlıklı bu çalışma **25 / 10 / 2013** tarihinde yapılan savunma sınavı sonucunda oybirliği / oyçokluğu ile başarılı bulunarak, jürimiz tarafından doktora tezi olarak kabul edilmiştir.

Ünvanı, Adı Soyadı

Danışman ve Üyeler

İmza

Prof. Dr. Önder KUTLU

Danışman

Prof. Dr. Mustafa AYDIN

Üye

Prof. Dr. Birol AKGÜN

Üye

Doç. Dr. Mehmet GÖKÜŞ

Üye

Doç. Dr. Ali ŞAHİN

Üye

ÖNSÖZ

Öncelikle, sağlam bir akademik bakış ve disiplinle, büyük bir nezaket içerisinde rehberlik yaparak çalışmamıza yön veren, en çok ihtiyaç duyduğum anlarda kritik müdahale ve yardımlarıyla tezin tamamlanmasında en büyük desteği sağlayan tez danışmanım Prof. Dr. Önder Kutlu'ya teşekkür ederim. Ayrıca, tez izleme jürisinde yer alarak değerli katkılarını esirgemeyen Prof. Dr. Mustafa Aydın ve Doç. Dr. Mehmet Göküş'e teşekkürü bir borç bilirim.

Tez çalışmam esnasında yakın ilgilerini esirgemeyerek, akademik bilgiye ve çalışmalara verdikleri değer ve önemi destek ve katkılarıyla gösteren, bilgi ve görüşlerini mümkün olan en açık şekilde paylaşan başta TİB Başkan V. Dr. Osman Nihat Şen, TİB Hukuk Dairesi Başkan V. Adil Biçer, TİB İdari Daire Başkan V. Ferruh Seçer, Bilgi Toplumu Dairesi Başkanı Emin Sadık Aydın ve Başbakanlık E-Devlet Grubu Başkanı Dr. A. Ramazan Altınok olmak üzere Dr. Yasin Söyler, Dr. Şahin Bayzan, Ömer Boz, Mehmet Sarı, Lütfi Güvener, Rıdvan Kahveci, Mustafa Küçükali ve Hamit Tabi ile ilgili kurumların tüm çalışanlarına teşekkür ederim.

Bu güne kadar hayatımın her anında varlıklarını her zaman yanı başımda hissettiğim, destek ve yardımlarını, emek ve fedakarlıklarını hiçbir zaman esirgemeyen ve hayatım boyunca kendilerine müteşekkir kalacağım annem ve babam için ise nasıl bir teşekkür cümlesi kurabileceğimi bilemiyorum.

Uzun süren ders ve tez döneminde onlara ayırmam gereken zamanı, büyük bir özveri ve sabırla görmezden gelerek beni her konuda destekleyen, sorumluluklarımı paylaşarak bana uygun çalışma koşulları oluşturan, hayatıma değer katan çocuklarım Elif Sena, A. Afra, S. Rüveyda ve İbrahim Zeki'ye ve eşim Fikran Betül'e ise minnet ve şükranlarım sonsuzdur.



T. C.
SELÇUK ÜNİVERSİTESİ
Sosyal Bilimler Enstitüsü Müdürlüğü



Öğrencinin	Adı Soyadı	Ahmet KILIÇ		
	Numarası	114128002001		
	Ana Bilim / Bilim Dalı	Kamu Yönetimi/Kamu Yönetimi		
	Programı	Tezli Yüksek Lisans ☐	Doktora ☒	
	Tez Danışmanı	Prof. Dr. Önder KUTLU		
Tezin Adı		Devlet Eli İle İnternet İçerik Düzenlemesi Sorunu: TİB Örneği		

ÖZET

Bilgi toplumu ve İnternet olgusu hem yeni kurum, kavram ve ilişkileriyle hem de beraberinde getirdiği sorunlarla birçok yeni tartışmanın odağı olmaktadır. İnternet içerik düzenlemesi sorunu da bu tartışma alanlarından birisini oluşturmaktadır. Zira, İnternet ortamında yer alan pornografi, çocuk pornografisi, şiddet, ırkçılık, ayrımcılık ve nefret içerikleri, kumar ve bahis, intihara ve uyuşturucuya yönlendirme, siber zorbalık gibi yasadışı ve zararlı içerikler tüm toplumu etkilemekle birlikte bilhassa çocuklar, gençler ve aileler için önemli riskler, tehlikeler ve sorunlar oluşturmaktadır.

Bu durum, İnternet ortamında işlenen suçlar ve yaşanan olumsuzluklarla ilgili olarak erişimin engellenmesine kadar varan bir takım yaptırımları, bu alanla ilgili yükümlülük ve sorumlulukların düzenlenmesi konusunu gündeme getirmiştir. Bu gelişme, ifade özgürlüğü ve bilgiye erişim özgürlüğü bağlamında bilgi ve düşüncenin serbest dolaşımına engel olacağı yönünde ciddi eleştirilerle karşılaşmıştır.

Bu çerçevede, İnternetin diğer kitle iletişim araçlarından farklı olan özellikleri; çok boyutlu/aktörlü ve dinamik olması, tekniği, alt yapısı, işleyiş biçimi ve uluslararası niteliği, suç yeri ve zamanı, sorumlu olabilecek kişiler vb. yönünden diğer yayıncılık

türleriyle bağdaşmayan özgün özelliklere sahip olması sebebiyle, içerik düzenlemesinin nedenleri ve konuları, uygulanan modeller, ölçütler, ülkelerin konuya yaklaşımları, hukuksal ve örgütsel yapılar ve işleyişleriyle ilgili konular tüm dünyada tartışılmaya devam etmektedir. Keza, bu tartışmaların benzerleri Türkiye’de de yaşanmaktadır. Özellikle, içerik düzenlemesi için çıkartılan 5651 sayılı Kanun ve uygulamayı gerçekleştiren TİB, bu tartışmaların merkezinde yer almaktadır.

Tezde “İnternet içerik düzenlemesi sorununun mahiyeti nedir ve nasıl çözülür? Türkiye bu işin neresindedir?” sorusunun işaret ettiği temel probleme cevap bulunmaya çalışılmıştır. Tezin amacı, bu kritik sorunu diğer ülkeler ve ülkemizdeki uygulamaları ve teorik tartışmalarıyla birlikte derinlemesine irdeleyerek, soruna ilişkin çözümler üretmeye çalışmaktır.

Tezde, nitel araştırma yöntemlerinden “doküman inceleme” ve “mülakat” yöntemi kullanılmıştır. Buna göre, konuyla ilgili tüm kaynaklar incelenirken, ilgili kamu kurumlarının yöneticileriyle ve uzmanlarıyla mülakat çalışması yapılmıştır. Elde edilen tüm verilerin analizi ve yorumlanmasıyla temel/alt problemlere cevap olabilecek temel/alt hipotezler oluşturulmuş ve bunlar tez içerisinde tartışılarak doğruluğu ve geçerliliği test edilmiştir. Bu yolla elde edilen sonuçlar ve bu sonuçlar bağlamında oluşturulan öneriler çalışmanın son bölümünde kayıt altına alınmıştır.

Tezde, İnternet içerik düzenlemesi sorununun, İnternetin çok boyutlu/aktörlü ve dinamik kendine özgü yapısı nedeniyle karmaşık, çözümü birçok değişkene bağlı ve zor bir sorun olduğu görülmüştür. Fakat, İnternetin içerik güvenliğinin sağlanması için kamu otoritelerince düzenlenmesi ve denetlenmesi gereği de ortaya çıkmıştır. Bu kapsamda sorunun çözümü için düzenlemelerin oluşturulması ve uygulanması aşamalarında yerine getirilmesi gereken bazı önemli temel şartlar tespit edilmiştir.

Buna göre, İnterneti, sunduğu imkanlar ve fırsatlar yanında, riskler ve tehlikeleriyle birlikte ele alan bir yaklaşımın gerekli olduğu belirlenirken, bu sürecin ilgili sektör, kamu, STK ve üniversitelerin içinde yer aldığı “birlikte düzenleme” ve yönetim ilkelerine göre yürütülmesi gerektiği tespit edilmiştir. Keza, düzenlemelerin ifade

özgürlüğü ve bilgiye erişim özgürlüğünü zedelemekten ve İnternetin kendine özgü yapısı ve özellikleri gözetilerek yapılması ve uygulanması gerektiği ortaya çıkmıştır.

Bu çerçevede, uygun yöntem ve yaklaşımlar içeren bütüncül strateji ve politikalar geliştirilmesi ve uygulanması suretiyle ve uluslararası işbirliği sağlanarak, İnternette yer alan yasadışı ve zararlı içeriklerle mücadele edilmesi ve risk/tehlikelerin minimize edilmesinin mümkün ve gerekli olduğu sonucuna varılmıştır. Türkiye'nin ise, İnternet içerik düzenlemesi konusunda, bazı eksiklerine rağmen, yasadışı ve zararlı içeriğe devlet eli ile sınırlı müdahaleyi öngören kendine özgü, önemli ve örnek bir uygulama geliştirdiği sonucuna ulaşılmıştır.

Anahtar Kelimeler: İnternet içerik düzenlemesi, bilgi toplumu, İnternet yönetiřimi, güvenli İnternet, erişimin engellenmesi, uyar-kaldır, müstehcenlik.



T. C.
SELÇUK ÜNİVERSİTESİ
Sosyal Bilimler Enstitüsü Müdürlüğü



Öğrencinin

Adı Soyadı	Ahmet KILIÇ		
Numarası	114128002001		
AnaBilim/ Bilim Dalı	Kamu Yönetimi/Kamu Yönetimi		
Programı	Tezli Yüksek Lisans	☐	Doktora ☒
Tez Danışmanı	Prof. Dr. Önder KUTLU		
Tezin Adı	Internet Content Regulation by the State: The Case of Telecommunication Communication Directorate		

SUMMARY

Knowledge society and Internet phenomenon have been subject to many arguments and discussions across the field due to its new emergence, conceptualization and relations. One of the major arguments related to the issue is Internet content regulation. Illegal and harmful contents (i.e. pornography, child porn, violence, racism, discrimination and hate speech, gambling and lottery, suicide and guidance to drugs, cyber bullying) affect not only the entire society in general but also damage mental and physical well beings of children and families in particular.

This has brought the questions of regulating the liability and responsibility because of resultant drawbacks and harmful effects and sanction up to blocking the access concerning the deterioration and crimes committed through internet environment. This has been gravely criticized by the public as being limiting freedom of information and dealt within the framework of the freedom of expression and freedom of access to information.

Internet and mass media differs greatly from each other on the grounds as such: multidimensional, multi-actoral and dynamic content and its techniques, and infrastructure, mode of operation and international nature, time and place of the crime, responsible and the unique features. The reasons for the need and the dimensions Internet bear are heavily discussed and yet the jury is still out. Certain regulation methods and related topics about operation are multi dimensional. This is valid for Turkey as well. This is more evident especially by the recent law (No: 5651 passed in 2007 by Turkish Parliament) and by the Telecommunication Communication Directorate performing the responsibility about regulation of Internet content.

Within this frame, the thesis intends to answer the following questions: “What are conditions and costs of Internet content regulation problem, and how could the shortcomings be defeated at the lowest costs? What about Turkey? What are the most efficient and effective solutions in Turkey?”. The main aim of the thesis is to highlight various facets of regulation and evaluate different elements concerning the main topic. This involves examination of theoretical and practical points, together with the examples brought by different political and administrative systems.

During the course of the thesis qualitative research methods have been deployed i.e. “document review”, “interview” techniques and so on. Accordingly, the examination necessitates the use of primary and secondary materials: Official document reviews, interviews and other material. The interviewees include academics, practitioners in the field and the primary decision makers, mainly from TCD. The data obtained through the analysis and interpretation of the analytic approaches with hypothesis and sub-hypothesis would give a concrete answer to the basic problem and sub-problems; the hypotheses have been evaluated to test their validity and accuracy.

The thesis has found through the evaluation of the material that it has been evident without doubt that Internet is versatile, multi-actoral, dynamic, and complex due to its peculiarity in the terms of structure and character. The question is a very difficult one and therefore depends on various variables. Besides, it has been observed that in

order to provide an acceptable level of Internet content safety, public authorities should regulate and supervise accordingly. This of course needs answering of a number of eligibility and qualification requirements to be fulfilled.

Consequently, while it is necessary to produce a unique and adept approach in conjunction with the risk and dangers resides over the opportunities offered by Internet. It is also important to regulate this process in line with governance principles and a comprehensive approach in cooperation with the sector, the public, NGOs and universities. It has been found that the regulation should be carried out with little harm possible to the development and growth; freedom of speech and freedom of access to information and surrounding conditions to consider the peculiar structure and character of Internet.

Eventually, by developing and implementing totalitarian strategies and policies to include appropriate approaches and to combat harmful and illegal contents of Internet, it would be necessary to minimize via international co-operation. As far as the Internet content regulation is concerned and despite some shortcomings, Turkey has been developing an exemplary, important and distinctive strategy by the establishment of TCD and issuing the law to govern the implementation process.

Key Words: Internet content regulation, information society, Internet governance, safe Internet, blocking access, notice and take down, obscenity.

İÇİNDEKİLER

BİLİMSEL ETİK SAYFASI.....	iii
DOKTORA TEZİ KABUL FORMU	iv
ÖNSÖZ	v
ÖZET	vi
SUMMARY	ixix
İÇİNDEKİLER.....	xii
KISALTMALAR.....	xxii
TABLolar LİSTESİ.....	xxvii
ŞEKİLLER LİSTESİ	xxviii
GİRİŞ	1
I. Problem	1
II. Amaç.....	6
III. Yöntem	7
IV. Materyaller	9
V. Sınırlılıklar	11
VI. Hipotezler/Alt Hipotezler	13

BİRİNCİ BÖLÜM

BİLGİ TOPLUMU VE İNTERNET: KAVRAMSAL, KURAMSAL VE TARİHSEL ARKAPLAN

1.1. BİLGİ TOPLUMU	21
1.1.1 Kuramsal Çerçeve: Bilgi Toplumu Kavramı ve Özellikleri, Bilgi Toplumunda Devlet ve Kamu Yönetimi ve Kurama Yöneltilen Eleştiriler	21
1.1.1.1. Bilgi Toplumu Kavramı ve Özellikleri.....	22
1.1.1.1.1 Bilgi Toplumu Kavramı	22
1.1.1.1.2 Bilgi Toplumu'nun Özellikleri	24
1.1.1.2 Bilgi Toplumu'nda Devlet ve Kamu Yönetimi.....	25
1.1.1.2.1 Tarihsel ArkaPlan ve Bugün.....	25
1.1.1.2.2 Yönetişim	29
1.1.1.2.3 E-Devlet	30

1.1.1.3	Bilgi Toplumu Kuramına Yöneltilen Eleştiriler	33
1.1.1.3.1	Tüm Dünya Bilgi Toplumu Aşamasında Değil.....	33
1.1.1.3.2	Toplumların Tarihsel ve Yapısal Gerçekleri Farklı.....	34
1.1.1.3.3	Kapitalizmde Geline Son Nokta: Bilgi Toplumu	36
1.1.2	Bilgi Toplumu Sorunları.....	37
1.1.2.1	‘Büyük Birader’ Ya Da ‘Gözetim Toplumu’ Korkusu.....	37
1.1.2.2	Sayısal Uçurum	41
1.1.2.3	Güvenlik Korkusu Ya Da Risk Toplumu	42
1.1.2.4	Tüketim Toplumu ve Yabancılaşma	45
1.1.2.5	Bilgi Kirliliği ve Enformatik Cehalet.....	46
1.1.3	Bilgi Toplumu ve İnternet	49
1.1.3.1	İnternetin Kullanım Alanları ve Sağladığı Faydalar	51
1.1.3.2	İnternette Gelen Sorunlar.....	52
1.1.3.2.1	İnternette Zararlı ve Sakıncalı İçerik Sorunu	53
1.1.3.2.1.1	Pornografi ve Çocuk Pornografisi İçerikleri.....	54
1.1.3.2.1.1.1	Pornografik İçerikler	54
1.1.3.2.1.1.2	Çocuk Pornografisi İçerikleri.....	57
1.1.3.2.1.1.3	İnternette Pornografi ve İfade Hürriyeti	64
1.1.3.2.1.2	Şiddet, Vahşet, Nefret ve İntihara Yönlendirme İçerikleri	70
1.1.3.2.1.3	Kumar / Bahis ve Uyuşturucuya Yönlendirici İçerikler....	73
1.1.3.2.1.4	Telif Hakkı İhlallerine Ait İçerikler	74
1.1.3.2.2	İnternette Güvenlik ve Mahremiyet İhlali Sorunu.....	75
1.1.3.2.2.1	İnternette Güvenlik Sorunu.....	75
1.1.3.2.2.2	İnternette Mahremiyet Sorunu	79
1.1.3.2.3	İnternetin Sebep Olduğu Toplumsal Sorunlar	81
1.1.3.2.3.1	İnternetin Aile Üzerindeki Olumsuz Etkileri.....	81
1.1.3.2.3.2	İnternetin Çocuklar Ve Gençler Üzerindeki Olumsuz Etkileri.....	87
1.1.3.2.3.2.1	Cinsel İstismar ve Pornografi Sorunu.....	87
1.1.3.2.3.2.2	Dijital Oyunlar Sorunu	93
1.1.3.2.3.2.3	Siber Zorbalık Sorunu	97

1.1.3.2.3.3	İnternet Bağımlılığı	98
1.1.3.2.3.4	Sosyal Ağlar ve Etkileri.....	102
1.2	İNTERNET	107
1.2.1	İnternetin Gelişimi	107
1.2.2	Dünyada İnternet Kullanımı	109
1.2.3	İnternetin Yapısal Unsurları	111
1.2.3.1	TCP/IP Protokolü	112
1.2.3.2	World Wide Web (www).....	112
1.2.3.3	Alan Adı ve Adreslerin Gruplandırılması:	113
1.2.4	İnternetin Alt Yapısı.....	114
1.2.5	İnternetin Aktörleri	115
1.2.5.1	İnternet Servis Sağlayıcılar	115
1.2.5.2	İnternet Erişim Sağlayıcılar	116
1.2.5.3	İnternet Yer Sağlayıcılar	117
1.2.5.4	İnternet İçerik Sağlayıcılar.....	118
1.2.6	İnternetin Geleceği: Web 1.0 dan Web 3.0'a	119
1.2.7	İnternetin Yönetimi	121
1.2.7.1	İnternet Yönetimiyle İlgili Kurumlar	121
1.2.7.1.1	ICANN	121
1.2.7.1.2	IANA.....	125
1.2.7.1.3	Kök Sunucu Operatörleri	126
1.2.7.1.4	Diğer Kurumlar.....	126
1.2.7.2	İnternetin Uluslararası Yönetim Sorunu ve İnternet Yönetişimi .	127
1.2.7.2.1	İnternetin Uluslararası Yönetim Sorunu	127
1.2.7.2.2	İnternet Yönetişimi	132

İKİNCİ BÖLÜM

DÜNYADA İNTERNET İÇERİĞİNİN DÜZENLENMESİ: YAKLAŞIMLAR, YÖNTEMLER VE UYGULAMALAR

2.1	İÇERİK DÜZENLEMESİ TARTIŞMALARI, NEDENLERİ VE KONULARI.....	142
2.1.1	İçerik Düzenlemesine İlişkin Başlıca Tartışma Alanları.....	142

2.1.2	İçerik Düzenlemesinin Nedenleri ve Konuları	150
2.2	İÇERİK DÜZENLEMESİNDE TEMEL YÖNETİMSSEL YAKLAŞIMLAR	154
2.2.1	Devlet Düzenlemesi	154
2.2.2	Kendi Kendine/Öz Düzenleme	156
2.2.3	Birlikte / Ortak Düzenleme (Co-Regulation)	161
2.3	İÇERİK DÜZENLEMESİNDE TEMEL YÖNTEMLER	163
2.3.1	Filtreleme ve Erişim Engelleme Ve Engellemeyi Aşma Yöntemleri ..	164
2.3.1.1	Filtreleme ve Erişim Engelleme Yöntemleri	165
2.3.1.1.1	Teknik Açıdan Erişim Engelleme Yöntemleri	165
2.3.1.1.1.1	Engellemenin Kapsamına Göre	165
2.3.1.1.1.2	Engelleme Sistemine Göre	167
2.3.1.1.1.3	Kullanılan Tekniğe Göre	167
2.3.1.1.1.3.1	IP Yoluyla Engelleme.....	168
2.3.1.1.1.3.2	Alan Adı Yoluyla Engelleme.....	169
2.3.1.1.1.3.3	URL Yoluyla Engelleme	171
2.3.1.1.1.3.4	Proxy Yoluyla Engelleme	172
2.3.1.1.1.3.5	İçerik Engellemesi.....	172
2.3.1.1.1.3.6	DDOS Atakları.....	174
2.3.1.1.1.3.7	Alan Adı İptali Yolu ile Engelleme.....	174
2.3.1.1.1.3.8	Fiziksel Sunucu Müdahalesi Yoluyla Engelleme.....	175
2.3.1.1.1.3.9	Ağ Hatası Gösterme Yoluyla Engelleme.....	175
2.3.1.1.2	Sosyo-Ekonomik Açıdan Erişim Engellenme Yöntemleri	176
2.3.1.2	Filtreleme ve Erişim Engellemesini Aşmada Kullanılan Yöntemler	178
2.3.1.2.1	IP Değiştirme Yöntemi	179
2.3.1.2.2	Alan Adı Sunucusu Değiştirme Yöntemi.....	180
2.3.1.2.3	URL Gizleme Yöntemi	181
2.3.1.2.4	Proxy Kullanma Yöntemi.....	181
2.3.1.2.5	İçerik Aldatması Yöntemi	182
2.3.1.2.6	Kopya İçerik Kullanımı Yöntemi	183

2.3.1.2.7	Önbellek Kullanımı Yöntemi	184
2.3.2	Filtreleme ve Erişim Engelleme Dışındaki Pozitif Yöntemler	187
2.3.2.1	Uyar-Kaldır	187
2.3.2.2	Özel Anlaşmalar Yapma	189
2.3.2.3	Bilinçlendirme Faaliyetleri	192
2.3.2.4	İnternet Etiği Çalışmaları	195
2.3.2.5	Pozitif İçerik Oluşturma	197
2.4	İÇERİK DÜZENLEMESİNİN ÖLÇÜTLERİ	200
2.4.1	Açıklık	200
2.4.2	Şeffaflık	202
2.4.3	Kısıtlılık	203
2.4.4	Sorumluluk	205
2.5	DÜNYADA İÇERİK DÜZENLEMESİ UYGULAMALARI	211
2.5.1	Uluslararası Kuruluşlar	211
2.5.1.1	Avrupa Konseyi	212
2.5.1.1.1	Siber Suç Sözleşmesi	212
2.5.1.1.2	İnternette İletişim Özgürlüğü Deklarasyonu	214
2.5.1.1.3	Bilgi Toplumunda İnsan Hakları ve Hukukun Üstünlüğü Bakanlar Komitesi Bildirgesi	215
2.5.1.2	Avrupa Güvenlik ve İşbirliği Teşkilatı	216
2.5.1.3	Avrupa Birliği	217
2.5.1.3.1	Norm Oluşturma Çalışmaları: Kararlar, Tebliğler, Direktifler, Eylem Planları, Programlar	217
2.5.1.3.1.1	“Haberleşmede Hukuka Aykırı ve Zararlı İçerik” ve “Yeşil Kitap” Tebliğleri	218
2.5.1.3.1.2	Yasadışı ve Zararlı İçeriklerle İlgili Hükümet Temsilcileri Kararı	219
2.5.1.3.1.3	Güvenli İnternet Eylem Planları ve Programları	220
2.5.1.3.1.4	İnternette İfade Özgürlüğü Konusunda AP Kararı	221
2.5.1.3.1.5	E-Ticaret Direktifi	223
2.5.1.3.2	İçerik Düzenleme Politikası	225

2.5.2	Devletler	235
2.5.2.1	Amerika Birleşik Devletleri.....	235
2.5.2.1.1	Yasal Çerçeve	235
2.5.2.1.1.1	Müştehcen İçerikle Mücadele Yasaları	236
2.5.2.1.1.1.1	İletişim Ahlakı Yasası	237
2.5.2.1.1.1.2	Çocukların Online Yayınlarından Korunması Yasası	239
2.5.2.1.1.1.3	Çocukları İnternette Koruma Kanunu	240
2.5.2.1.1.2	Çocuk Pornografisi ve İstismarına İlişkin Yasalar	241
2.5.2.1.1.3	Terörizmle Mücadele Yasaları.....	242
2.5.2.1.1.4	Telif Hakkı İhlallerine İlişkin Yasalar.....	243
2.5.2.1.1.5	İnternette Kumarın Yasaklanması Yasası.....	244
2.5.2.1.2	İçerik Düzenleme Politikası	245
2.5.2.2	Avustralya	253
2.5.2.2.1	Yasal Çerçeve	254
2.5.2.2.1.1	Yayın Hizmetleri Yasası.....	254
2.5.2.2.1.2	Sınıflandırma Yasası	256
2.5.2.2.1.3	Sınıflandırma Yönergesi.....	258
2.5.2.2.2	İçerik Düzenleme Politikası	260
2.5.2.3	İngiltere.....	265
2.5.2.3.1	Yasal Çerçeve	266
2.5.2.3.2	İçerik Düzenleme Politikası	268
2.5.2.4	Fransa.....	276
2.5.2.4.1	Yasal Çerçeve	276
2.5.2.4.2	İçerik Düzenleme Politikası	282
2.5.2.5	Almanya.....	291
2.5.2.5.1	Yasal Çerçeve	291
2.5.2.5.2	İçerik Düzenleme Politikası	295
2.5.2.6	Rusya Federasyonu.....	304
2.5.2.6.1	Yasal Çerçeve	304
2.5.2.6.2	İçerik Düzenleme Politikası	306
2.5.2.7	Brezilya.....	311

2.5.2.7.1	Yasal Çerçeve	311
2.5.2.7.2	İçerik Düzenleme Politikası	312
2.5.2.8	Çin Halk Cumhuriyeti	319
2.5.2.9	Farklı Ülkelerin Önemli Bazı Uygulamaları	326

ÜÇÜNCÜ BÖLÜM

TÜRKİYE’DE İNTERNET İÇERİĞİNİN DÜZENLENMESİ VE TİB ÖRNEĞİ

3.1	TÜRKİYE’DE İNTERNETTEN KAYNAKLANAN SORUNLAR.....	337
3.1.1	Türkiye’de İnternetin Gelişimi ve Kullanımı	337
3.1.1.1	Türkiye’de İnternetin Gelişimi.....	337
3.1.1.2	Türkiye’de İnternet Kullanımı	339
3.1.2	Türkiye’de İnternetin Getirdiği Sorunlar	346
3.1.2.1	Toplumsal Sorunlar	347
3.1.2.1.1	Aile Üzerindeki Olumsuz Etkileri	347
3.1.2.1.2	Çocuklar ve Gençler Üzerindeki Olumsuz Etkileri	352
3.1.2.1.2.1	Cinsel İstismar, Pornografi ve Fuhuş	352
3.1.2.1.2.2	Siber Zorbalık	356
3.1.2.1.2.3	Şiddet, Nefret ve İntihara Yönlendirme	357
3.1.2.1.2.4	Kumar, Bahis, Şans Oyunları ve Uyuşturucuya Teşvik İçerikleri.....	358
3.1.2.1.2.5	İnternet Bağımlılığı	359
3.1.2.1.2.6	Dijital Oyunlar	360
3.1.2.1.2.7	Sosyal ağlar.....	361
3.1.2.2	Güvenlik Sorunu ve Mahremiyet İhlali	363
3.1.2.3	İnternet Kafeler	365
3.2	TÜRKİYE’DE İNTERNET İÇERİK DÜZENLEMESİNİN TARİHÇESİ.....	367
3.2.1	5651 Sayılı Kanun Öncesi	367
3.2.1.1	Yasal Düzenlemeler	368
3.2.1.2	Kurumsal Yapılar	371
3.2.1.3	Bilgi Toplumu Çalışmaları ve e-Dönüşüm Türkiye Projesi	374
3.2.1.3.1	Kısa Dönem Eylem Planı (2003-2004).....	374
3.2.1.3.2	“Bilgi Toplumuna Dönüşüm Politikası” Belgesi.....	375

3.2.1.3.3	Eylem Planı (2005)	376
3.2.1.3.4	Bilgi Toplumu Stratejisi (2006-2010).....	377
	Bilgi Toplumu Stratejisi (2006-2010) Eylem Planı	380
3.2.1.4	Uygulamalar.....	382
3.2.2	5651 Sayılı Kanun'un Gelişimi	385
3.2.2.1	Bilişim Ağı Hizmetlerinin Düzenlenmesi Ve Bilişim Suçları Hakkında Kanun Tasarısı.....	386
3.2.2.2	Bilişim Sistemi Üzerinden Suç Teşkil Eden Zararlı Yayınlarla Mücadele Hakkında Kanun Teklifi	392
3.2.2.3	5651 Sayılı Kanun'un TBMM Süreci	394
3.2.2.3.1	Genel Gerekçe	394
3.2.2.3.2	Adalet Komisyonu Çalışmaları	397
3.2.2.3.3	TBMM Müzakereleri	402
3.3	5651 SAYILI KANUN VE TİB SONRASI	409
3.3.1	5651 Sayılı Kanun Sonrası Oluşan Hukuki Çerçeve	409
3.3.1.1	5651 Sayılı Kanun'un Getirdiği Hükümler	410
3.3.1.2	Katalog Suçlarına İlişkin Yasalar.....	417
3.3.1.2.1	İntihara Yönlendirme	417
3.3.1.2.2	Çocukların Cinsel İstismarı	419
3.3.1.2.3	Uyuşturucu veya Uyarıcı Madde Kullanılmasını Kolaylaştırma	420
3.3.1.2.4	Sağlık İçin Tehlikeli Madde Temini	423
3.3.1.2.5	Müstehcenlik	424
3.3.1.2.6	Fuhuş	432
3.3.1.2.7	Kumar Oynanması İçin Yer ve İmkan Sağlama	433
3.3.1.2.8	Sabit İhtimalli Veya Müşterek Bahis Oynatılması	435
3.3.1.2.9	Atatürk Aleyhine İşlenen Suçlar.....	436
3.3.1.3	İkincil Düzenlemeler	438
3.3.1.3.1	Erişim Sağlayıcılara ve Yer Sağlayıcılara Faaliyet Belgesi Verilmesine İlişkin Usul ve Esaslar Hakkında Yönetmelik.....	439
3.3.1.3.2	İnternet Toplu Kullanım Sağlayıcıları Hakkında Yönetmelik.....	443

3.3.1.3.3	İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik	445
3.3.1.3.4	Elektronik Haberleşme Sektörüne İlişkin Yetkilendirme Yönetmeliği	449
3.3.1.3.5	Elektronik Haberleşme Sektöründe Tüketici Hakları Yönetmeliği	450
3.3.1.3.6	Bilgi Teknolojileri ve İletişim Kurumu Teşkilat Yönetmeliği	450
3.3.2	İnternet İçerik Düzenlemesi İle İlgili Kurumlar	451
3.3.2.1	Ulaştırma, Denizcilik ve Haberleşme Bakanlığı.....	451
3.3.2.2	Bilgi Teknolojileri ve İletişim Kurumu	453
3.3.2.3	Telekomünikasyon İletişim Başkanlığı	457
3.3.2.4	İnternet Geliştirme Kurulu.....	459
3.3.2.5	Çocuk ve Aile Profil Kriterleri Çalışma Kurulu	460
3.3.2.6	Küçükleri Muzır Neşriyattan Koruma Kurulu	461
3.3.2.7	Sinema Genel Müdürlüğü Değerlendirme ve Sınıflandırma Kurulu	463
3.3.2.8	Radyo ve Televizyon Üst Kurulu.....	465
3.3.2.9	Bilgi Toplumu Dairesi Başkanlığı.....	470
3.3.2.10	Aile ve Toplum Hizmetleri Genel Müdürlüğü.....	471
3.3.3	5651 Sayılı Kanun'un ve TİB'in Uygulamaları	474
3.3.3.1	İnternet Bilgi İhbar Merkezi	474
3.3.3.2	Erişim Engelleme Uygulamaları	478
3.3.3.3	İçeriğin Yayından Çıkarılması Uygulamaları.....	490
3.3.3.4	Güvenli İnternet Hizmeti Uygulaması.....	492
3.3.3.5	İçerik Filtreleme Uygulamaları	496
3.3.3.6	Yetkilendirme Uygulamaları	497
3.3.3.7	İnternetin Güvenli Kullanımı Uygulamaları.....	499
3.3.3.8	Koordinasyon Çalışmaları	502
3.3.3.9	İçerik Düzenlemesi Ölçütleri ve Türkiye Uygulaması.....	507
	GENEL DEĞERLENDİRME	519
	SONUÇLAR.....	590

KAYNAKÇA	618
EK-1: ÖNERİLER	692
A. Politikalar	692
1. Bütüncül Bilgi Toplumu ve İnternet Strateji ve Politikaları Oluşturulması	692
2. İnternetin Sosyal Boyutu İle İlgili Araştırmalara Olan İhtiyaç	695
3. İnternet Yönetişiminin Gerçekleştirilmesi	697
4. İnternet İçerik Güvenliği İçin Özel Bütçe Oluşturulması	698
5. Pozitif Yerli İçerik Oluşturulmasının Teşvik Edilmesi	698
6. Bilinçlendirme Çalışmalarının Artırılması	701
7. Küresel Şirketler İle Özel Anlaşmalar Yapma	703
8. Erişim Engelleme Politikasının Gözden Geçirilmesi	704
9. Öz Düzenleme Uygulamalarının Teşvik Edilmesi	707
10. İnternet STK'larının Güçlendirilmesi	709
11. Yer Sağlayıcılığın Geliştirilmesi ve Kayıt Altına Alınması	711
12. Yaş Doğrulama Uygulamasının Genişletilmesi	712
13. İnsan ve Toplum Merkezli Yaklaşım	713
14. Tüketicilere Seçme ve Tercihle Bulunma Özgürlüğü Sunulması	715
15. "İnternet Erişim Hakkı" ve "İçerik Seçme Hakkı"na Anayasal Güvence..	716
B. Kurumsal Yapılar	717
1. Bilişim ve Yayıncılık/Bilişim Bakanlığı	717
2. Bilgi Teknolojileri, İletişim ve Yayıncılık/Bilişim Kurumu	719
3. İnternet İçerik Güvenliği Başkanlığı	720
4. İnternet Geliştirme Kurulu	724
5. Sınıflandırma Kurumu	726
6. İnternet Etik Kurulu	728
7. İnternet Arabuluculuk Kurulu	729
8. Veri Değerlendirme ve Analiz Dairesi Başkanlığı	730
9. İhbar Merkezi	731
10. Yardım Hattı	735
11. İhtisas Mahkemeleri	736
EK-2: MÜLAKAT SORULARI	737

KISALTMALAR

ACA	Australian Communications Authority
ACLU	American Civil Liberties Union
ACM	Association for Computing Machinery
ACMA	Australian Communications and Media Authority
ADSL	Asymmetric Digital Subscriber Line
AFA	Association Des Fournisseurs D'accès Et De Services Internet
AFRINIC	African Network Information Centre
AITP	The Association of Information Technology Professionals
ALIA	Australian Library and Information Association
APNIC	Asia Pacific Network Information Centre
ARIN	American Registry for Internet Numbers
ARJEL	L'autorité De Régulation Des Jeux En Ligne
ARPANET	Advanced Research Project Authroty Net
ASAGEM	Aile ve Sosyal Araştırmalar Genel Müdürlüğü
ATHGM	Aile ve Toplum Hizmetleri Genel Müdürlüğü
BBFC	British Board Of Film Classification
BCS	British Computer Society
BpiM	Bundespruffstelle Für Jugendgefarhdende Medien
BT	British Telecom
CDA	Communications Decency Act
CDN	Content delivery network
CEOP	Child Exploitation And Online Protection Centre

CERN	Centre Européen Recherces Nucléaires
CHI	Child Helpline International
CIIRC	China Internet Illegal Information Reporting Centre
CIPA	Children's Internet Protection Act
CNIL	Commission Nationale De L'informatique Et Des Libertés
CNN	Conseil National Du Numérique
COP	Child Online Protection
COPA	Child Online Protection Act
CSA	Conseil Supérieur De L'audiovisuel
CSAM	Child Sexual Abuse Material
CVIP	Child Victim Identification Program
DADVSI	Loi Sur Le Droit D'auteur Et Les Droits Voisins Dans La Société De L'information
DDOS	Distributed Denial of Service
DMCA	The Digital Millennium Copyright Act
DUI	Délégation Aux Usages De l'Internet
DYY	Forum Des Droits Sur L'internet
EARN	European Academic and Research Network
ECO	Verband Der Deutschen Internetwirtschaft e.V.
ESRB	Entertainment Software Rating Board
FCACP	Financial Coalition Against Child Pornography
FCC	Federal Communications Commission
FOSI	Family Online Safety Institute
FSB	Federal'naya Sluzhba Bezopasnosti

FSM	Herzlich Willkommen Auf Der Website Der Freiwilligen Selbstkontrolle Multimedia
GAC	Governmental Advisory Committee
GIC	Global Internet Council
GIPC	The Global Internet Policy Council
GPRS	General Packet Radio Service
HADOPI	Haute Autorité Pour La Diffusion Des Oeuvres Et La Protection Des Droits Sur Internet
HRW	Human Rights Watch
IAB	Internet Architecture Board
IAHC	Internaitonal Ad-Hoc Committee
IANA	Internet Assigned Numbers Authority
ICAC	Internet Crimes Against Children Task Forces
ICANN	Internet Corporation for Assigned Names and Numbers
ICE	Immigration and Customs Enforcement
ICRA	Internet Content Rating Association
IEEE	The Institue of Electrical and Electronics Engineer
IESG	Internet Engineering Steering Group
IETF	Internet Engineering Task Force
IGF	Internet Governance Forum
IIC	International Internet Council
INACH	International Network Against Cyberhate
INCB	International Narcotics Control Board
INETD	İnternet Teknoloji Derneği

INHOPE	The International Association of Internet Hotline Providers
INSAFE	European Safer Internet Network
IRTF	Internet Research Task Force
ISFE	Interactive Software Federation of Europe
ISOC	Internet Society
ISPA-UK	Internet Service Providers Association of United Kingdom
ITU	International Telecommunication Union
IWF	Internet Watch Foundation
JANET	Joint Academic Network
JMStV	Jugendmedienschutz-Staatsvertrag
KCSC	Korea Communications Standards Commission
KJM	Kommission Für Jugendmedienschutz Landesmedienanstalten
LCEN	Pour La Confiance Dans L'économie Numérique
LICRA	League Against Racism and Anti-Semitism
Loppsi	Programmation Pour La Performance De La Sécurité Intérieure
MDA	Media Development Authority
NAP	Network Access Point
NCMEC	The US National Center For Missing And Exploited Children
NICAM	Netherlands Institute for the Classification of Audiovisual Media
NSF	National Science Foundation
NSFNet	National Science Foundation Network
NSI	Network Solutions Inc.
NTIA	The Telecommunications and Information Administration

ONI	OpenNet Initiative
PEGI	Pan-European Game Information
PICS	The Platform for Internet Content Selection
PNVD	Partij voor Naastenliefde, Vrijheid en Diversiteit
RIPE NCC	Reseaux IP Europeens Network Coordination Centre
RSF	Reporters Without Borders
SOME	Siber Olaylara Müdahale Ekipleri
TBD	Türkiye Bilişim Derneği
TBV	Türkiye Bilişim Vakfı
TDG	Teledienstegesetz
TİD	Tüm İnternet Derneği
TUBİDER	Bilişim Sektörü Derneği
TÜBİSAD	Türkiye Bilişim Sanayicileri ve İşadamları Derneği
TÜDOF	Türkiye Dijital Oyunlar Federasyonu
UCL	University College London
UIGEA	Unlawful Internet Gambling Enforcement Act
UKIE	The Association For UK Interactive Entertainment
UKSIC	UK Safer Internet Centre
USK	Unterhaltungssoftware Selbstkontrolle
USOM	Ulusal Siber Olaylara Müdahale Merkezi
WGIG	The Working Group on Internet Governance
WIPO	World Intellectual Property Organization
WSIS	The World Summit on the Information Society

TABLolar LİSTESİ

Tablo 1.1. 1995 ve 2012 yıllarında en çok İnternet kullanıcıısına sahip ülkeler ..	10909
Tablo 1.2. Dünya genelinde en çok İnternet kullanıcıısına sahip ilk 20 ülke.....	11010
Tablo 1.3. Dünyada bölgesel olarak İnternet kullanıcı ve nüfus istatistiği	11111
Tablo 3.1. Türkiye’de Cinsiyete Göre İnternet Kullanıcı Oranları(%)	340
Tablo 3.2. Türkiye’de Yaş Gruplarına Göre İnternet Kullanıcı Oranları (%)	340

ŞEKİLLER LİSTESİ

Şekil 2.1. Ülkelerin İnternete müdahale nedenleri.....	15151
Şekil 2.2. Bilgi İletişim Etiği Komitesi SafeNet Değerlendirme Standartları.....	33131
Şekil 2.3. Bilgi İletişim Etiği Komitesi SafeNet Yaş Gruplarına Göre Tavsiyeler	33131

GİRİŞ

Bu kısımda tezin cevap bulmak istediği temel ve alt problemler, amacı, çalışma yapılırken nasıl bir yöntem takip edildiği, materyalleri, sınırlılıkları ve son olarak da, temel hipotezi ve alt hipotezleri ortaya konulmuştur.

I. Problem

İçinde bulunduğumuz döneme bilgi çağı denilmesinin temel nedenlerinden birisi elektronik sahasında yaşanan gelişmelerin en önemlisi olan İnternetin kullanıma açılması olmuştur. Bu gün 2.5 milyar kullanıcı sayısına ulaşan İnternetin temsil ettiği bilişim devriminin Dünyayı “Sanayi toplumu”ndan “Bilgi toplumu” aşamasına taşıdığı görülmektedir. Hatta bu yeni dönem için “Ağ toplumu” (Castells, 2008: 621), “İnternet toplumu” (Uğur ve Bilici, 1998: 449), “siber toplum” (Subaşı, 2005: 108) gibi kavramlar da kullanılmaktadır.

Başlangıçta ABD’de soğuk savaş döneminde savunma sisteminin parçası olarak geliştirilen ARPANET isimli askeri bir projenin daha sonra sivil kullanıma açılması, insanların hayatında, birbiriyle, içinde yaşadığı çevre ve toplum ile, bağlı bulunduğu devletle ve diğer toplum ve devletlerle ve hatta tüm dünya ile ilişkilerinde bir dizi değişiklik meydana getirmiştir.

İnternetin kendisinden önceki tüm iletişim araçlarının fonksiyonlarına sahip olması (telgraf, telefon, televizyon gibi), etkileşimli olması (on-line olarak iletişim sağlaması), coğrafi sınırları ortadan kaldırması, multimedya içeriğin dünyanın herhangi bir yerinden başka bir yerine saniyeler içinde ulaşabilmesi, web teknolojilerindeki gelişmeler sayesinde bu iletişimin güvenli ve kriptolu olarak yapılabilmesi gibi olanaklar sunması daha önce görülmemiş derecede kapsamlı bir teknoloji ile karşı karşıya kalındığını göstermektedir (Altınok, 2008: 1).

Süreç içerisinde bu teknolojinin daha büyük bir hızla gelişim göstermesi, bilginin çok daha hızlı ve ucuz bir şekilde yayılmasına olanak sağlarken, hayatın her alanında etkilerini güngeçtikçe daha da artıran büyük bir değişime neden olmaktadır. Bu

durum bir bütün olarak geleneksel toplumsal, ekonomik, siyasi ve kültürel yapıyı etkileyerek köklü değişim ve dönüşümlerin önünü açmaktadır. Doğal olarak bu değişim ve dönüşümler yeni yönetsel ve hukuksal sorunlar ortaya çıkarmaktadır.

Bu yeni süreçte İnternetin iletişim, bilgi edinme ve paylaşım gibi iyi amaçlarla kullanılması yanında, bir suç aracı olarak kullanılması ve barındırdığı yasadışı ve zararlı içeriklerden kaynaklanan sorunlar giderek yaygınlaşmaktadır. Bu çerçevede, bilişim teknolojilerinden faydalanarak gücünü ve etkinliğini artıran terör ve suç örgütlerinin faaliyetlerini bu ortama taşınması, bilgi hırsızlığı ve dolandırıcılık gibi suçların bu ortamda işlenmeye başlanması, özel hayatın gizliliğine ve kişilik haklarına saldırı niteliğindeki yayınların İnternette giderek çoğalması, bahis, kumar ve fuhuş için İnternetin yeni olanaklar sunması ile çocukların cinsel istismarı, pornografik içerik, şiddet, ırkçılık gibi yasadışı ve zararlı yayınların giderek artması İnternetin kötü amaçla kullanılabileceğini açıkça gözler önüne sermiştir.

Bu durum, esas itibarıyla özgür bir alan olduğu düşünülen İnternet ortamında işlenen suçlar ve yaşanan olumsuzluklarla ilgili olarak erişimin engellenmesine kadar varan bir takım yaptırımları ve bu alanla ilgili yükümlülük ve sorumlulukların düzenlenmesi konusunu gündeme getirmiştir. Buna karşılık, İnternetin kendine özgü yapısı ve teknik özellikleri bakımından kontrol ve denetime elverişsiz olması yanında, bugüne kadar düşünce özgürlüğünün tam ve doğrudan geçerli olduğu ve kolaylıkla kullanılabildiği tek alanın İnternet olduğu ve filtrelenebilir ve denetlenmesiyle özgürlükçü yapısının bozulacağına yönelik itirazlar olmuştur.

Özellikle, bu düzenlemelerin devlet eli ile yapılması ise, bir kısım İnternet kullanıcıları, uzmanlar ve hukukçular tarafından bunun bir “sansür” olacağı; ifade özgürlüğü ve bilgiye erişim özgürlüğü ile bağdaşmadığı, bilgi ve düşüncenin serbest dolaşımına engel olacağı yönünde ciddi eleştirilerle karşılaşmaktadır. Bu eleştirilerin ortaya çıkmasında, İnternetin, bireysel bir kullanım ve iletişim aracı olması özelliğinin yanı sıra aynı zamanda günümüzün en önemli kitle iletişim aracı olarak da işlev görmesi; web siteleri aracılığıyla her türlü düşüncenin açıklanması ve

propagandasının yapılması, İnternet gazeteciliği aracılığıyla her türlü haberin anında geniş halk kitlelerine duyurulmasının mümkün olmasının önemli bir etkisi vardır.

Öte yandan, İnternetin diğer kitle iletişim araçlarından farklı olan özellikleri; çok boyutlu, çok aktörlü ve dinamik olması, tekniği, alt yapısı, işleyiş biçimi ve uluslararası niteliği, suç yeri ve zamanı, sorumlu olabilecek kişiler vb. yönünden diğer yayıncılık türleri ile bağdaşmayan kendine has özelliklere sahip olması nedeniyle, İnternetin kim tarafından, nasıl ve hangi konular kapsamında düzenlenmesi gerektiği, hatta İnternet üzerinde bir düzenlemenin mümkün olup olmayacağı gibi konular tüm dünya ülkelerinde yakın dönemin önemli tartışma konularından birisi olarak güncelliğini sürdürmektedir.

Buna karşın, İnternetin tüm toplum ve özellikle çocuklar, gençler ve aileler için oluşturduğu risk ve tehlikelerin bertaraf edilmesi ve İnternetin güvenli kullanımının sağlanması amacıyla ya da farklı ekonomik ve siyasal nedenlerle ülkelerin, giderek artan bir oranda, İnternet içeriğiyle ilgili “önlem” ve “müdahaleleri” kapsayan düzenlemeler yapmakta oldukları görülmektedir. Bu durum, özellikle düzenlemelerin “yöntemi” ve “kapsamı” konusundaki tartışmaları daha da büyötmektedir.

“Yöntem”e ilişkin temel görüş ayrılığı, içerik düzenlemelerinin doğrudan devlet eliyle mi, yoksa sivil inisiyatif tarafından mı, ya da her ikisinin birlikte mi yapmasının ve uygulamasının uygun olacağı noktasında ortaya çıkmaktadır. Dolayısıyla, tartışmaların merkezinde, İnternet içeriğinin düzenlenmesinde ve uygulamasında devletin rolü konusu yer almaktadır. Bu bağlamda, “Devlet İnternet içeriğine ilişkin önlem alma ve müdahalede bulunma konusunda aktif rol almalı mı? Düzenleme ve uygulamaların neresinde olmalı?” soruları etrafında tartışmalar yoğunlaşmaktadır.

“Kapsam” konusunda ise, içerik düzenlemesinin sınırları hususunda ihtilaflar yaşanmakta; hangi içerik türlerinin, hangi sınırlar içerisinde düzenlemelere konu edilmesinin uygun olacağı tartışılmaktadır. Yani, yasadışı ve zararlı olarak kabul edilerek önlem alınacak ve mücadele edilecek içerik türleri hangileri olmalıdır,

bunlar ne oranda sınırlandırılmalıdır ve bunları belirleyecek ölçütler neler olmalıdır gibi soru ve sorunlara cevap bulunmaya çalışılmaktadır.

Diğer yandan, İnternet, kendisini denetim ve kontrol altına almaya çalışan ulus devletler için bazı zorluklar meydana getirmiştir. Bu zorlukların en önemlisi de İnternetin, klasik ulusal egemenlik anlayışlarına meydan okuyan karmaşık, çok değişkenli, dinamik ve sınır tanımayan küresel yapısıdır. Devletlerin ülke sınırları içerisinde vatandaşlarına hukuk kuralı koyma ve bunu uygulama meşruiyetlerini esas alan klasik ulusal egemenlik yaklaşımları, ulusal sınır tanımayan bu teknoloji karşısında çoğu zaman geçersiz kalmaktadır. Dolayısıyla, İnternet teknolojisi bugün “egemenlik” kavramını yeniden düşünmeye mecbur kılmakta ve İnternetin düzenlenmesi konusu “düzenleme” ve “devletin egemenlik yetkisi” kuramlarının temelden sorgulandığı bir mecraya doğru ilerlemektedir (Beceni, 2004: 5).

İnternetin, ulus devletleri zor durumda bırakan bu yapısı, sorunun İnternetin uluslararası yönetimi ve işbirliği boyutunu tartışmaya açmaktadır. Nitekim, İnternetin yönetiminden sorumlu, yaptırım uygulamaya yetkili uluslararası meşruluğu olan merkezi bir örgütün bulunmaması ve bu boşluğun daha çok İnternetin mucidi olan ABD tarafından kendi ulusal çıkarlarına göre doldurulması, diğer önemli bir sorun olarak uluslararası düzeyde tartışılmaktadır.

Kısaca, ulusal ve uluslararası boyutlarıyla İnternet içerik düzenlemesinin nedenleri ve konuları, uygulanan modeller, ölçütler, ülkelerin konuya yaklaşımları, hukuksal ve örgütsel yapılar ve bunların işleyişleriyle ilgili konular az gelişmiş, gelişmekte olan veya gelişmiş tüm ülkelerin önemli bir sorunu olarak gündemdeki yerini muhafaza etmektedir. Nitekim, İnternet içeriğine müdahelenin nedenleri, kapsamı ve yöntemlerine ilişkin belirsizlikler, komünist düzene sahip Çin’de olduğu kadar, AB ülkeleri olan Almanya ve Fransa’da da bir sorun olarak tartışılmaktadır (Ronald Deibert vd., 2008: 33).

Dünyada yaşanan bu gelişme ve tartışmaların benzerleri ülkemizde de görülmektedir. Zira, Türkiye özellikle genç nüfusu ve girişimci özel sektörü eliyle bilişim ve bilgi

teknolojileri alanında hızlı bir gelişme göstermektedir. 40 milyona yaklaşan İnternet kullanıcı sayısı bu gelişmenin bir göstergesidir. Bu nedenle, tüm dünyada olduğu gibi ülkemiz de İnternetin başını çektiği bilişim teknolojilerindeki gelişmelerin tetiklediği bu değişim ve dönüşümden etkilenmektedir. Dolayısıyla, bu süreçte yaşanan bir takım problemler, sorunlar ve sancılar Türkiye için de söz konusu olmaktadır. Bu bağlamda, Dünya ile paralel olarak, bilişim suçları ile yasadışı ve zararlı İnternet içeriğiyle mücadele edilmesi, İnternet ortamında yapılan yayınların düzenlenmesi ve filtreleme konuları tartışılmakta ve bazı uygulamalar geliştirilmektedir.

Bu çerçevede, 4.5.2007 tarihinde çıkarılan 5651 sayılı “İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun” ve bu kanununla düzenlenen konularla ilgili görevli kamu kurumu olarak ortaya çıkan Telekomünikasyon İletişim Başkanlığı (TİB) İnternet Dairesi söz konusu tartışmaların merkezinde yer almıştır. TİB, kuruluşundan sonra mahkeme kararıyla da olsa YouTube ve Geocities gibi uluslararası üne sahip İnternet sitelerinin erişimine engel olmasıyla ve İnternet içeriğinin düzenlenmesi konularında yapmış olduğu diğer uygulamalarla tartışılmaya devam etmektedir.

Bu kapsamda, tezde tüm bu soru/sorun alanlarını içine alacak şekilde ele aldığımız temel problem, “İnternet içerik düzenlemesi sorunu ve çözümü”dür. Ayrıca, bu kapsamda “Türkiye’de İnternet içerik düzenlemesi sorunu ve çözümü” genel problem perspektifinde ele alınmıştır. Yani, tezde konu edindiğimiz temel problem “İnternet içerik düzenlemesi sorununun mahiyeti nedir ve nasıl çözülür? Türkiye bu işin neresindedir?” sorusuna cevap bulmaktır. Bir başka deyişle, tezde, İnternette yer alan yasadışı ve zararlı içeriklerin önlenmesi ve bu tür içeriklerle mücadele edilmesi kapsamında yapılan düzenlemelerle ilgili gündeme gelen sorunlar ve bunların çözüm yollarını içine alan güncel temel probleme cevap verilmeye çalışılmıştır.

Bu bağlamda tezde, söz konusu temel probleme bağlı olarak; sorunun bilgi toplumu bağlamı, içerik düzenlemesinin gerekliliği, içerik düzenlemesi sorununun mahiyeti, boyutları, değişkenleri, dinamikleri, sınırlılıkları, çözümünün koşulları, içerik düzenlemesinin mümkün olmasının şartları, içerik düzenlemesinin nedenleri,

konuları, ölçütleri, yöntemleri, çözüm yolları, tartışma alanları, ülkelerin konuya yaklaşımları, strateji ve politikaları, hukuksal ve örgütsel yapıları, uygulamaları gibi alt problem alanlarına tez içinde cevap bulunmaya çalışılmıştır. Keza, tüm bu problem alanlarının Türkiye örneğindeki yeri ve karşı cevapları da araştırılarak, söz konusu alt problem alanlarına ilişkin verilen cevaplar bütününden, tezin temel probleminin cevabı oluşturulmuştur.

II. Amaç

BBC'nin 26 ülkede 27 bin kişiyle yaptığı bir araştırmada, Avrupa'da İnterneti hak olarak görenlerin en yüksek olduğu ülke, %90'ı geçen bir oranla Türkiye olmuştur (BBC, 08.03.2010a). Buna karşılık, İnterneti güvenli bulma konusunda Türkiye'den katılan kullanıcıların ikiye ayrıldığı görülmektedir. Güvenli olduğuna inananların oranı %46 iken, güvenli bulmayanların oranı %50'dir (BBC, 08.03.2010b). Bu sonuçlardan Türk vatandaşlarının İnterneti bir hak olarak gördüğü fakat güvenli bulmadığı sonucunu çıkartmak mümkündür.

Diğer yandan, toplumların gelişimlerinde etkili bir araç olduğu bilinen İnternetin değeri/önemi hükümetler, toplumlar ve bireyler açısından her geçen gün artmaktadır. Bu durum, tüm hükümetlerin önüne zor ve karmaşık bir görev çıkartmaktadır. O da, İnternetin sunduğu engin fırsatlardan en yaygın ve etkin biçimde yararlanılmasını sağlamak ile vatandaşların ve toplumun bunun getireceği risklerden ve tehlikelerden korunması arasında bir denge tutturulmasını sağlamak sorumluluğudur.

Ülkemiz ve insanlık için kritik öneme sahip İnternetin sağladığı büyük olanak ve fırsatların ıskalanmaması, doğru anlaşılması, isabetsiz ve yanlış karar ve uygulamalara konu edilmemesi, doğru yönetilmesi ile mümkündür. Bu bağlamda özellikle kamu otoritelerinin, genel olarak İnternet olgusunu, özel olarak ise bunun bir parçası olarak içerik düzenlemesine ilişkin konuları nasıl ele almaları gerektiği konusu ciddi bir sorun olarak karşımızda durmaktadır. Tezin amacı, bu kritik sorunu diğer ülkeler ve ülkemizdeki uygulamaları ve teorik tartışmalarıyla birlikte derinlemesine irdeleyerek, soruna ilişkin çözümler üretmeye çalışmaktır.

III. Yöntem

Teze konu araştırmada nitel araştırma yöntemlerinden “doküman inceleme” ve “mülakat” yöntemi kullanılmıştır. Buna göre, doküman incelemesi yaklaşımına uygun olarak, öncelikle ön bir kaynak taraması yapılarak konuyla ilgili olabilecek tüm basılı ve dijital ortamdaki yazılı, sesli ve görüntülü birincil ve ikincil kaynaklar gözden geçirilmiştir. Daha sonra, bunlar içerisinde özel olarak İnternet içerik düzenlemesi konusunu ele almış kaynaklar incelenerek elde edilen veriler, şekiller ve tablolarla desteklenerek gerekli karşılaştırmalar yapılarak analitik yaklaşımlarla analiz edilmiş ve yorumlanmıştır. Böylece, temel problem ve alt problem alanları netleştirilmiş ve konunun sınırları çizilmiştir. Akabinde, benzer bir yöntemle mevcut kaynakların tekrar gözden geçirilmesi ve konuyla ilgili uzmanlarla yapılan görüşmeler neticesinde elde edilen verilerin analizi ve yorumlanması sonucu ulaşılan bulgular ile temel probleme ve alt problemlere cevap teşkil edebilecek temel hipotezler ve alt hipotezler oluşturulmuştur.

Bu aşamadan sonra, tüm problem ve hipotezler çerçevesinde tez konusu ile ilgili ulaşılabilen tüm Türkçe ve İngilizce kaynaklar detaylı olarak taranmış ve derinlemesine incelenmiştir. Bu çerçevede, Dünyada ve Türkiye’de bu alanda yapılmış yazılı, işitsel ve görsel yayınlar incelenmiş, teorik tartışmalar, uygulamalar ve bunlara ilişkin eleştiriler gözden geçirilmiştir. Özellikle, konuyla ilgili dünyadaki eğilimleri ortaya çıkartabilmek ve ülkelerin tecrübelerinden faydalanabilmek için uluslararası örgütler ve dünyanın farklı bölgelerinde yer alan ve İnternet toplumu için farklı yönleri ile önem taşıyan ülkelerin içerik düzenlemeye ilişkin oluşturdukları hukuki çerçeve, örgütsel yapılar ile politika ve uygulamaları ayrı ayrı incelenmiştir. Bu kapsamda 22 ülke incelemesi yapılmıştır.

Daha sonra, tüm bu süreçte elde edilen verilerin analizi ve değerlendirilmesiyle elde edilen bilgi, düşünce, yaklaşım, tespit ve sonuçlarla Türkiye örneğini karşılaştırmak için konunun Türkiye boyutuna nüfuz edilmeye çalışılmıştır. Bu kapsamda, konu ile ilgili teorik tartışmalar ve uygulama alnındaki düşünce, değerlendirme, beklenti ve gelişmeleri saptamak ve derinlemesine analize olanak sağlamak amacıyla, içerik

düzenlemeleriyle ilgili kamu kurumlarının yöneticileriyle ve konunun uzmanı olan kişilerle mülakat çalışması yapılmış ve elde edilen düşünce, fikir, görüş ve öneriler toplanarak değerlendirilmiştir. Bu kapsamda, 2 yönetici ve 5 uzman ile yüz yüze ve zamanla sınırlı olmayan “derinliğine görüşme” gerçekleştirilmiştir.

Keza, mülakat çalışması kapsamında kendileriyle görüşme yapılmış olan yönetici ve uzmanların dışında, TİB, BTK, Bilgi Toplumu Dairesi, Başbakanlık E-Devlet Çalışma Grubu, İnternet sektörü ve konuyla ilgili akademisyenlerden onlarca kişi ile de ayrıca yüz yüze, telefonla veya İnternet üzerinden “sınırlı görüşmeler” yapılmıştır. Özellikle, 5651 sayılı Yasa’nın ilk hazırlık aşamasından itibaren TBMM safahatında komisyonlarda görev alan, yasalaşmasından sonra TİB İnternet Dairesi’nin kurulmasında ve sonrasında uygulamanın sürekli içinde bulunan, tüm süreçlere, olaylara, tartışmalara bizzat tanıklık yapmış birçok kişi ile görüşülmüş ve kendilerinden bilgiler, görüşler ve değerlendirmeler alınmıştır.

Son olarak, eldeki tüm veriler, kurgulanan tez sistematığı içinde, temel hipotez ve alt hipotezlerin değerlendirilmesine olanak tanıyacak şekilde yazılı hale getirilmiştir. Yazım aşamasında temel hipotez ve alt hipotezler mevcut veriler çerçevesinde tartışılmış, doğrulukları ve geçerlilikleri ölçülmeye ve test edilmeye çalışılmıştır. Bu yolla elde edilen neticeler çalışmanın sonuç bölümünde kayıt altına alınmıştır. Böylece, temel hipotez ve alt hipotezler çerçevesinde tezin konusunu teşkil eden İnternet içerik düzenlemesi sorunu, derinlemesine analiz edilebilme ve buna göre sonuçlara ulaşılma imkanı bulmuştur. Bilahare elde edilen sonuçlara göre Türkiye için öneriler sunulmuştur.

Araştırmada, alt hipotezler etrafında İnternet içerik düzenlemesi sorunu ve çözümüyle ilgili olarak göz önünde bulundurulması ve değişken olarak hesaba katılması gereken tüm konu, aktör, boyut, unsur ve belirleyicilere değinilerek, adeta konuyla ilgili hassasiyeti ve etkisi olabilecek tüm sinir uçları meydana çıkartılmaya çalışılmış ve söz konusu her bir değişken için değerlendirmeler yapılarak ortaya çıkan görüşler ile temel hipotezin örgüsü tamamlanmıştır. Bu kapsamda mevcut durum, bir kamu yönetimi sorunu boyutuyla politikalar, düzenlemeler, uygulamalar

ve örgütsel yapılar temelinde irdelenmiş ve elde edilen sonuçlar bağlamında aynı düzlem kullanılarak geleceğe yönelik projeksiyonlar ve öneriler geliştirilmiştir.

Çalışmada İnternet içerik düzenlemesi sorununun gerçek boyutları ile anlaşılabilmesi için söz konusu sorununun yaslandığı bilgi toplumu ve İnternet olgusunun tarihsel ve kuramsal arka planına mercek tutulmuş ve çalışma boyunca bu iki olgu mümkün olduğunca nesnel, tarafsız ve dengeli bir şekilde ele alınmaya çalışılmıştır. Bunun için çalışmada, popüler söylemin kolaycılığına teslim olmamak adına, bilgi toplumu ve İnternet fetişizmi yapmaktan mümkün olduğunca uzak kalınmaya gayret edilmiştir. Bu nedenle, hakim görüşün aksine, genellikle kamufle edilmeye çalışılan İnternetin riskler, tehlikeler ve sorunlar boyutuna sık sık vurgu yapılarak ve sorunun sosyal maliyetler boyutuna dikkat çekilerek, İnternet içerik düzenlemesi sorununu ortaya koyan gerçeğe en yakın fotoğraf karesi yakalanmaya çalışılmıştır.

IV. Materyaller

Tez çalışmasında, oluşturulan temel ve alt hipotezleri test etmeye yarar verileri elde edebilmek amacıyla, ulaşılabilen tüm Türkçe ve İngilizce birincil ve ikincil kaynaklar kullanılmıştır. Bu kapsamda basılı ve dijital ortamdaki ulaşılabilen tüm yazılı, sesli ve görüntülü kaynaklar; kamu kurumlarının, özel sektör kuruluşlarının, STK'ların ve üniversitelerin yayınlanmış raporları, bilimsel tezler, uzmanlık tezleri, kitaplar, dergiler, makaleler, anketler, gizlilik değeri olmayan kurum içi yazı, belge ve bilgi notları, arşivler, gazeteler, röportajlar ve mülakatlar vb. değerlendirilmiştir.

Özellikle, birincil kaynak olarak araştırma kapsamında gerçekleştirmiş olduğumuz “derinlikli görüşmeler” ve “sınırlı görüşmeler”in çalışmaya katkısı büyük olmuştur. Hipotezlerin test edilmesinde, temel probleme verilecek cevapların oluşturulmasında ve çözüm yollarının gösterilmesinde görüşme yapılan kişilerin yönlendirici etkisini ayrıca belirtmek gerekmektedir. Ayrıca, Bilgi Teknolojileri ve İletişim Kurumu, TİB ve Bilgi Toplumu Dairesi'nde hazırlanmış uzmanlık tezleri, rapor, araştırma ve makaleler de araştırma konumuzla ilgili önemli veriler sunmuşlardır.

İnternet içerik düzenlemesi ile ilgili Türkçe kaynaklar çok sınırlıdır. Kategorik olarak İnternetin teknik boyutuna ve teknik yönden İnternetin regüle edilmesine yönelik bazı akademik tezler göze çarpsa da İnternetin sosyal yönüne ilişkin akademik tezlerin çok az olması dikkat çekmektedir. Keza, konusu doğrudan içerik düzenlemesiyle ilgili olan kamu yönetimi alanında yapılmış herhangi bir yüksek lisans veya doktora tezine rastlanılmamıştır. Farklı hukuk dallarında yapılmış ve belki İnternet hukuku kapsamında değerlendirebileceğimiz, içerik düzenlemesi konusunun erişim engelleme, ifade ve iletişim özgürlüğü gibi farklı yönlerini ilgilendiren veya basın yayın alanında “yayıncılık” boyutu ile İnterneti ele alan bazı yüksek lisans tezleri bulunmaktadır. Yine, bir yönüyle içerik düzenlemelerini ilgilendiren bilişim suçları, özel hayatın gizliliği gibi konularda yapılmış az da olsa yüksek lisans ve doktora tezlerine rastlanılmaktadır.

Keza, konumuzla ilgili raporlar, araştırmalar ve akademik makaleler bakımından ise, akademik tezlere göre nispeten biraz daha iyi bir durum gözükmeyle birlikte, genel tabloda çok fazla bir değişiklik görülmemektedir. Nitekim, İnternetle ilgili yakın zamanda yayınlanan raporlar, araştırmalar ve akademik makaleler açısından gözle görülür bir ilginin varlığından bahsetmek mümkün olsa da bunların daha ziyade teknik içerikli veya sosyal alanda olsa bile ekonomi ve hukuk ağırlıklı olduğu görülmektedir. İçerik düzenlemesi konusuyla ilgisi bulunanların ise, yine konunun bir yönüne veya alt başlıklarından birisini ele aldığına rastlanılmaktadır.

Az da olsa doğrudan içerik düzenlemesini konu edinen araştırma, rapor, makale ve köşe yazılarının çoğunun ise, akademik ve bilimsel bakış açısından, sorunu farklı boyutlarıyla ele alan bütüncül kavrayıştan yoksun oldukları görülmektedir. Özellikle, Türkiye uygulamasıyla ilgili olanlarda ise, genellikle, popüler görüş ve eleştirilerin ve yüzeysel yaklaşımların hakimiyeti söz konusudur.

İnternet içerik düzenlemesine ilişkin İngilizce kaynaklar ise bir hayli fazladır. Özellikle, üniversitelerin, araştırma merkezlerinin ve enstitülerin yanında, büyük sektör firmalarının, STK’larının, insan hakları örgütlerinin, ülkelerin bilinçlendirme ve ihbar merkezlerinin yayınladığı ve birçoğuna elektronik ortamda ulaşılabilen çok

sayıda kitap, rapor, araştırma, tez ve makaleler bulunmaktadır. Fakat, bunların bir çoğunun yasadışı ve zararlı içeriklerle ilgili müdahale ve mücadelelere ve bu konudaki düzenlemelere çok sıcak bakmadıklarına rast gelinmektedir. Keza, İnternetteki sakıncalı içeriklerin oluşturduğu riskler ve sosyal maliyetlere ilişkin tez, araştırma, rapor veya makalelerin içerik düzenlemelerine ilişkin yapılan toplam yayınlar içindeki oranlarının oldukça düşük olduğu dikkat çekmektedir.

V. Sınırlılıklar

Çok farklı görüş ve tasnifler bulunmakla birlikte, İnternetin düzenlenmesiyle ilgili konular temel olarak dört başlık altında toplanabilir: Alan adı düzenlemeleri, Bilişim suçları ve telif haklarıyla ilgili düzenlemeler, Siber güvenlikle ilgili düzenlemeler ve İçerik düzenlemeleri. Bu başlıklardan alan adı düzenlemeleri ile diğerleri arasında net bir ayrıma gitmek mümkün olmakla birlikte, diğer kalanlar arasında net bir sınır koymak oldukça zordur. Bu nedenle sınırları müphem ve muğlak, birbiriyle içiçe ve ilişkili bu üç düzenleme alanının ihtiva ettiği konuları birbirinden tefrik ederken opsiyonel olmak ve katı şablonlar kullanmamak gerekmektedir. Bu gereklilik sebebiyle, çalışmamızda esas olarak içerik düzenlemesi kapsamında daha ziyade yasadışı ve zararlı içeriğin önlenmesiyle ilgili konular ele alınsa da, yer yer bilişim suçları ve telif hakları ile siber güvenlikle ilgili konulara da değinilmiştir.

İnternet içerik düzenlemesi başlığı altında ise, yasadışı ve zararlı içeriklerin neler olduğuna, bunlarla mücadelenin gerekliliğine, yöntemine, yönetimine ve sınırlılıklarına ilişkin teorik tartışma ve uygulamalar ele alınmıştır. Diğer bir ifade ile, bu çalışma kapsamında, bir bilgi toplumu olgusu olan İnternetin yönetimi ve kontrolü genel çerçevesinde İnternet içerik düzenlemesi konuları bir kamu yönetimi sorunu olarak, yukarıda sunulan bağlamı içinde incelenmiştir.

Keza, bahsi geçen İnternet içerik düzenlemesinin kapsamı konusundaki muğlaklık, konunun/sorunun tüm boyutları ile ortaya konulmasında önemli bir handikap oluşturmaktadır. Bu durum, konunun/sorunun nerede başlayıp nerede bittiğine ve sınırlarının ne olduğuna ilişkin belirsizlikler meydana getirirken, zincirleme olarak,

sorunun ve çözümünün mahiyeti, değişkenleri ve dinamiklerinin belirlenmesi konusunda da tereddütlere ve ihtilaflara neden olmaktadır. Her ne kadar, tereddütlere neden olan konuların hepsinin ortak paydası “İnternetin düzenlenmesi” üst başlığı altında olduğu için nispeten çözümü kendi içinde bulmak mümkün gibi gözükse de, bu konu, çalışmamızın önemli sınırlılıklarından birisini oluşturmaktadır.

Çalışmamızın önemli sınırlılıklarından birisi de, ele aldığımız konunun oldukça yeni olmasıyla ilgilidir. İnternet kısa sürede hayatımızın her alanında önemli değişiklikler meydana getirirse de, geçmiş 40-45 yıla dayanmaktadır. Bu rakam insan ömrü için uzun bir zaman dilimini ifade etse de, binlerce yıllık insanlık tarihi açısından oldukça kısadır. Dolayısıyla, çok kısa sürede büyük değişikliklere neden olsa da, bu bakımdan İnternetin emekleme dönemindeki bir çocuğa benzetilmesi mümkündür.

Bu nedenle, bilgi toplumu ve özellikle İnternetin henüz yeni olduğunu ve devam eden tamamlanmamış bir süreci ifade ettikleri söylenebilir. Dolayısıyla, kavram, kuram, örgüt, yapı, işleyiş, ilişki, süreç, yaklaşım ve diğer özellikleri bakımından birçok belirsizlikler taşıdığı, oturmamış ve yerleşik olmayan yapısı sebebiyle birçok soruna gebe olduğu görülmektedir. Çalışmamızın konusunu teşkil eden İnternet içerik düzenlemesi de bu kapsamda daha da yeni bir konudur. Bu nedenle, yönü, nereye gideceği, nasıl şekilleneceği şimdiden kestirilmesi güç ve açık olmayan; yerleşik kavram, kurum, işleyiş, ilişki, yapı ve uygulamalara sahip olmadığı için tanımlanması, anlaşılması, hakkında kesin hüküm verilmesi zor, riskli ve peşinen bazı eksiklik, noksanlık ve hatalar yapmaya açık ve yatkın bir konudur.

Çalışma konumuzun doğasından kaynaklı diğer bir sınırlılık ise, ele alınan konunun çok yönlü, çok aktörlü, çok değişkenli, çok bilinmeyenli, karmaşık, girift, kaotik, dağınık ve aynı zamanda dinamik bir yapıya ve özelliğe sahip olmasıyla ilgilidir. Bu özelliklerinin birçoğunu İnternetin kendine özel yapısından alan çalışma konumuz, bu nedenlerle bir tez çalışması sınırlılığı içinde tüm gerçekliği ve hakikatı ile ortaya konulmaya uygun değildir. Mutlaka görülemeyen, farkedilemeyen, tespit edilemeyen veya eksik ve yanlış görülen/tespit edilen bazı yönleri olacaktır. Dolayısıyla, birçok

farklı bilim dallarının kesişim noktasında bulunan bu karmaşık konunun bir tez çalışması içinde tüm yönleriyle vuzuha kavuşturulması beklenilmemelidir.

Kuşkusuz, bu tez çalışması, İnternet içerik düzenlemesiyle ilgili ortaya atılan tüm sorulara ve sorunlara cevap bulma iddiasında değildir. Zira, sosyoloji, hukuk, kamu yönetimi, eğitim, siyaset, uluslararası ilişkiler, psikoloji, bilişim, teknik (mühendislik), ekonomi, antropoloji gibi pek çok alanı ilgilendiren ve multi-disipliner bir yaklaşım ve bir ekip çalışması ile ele alınması gereken bu konu geniş kapsamlı, uzun süreli ve yoğunlaşmış bir çalışmayı gerekli kılmaktadır.

Nitekim, konunun/sorunun bu tabiatı, doğru tespit ve çözümlere ulaşılabilmesi için konunun/sorunun her boyutunun ortaya konulmasının gerekliliğine olan inancımız ve bunu sağlamaya çalışma yönündeki yaklaşımımız nedeniyle, tez çalışmamız hacim olarak bir doktora tezinin sınırlarını zorlayacak bir büyüklüğe ulaşmıştır.

Bahsi geçen gerekliliğe rağmen, İnternet içerik düzenlemesi, günümüz devletlerinin ve ülkemizin önemli güncel ama bir o kadar da bakir ve üzerinde yeterince akademik çalışma yapılmamış kamu yönetimi sorunlarından birisidir. Nitekim, tez çalışması nedeniyle yapmış olduğumuz Türkçe literatür taramasında, konunun henüz yeni olmasının da etkisiyle, ülkemizde bugüne kadar çok sınırlı sayıda akademik çalışmaya konu edildiği tespit edilmiştir.

Bu durum, çalışmamızın önemli sınırlılıklarından birisini daha oluşturmaktadır. Daha önce çalışılmamış, üzerinde akademik iz bulunmayan, hakkında fazlaca bilimsel bilgi üretilmeyen bir konuda akademik çalışma yapmanın bütün zorlukları ve dezavantajları çalışma süresince yaşanmıştır. Dolayısıyla, tüm bunların etkilerine yönelik yansımaların tez çalışmamızda görülmesi mümkündür.

VI. Hipotezler/Alt Hipotezler

Tezin temel hipotezi şudur:

İnternet içerik düzenlemesi sorunu, İnternetin kendine özgü yapısından dolayı birçok boyutu ve aktörü olan, karmaşık, çözümü zor ve birçok değişkene bağlı, bilgi toplumu kaynaklı kamu yönetimi sorunudur. Bu sorun kapsamında İnternet, sunduğu eşsiz imkanlar ve fırsatlar yanında beraberinde getirdiği riskler ve tehlikelerle birlikte dengeli bir yaklaşımla ele alınarak, daha faydalı, bilinçli, güvenli ve etkin kullanımını sağlamak amacıyla; ifade özgürlüğü ve bilgiye erişim özgürlüğünü zedelemeyen ve İnternetin kendine özgü yapısı ve özellikleri gözetilerek, devlet eli ile, yönetim ilkeleri çerçevesinde düzenlenmeli ve denetlenmelidir. Bu çerçevede, zorlaştırmacı ve sınırlandırıcı bir takım engeller bulunmakla birlikte, uygun yöntem ve yaklaşımlar içeren bütüncül strateji ve politikalar geliştirilmek ve uygulanmak suretiyle ve uluslararası işbirliği mekanizmaları oluşturularak İnternette yer alan yasadışı ve zararlı içeriklerle mücadele edilmesi, risk ve tehlikelerin en aza indirilmesi mümkün ve gereklidir. Türkiye bu konuda bazı eksiklerine rağmen özgün ve önemli bir örnek uygulama geliştirmektedir.

Bu temel hipoteze bağlı alt hipotezler ise şunlardır:

1. İnternet içerik düzenlemesi sorununun ilk bağlamı “bilgi toplumu”dur. İnternet, “bilgi toplumu”nun en önemli ve değerli ürünüdür. Bu nedenle İnterneti anlayabilmek için “bilgi toplumu” arka planını anlamak gerekmektedir. Dolayısıyla, İnternet içerik düzenlemesi sorunu, bir “bilgi toplumu sorunu” olarak bu arka plan ile birlikte değerlendirilmelidir.
2. İnternet içerik düzenlemesi sorununun bir başka bağlamını da “bilgi toplumu ve devlet/kamu yönetimi” ilişki ve etkileşimi şekillendirmektedir. Sorunun bu bağlamı, İnternetin başrol oynadığı “bilgi toplumu” olgusunun “devleti/kamu yönetimi”ni nasıl dönüştürdüğü gerçeğinden hareketle, “devletin/kamu yönetiminin”, “bilgi toplumu” ile gündeme gelen bu yeni sorun alanına ilişkin tepki ve çözüm üretme çabasını ifade etmektedir. Yani, iki olgu arasındaki etkileşimli süreç İnternet içerik düzenlemesi sorunu üzerindeki önemli belirleyicilerden birisidir ve en somut sonucu “yönetişim” modeli ve “düzenleyici kurullar”ın ortaya çıkışı olmuştur.

3. Bilgi toplumu ve İnternet politikaları; bilgi toplumu ve İnterneti, sunduğu fırsatlar ve riskler, güçlü ve zayıf yönleri, faydaları ve zararları, imkanları ve sorunları bakımlarından olumlu ve olumsuz yönleri ile birlikte, nesnel ve bütüncül bir bakış açısıyla ele alan yaklaşımlar üzerine bina edilmelidir. Günümüzde, genellikle sadece imkan, fırsat ve yararlar üzerine odaklanmış “kutsayıcı” ve “kurtarıcı” popüler bir bilgi toplumu ve İnternet algısı oluşturulmaktadır. Bu ise, özellikle İnternet ortamında bulunan yasadışı ve zararlı içeriklerden kaynaklanan risk ve sorunların gerçek boyutları ile görülmesini zorlaştırmakta ve dolayısıyla, “içerik düzenlemesi” fikrini ve bu tür içeriklerle mücadeleyi zayıflatmaktadır.

4. İnternet güvenlik ve mahremiyet ihlallerine ilişkin sorunlar yanında, barındırdığı yasadışı ve zararlı içerikler ile birçok toplumsal sorunlara neden olmaktadır. İnternet ortamında yer alan pornografi, çocukların cinsel istismarı, şiddet, ırkçılık, ayrımcılık ve nefret içerikleri, kumar ve bahis, intihara ve uyuşturucuya yönlendirme, siber zorbalık gibi yasadışı ve zararlı içerikler tüm toplumu etkilemekle birlikte bilhassa çocuklar, gençler ve aileler için önemli riskler, tehlikeler ve sorunlar oluşturmaktadır. Özellikle pornografi ve çocukların cinsel istismarı, yeterli mücadele yapılmamasının da etkisiyle, İnternetin sunmuş olduğu imkanları kullanarak giderek tüm dünyayı saran küresel bir sorun haline gelmiştir. Bu tür yasadışı ve zararlı içeriklerle ulusal ve uluslararası ölçekte etkin bir mücadele gerekmektedir.

5. Bugün, fiziki bir coğrafya ile sınırlı olmayan İnternetin ciddi bir uluslararası yönetim ve işbirliği sorunu vardır. ABD etki ve etkinliği dışında, üzerinde tamamını kontrol eden tek bir ulusal veya uluslararası yasal bir otorite veya merkezi bir kural koyucu bulunmamak prensibine göre şekillendirilmiş İnternetin mevcut çok aktörlü idari yapısı; İnternetin güvenliğinin ve istikrarının sağlanması, telif hakları, zararlı içeriğin önlenmesi, veri gizliliği ve güvenliği, kültürel ve dilsel çeşitliliğin sağlanması için İnternetle ilgili uluslararası ve uluslararası düzenlemeler yapılması ve işbirliği geliştirilmesinin önündeki en büyük engeldir. İnternetin, bu işlevleri yerine getirmek ve kötüye kullanılmasını önlemek için, “İnternet yönetişi”ni gerçekleştirecek, İnternet ağının tamamını kontrol eden, yaptırım uygulamaya yetkili, meşru, tarafsız ve yasal bir uluslararası merkezi bir otoriteye ihtiyacı vardır.

6. İnternet sınırsız bir özgürlük alanı değildir. Devletlerin yasadışı ve zararlı İnternet içerikleriyle mücadeleyi öngören, risk ve tehlikeleri önlemeyi amaçlayan içerik düzenlemeleri gerçekleştirmeleri kaçınılmaz bir zorunluluk haline gelmiştir. Nitekim, İnternetin güvenli kullanımını sağlamak amacıyla ülkeler, giderek artan bir oranda, İnternet içeriğiyle ilgili düzenlemelere gitmektedir. Fakat, İnternetin çok değişkenli, dinamik ve sınır tanımaz yapısı devletlerin egemenlik haklarını kullanma yetkisini zorlamaktadır.

7. Ülkelerin tarihsel, sosyal, siyasal özellikleri, demokratiklik düzeyleri, ekonomik ve teknolojik gelişmişlikleri, İnterneti kullanım oranları ve bulundukları coğrafya gibi faktörler İnternet politikalarını etkilemektedir. Bu kapsamda, devletleri İnternet içeriği konusunda düzenleme yapmaya iten nedenler ve gereksinimler ile yasadışı ve zararlı kabul edilen içeriklerin konu ve sınırları, kullanılan araçlar, yöntemler, kriterler ve uygulama süreçleri farklılıklar göstermektedir.

8. İnternet içerik düzenlemeleri “ifade ve bilgiye erişim özgürlüğü” ve İnternetin çok yönlü/aktörlü ve dinamik özgün yapısıyla uyum içinde olmalıdır. Düzenlemelerde gerekli olan “en az ve sınırlı müdahale” nin tercih edilmesi, bu iki kriterle uygunluğu sağlamaya en elverişli yaklaşım tarzı olacaktır.

9. İnternet içerik düzenlemesi ve yasadışı ve zararlı içerikle mücadele politikalarının oluşturulması ve uygulamasında “birlikte/ortak düzenleme” yöntemini de içine alan “yönetişim modeli” sonuç alma konusunda en etkili ve demokratik ülkelerce tercih edilen yönetsel araçtır. Bu modelle birlikte, başka bir ek araç olarak “öz düzenleme” uygulamalarının teşvik edilmesi de gerekmektedir.

10. İnternet içerik düzenlemeleri belirli bir sistematik içermelidir. Erişim engelleme yöntemleri, belirli ve oldukça sınırlı sayıdaki suç türlerine en son çare olarak uygulanmalıdır. Öncelik, daha demokratik ve etkili sonuçlar doğuran, uyar-kaldır, özel sektör ile özel anlaşmalar yapma, bilinçlendirme ve İnternet etiği çalışmaları ve pozitif içerik oluşturma gibi olumlu düzenleme yöntemlerine verilmelidir. Zira,

İnternetin kendi doğasından ve teknik özelliklerinden dolayı, erişim engelleme yöntemleri yüzde yüz başarıyı sağlamadığı gibi bir çok sakıncalar doğurmaktadır.

11. İnternet düzenlemelerinde başarı; çok boyutlu, çok aktörlü ve dinamik olan İnternetin doğasına ve özelliklerine uygun olarak oluşturulacak ve uygulanacak çok boyutlu, çok aktörlü ve dinamik bütüncül bilgi toplumu ve İnternet politikalarıyla mümkündür. Bu kapsamda, içerik düzenlemesi sorunun çözümü ise, bütüncül bilgi toplumu ve İnternet politikalarının bir parçası olarak ele alınmak suretiyle belirlenmiş ve sorunun teknik, ekonomik, sosyal, siyasal, yönetsel tüm boyutlarını içine alan uygun kamu politikaları, karar ve uygulamalarıyla gerçekleştirilebilecektir.

12. İnternetin kendine özgü yapısından, uluslararası yönetim sorunlarından ve ülkelerin konuya farklı yaklaşımlarından dolayı yasadışı ve zararlı içeriklerin tamamen önlenmesinin mümkün olmayacağı kabul edilmekle birlikte, uygun yöntem ve yaklaşımlar içeren strateji ve politikalar geliştirilmesi ve uygulanması durumunda bu içeriklerden gelebilecek zararların minimize edilebilmesi mümkün ve gereklidir.

13. Dünyadaki İnternet içerik düzenlemelerini belirleyen en önemli parametrelerden birisi paranın gücüdür. Zira, ülkelerde İnternet içerik düzenlemelerinin asıl belirleyici unsuru büyük oranda sermaye ve piyasa olmaktadır. Sermaye, genelde İnternetin düzenlenmesi, özelde ise, içerik düzenlemelerinin yönünü, politikalarını, yasadışı içeriklerle mücadelenin kapsamını ve yöntemini büyük oranda belirlemektedir.

14. İnternet içerik düzenlemesi politika ve uygulamalarının meşruiyetini normatif olarak ölçülmesine imkan tanıyacak uluslararası geçerliliği olan kıstasların ve analitik analiz yöntemlerinin geliştirilmesi gerekmektedir. Böylece, bu alandaki sivil ve kamu otoritelerinin keyfi yorumları ile ülkelerin ve uygulamalarının değerlendirilerek mahkum edilmesinin önüne geçilebilir.

15. İnternet kullanımının hızla artış gösterdiği Türkiye, genç kullanıcıların çokluğu ve risk düzeyi yüksek İnternet kullanımı ile İnternet ortamından gelebilecek tehdit ve tehlikelere açık bir profil ortaya koymaktadır. Türkiye’de, yasadışı ve zararlı İnternet içeriği yanında İnternetin yanlış kullanımından da kaynaklanan önemli toplumsal

sorunlar ve güvenlik sorunları yaşanmaktadır. Bu durum özellikle, çocuklar, gençler ve aileler açısından ciddi riskler oluşturmaktadır.

16. Türkiye İnternet içerik düzenlemesi konusunda, bazı eksiklerine rağmen, yasadışı ve zararlı içeriğe devlet eli ile sınırlı müdahaleyi öngören kendine özgü, önemli ve örnek bir uygulama geliştirmektedir.

Söz konusu temel hipotez ve alt hipotezler etrafında yürütülecek tartışma ve değerlendirmeler üzerinden ele alınacak İnternet içerik düzenlemesi sorunu tezde üç bölümde incelenmiştir. Sosyal, siyasal, ekonomik ve teknik birçok boyutu ve çok değişkenli yapısı olan İnternet içerik düzenlemesi konusunun bilgi toplumu bağlamına dikkat çekilmesi ve teorik bir çerçeveye oturtulması, daha sonraki bölümlerde sunulacak tartışma ve değerlendirmeler için sağlıklı bir zemin oluşturacağı düşüncesiyle çalışmanın, birinci bölümünde bilgi toplumu ve İnternet konusu kavramsal, kuramsal ve tarihsel arkaplanı ile ortaya konulmaya çalışılmıştır.

Buna göre, önce genel olarak Bilgi Toplumu ve bu bağlamda devlet/kamu yönetimi konuları teorik ve tarihsel gelişimleri itibarıyla ele alınmış ve bilgi toplumunun sorunları ve özellikle bilgi toplumunun sembolü haline gelen İnternetin faydaları ve beraberinde getirdiği sorunlar irdelenmiştir. Daha sonra ise “İnternet” konusu tarihsel gelişimi, yapısal unsurları, altyapısı, aktörleri, geleceği yanında uluslararası yönetimi boyutlarıyla mercek altına alınmıştır.

Çalışmanın “Dünyada İnternet İçeriğinin Düzenlenmesi: Yaklaşımlar, Yöntemler ve Uygulamalar” başlıklı ikinci bölümünde ise, İnternet içeriğinin düzenlenmesine ilişkin tartışmalar, neden içerik düzenlemesine gereksinim duyulduğu, hangi tür içeriklerin yasadışı ve zararlı görüldüğü, içerik düzenlemesinde temel yönetsel yaklaşımlar, belli başlı içerik düzenleme yöntemleri ve içerik düzenlemesinin ölçütleri gibi konular çerçevesinde uluslararası kuruluşların ve ülkelerin içerik düzenlemesi uygulamaları incelenmiştir.

Böylece, İnternet içeriğinin düzenlenmesi konusu, Dünyadaki tartışmalar, temel yaklaşımlar ve uygulamalar açısından irdelenerek, bu çerçevede, Dünyada uygulanan

modeller, ülkelerin konuya yaklaşımları, hukuksal ve örgütsel yapılar ve bunların işleyişleri, devlet gücünün İnternet içeriğinin düzenlenmesinde kullanılıp kullanılmadığı veya ne ölçüde kullanıldığı gibi konular derinlemesine ele alınmıştır. Bu şekilde, birinci bölümdeki genel çerçeve bağlamında, çalışmanın odak noktasını oluşturan İnternet içerik düzenlemesi konusuna daha spesifik ve somut bir projeksiyon sunularak, bununla bir sonraki bölümde incelenecek olan Türkiye uygulaması ve TİB örneğinin değerlendirilmesine uygun bir zemin hazırlanmıştır.

Çalışmanın “Türkiye’de İnternet İçeriğinin Düzenlemesi: TİB Örneği” başlıklı üçüncü bölümünde ise, önce İnternet olgusunun Türkiye’ye yansıyan boyutunun anlaşılır kılınması için Türkiye’de İnternetin gelişimi, kullanım özellikleri, beraberinde getirdiği sorunlar ana hatları ile ele alınmıştır. Daha sonra, İnternet içerik düzenlemelerinin tarihçesi, 5651 Sayılı Kanunun öncesi, 5651 Sayılı Kanun’un gelmekte olduğunun habercileri olan tasarı ve teklifler, 5651 Sayılı Kanunun yasalaşma sürecinde yaşananlar, 5651 Sayılı Kanun’un getirdiği hükümler ve öngördüğü yeni hukuki çerçeve, Türkiye’de İnternet ile ilgili yetkili kurumlar, 5651 Sayılı Kanun’un yürürlüğe girmesi ve TİB’in devreye girmesinden sonra ortaya çıkan yeni örgütsel yapı, TİB’in içerik düzenlemesine ilişkin yaklaşımları ve uygulamaları gibi konular ele alınmış ve önceki iki bölümde öne çıkan tartışma, yaklaşım ve uygulamalar ışığında değerlendirilmiştir.

Son bölümde genel değerlendirme, sonuç ve öneriler kısmı yer almıştır. Bu çerçevede, önce “genel değerlendirme” başlığı altında çalışmanın bütünlüğü içinde toparlayıcı bir özet yapılmış ve son kez hipotezler bu bütünlük içinde kısaca değerlendirilmiştir. Daha sonra, tez içinde detaylı, “genel değerlendirme”de ise özet olarak ele alınan tüm hipotezlere ilişkin ulaşılan sonuçlar kısa açıklamalar ile kayıt altına alınmıştır. Bu arada, hipotezlerin “genel değerlendirme” ve “sonuç” başlıkları altındaki karşılıklarının takibini kolaylaştırmak için hipotez numaraları, söz konusu başlıkların altındaki metinlerin hipotezle ilgili bölümlerine de yazılmıştır.

Son olarak ise, tüm çalışma boyunca eldeki verilere göre incelenen, tartışılan, değerlendirilen ve bir takım tespitlere ve sonuçlara ulaşılan İnternet içerik

düzenlemesine ilişkin olarak ülkemizde geleceğe yönelik yapılması gerekenlere, ortaya çıkan sorunların çözümüne ilişkin öneriler sunulmuştur. Bu kapsamda, politika önerileriyle ilgili olanlar “politikalar”, örgütsel önerilerle ilgili olanlar ise “kurumlar” başlığı altında belirtilmiştir.

Henüz akademik ilgi odağı olmayan İnternet içerik düzenlemesi konusu hakkında ivedi olarak bilimsel çalışmalara ihtiyaç bulunmaktadır. Ümidimiz odur ki, bu tez, konusu itibariyle yeni fakat önemli bir konunun bilimsel verilerle tartışılmasının kapısını aralayarak sahadaki derin boşluğa işaret ederek bu alandaki kuramsal ve uygulamaya yönelik çalışmalara öncülük edecektir. Keza, bu çerçevede tez çalışmasının hem toplumda hem de konu ile ilgili politika belirleme konumunda olan kamu yöneticilerinde farkındalık oluşturmaya katkı sağlayacağı umulmaktadır.

BİRİNCİ BÖLÜM

BİLGİ TOPLUMU VE İNTERNET: KAVRAMSAL, KURAMSAL VE TARİHSEL ARKAPLAN

Sonraki bölümlerde ele alınacak konulara teorik bir çerçeve oluşturmayı amaçlayan bu bölümde; “bilgi toplumu” ve “İnternet” olguları kavramsal, kuramsal ve tarihsel arkaplanları ile ele alınırken, tezin ilk beş alt hipotezi de tartışılarak doğrulukları ve geçerlilikleri değerlendirilmiştir. Bu bağlamda önce bilgi toplumu olgusu ve bu çerçevede devlet/kamu yönetimi konuları, sonra da İnternet olgusu incelenmiştir.

1.1. BİLGİ TOPLUMU

21. Yüzyıl’ın başında bulunduğumuz şu günlerde, gelişmişlik düzeyi ne olursa olsun, bütün toplumları ilgilendiren çok köklü bir değişim ve dönüşüm sürecini yaşamaktayız. İçinde yaşanan bu sürecin adlandırılması, tarihte daha önce yaşanmış diğer köklü toplumsal değişikliklerden ayrılan yönlerinin belirlenmesi, gelecekte alabileceği olası biçimlerin şimdiden öngörülebilmesi açısından önemlidir.

Bu bakımdan, bilgi toplumu tartışmalarının gerisinde yatan düşünsel birikimin devlet/kamu yönetimi konularıyla ilintili olarak harmanlanarak irdelenmesiyle, günümüzde İnternet ile simgeleşen bu olgunun, hangi tarihsel ve kuramsal arkaplan üzerinde inşa edildiği daha açık bir biçimde görülebilecektir. Bu arkaplan üzerine, bilgi toplumuna ilişkin sorunlar ve bugünün önemli tartışma konuları olan İnternetin beraberinde getirdiği sorunlar ve sosyal etkilerini ele almak daha doğru olacaktır. Böylece, tezde yer alan ilk beş alt hipotezin doğruluğunun ve geçerliliğinin değerlendirilmesini sağlayacak donelere sahip olma imkanı hasıl olacak ve bu veriler çerçevesinde hipotezler tartışılarak test edilmiş olacaktır.

1.1.1 Kuramsal Çerçeve: Bilgi Toplumu Kavramı ve Özellikleri, Bilgi Toplumunda Devlet ve Kamu Yönetimi ve Kurama Yöneltilen Eleştiriler

Bilgi toplumuna ilişkin genel bir kuramsal çerçeve oluşturmak için, önce bilgi toplumu kavramı ve özellikleri ortaya konulmaya, daha sonra bilgi toplumunda

devlet ve kamu yönetimine ilişkin teorik ve uygulamaya yönelik değişim ve dönüşümler ana hatlarıyla ele alınmaya, sonrasında ise bilgi toplumu kuramına yöneltilecek eleştiriler gözden geçirilmeye çalışılacaktır.

1.1.1.1. Bilgi Toplumu Kavramı ve Özellikleri

Bilgi toplumu nedir? Kavramsal olarak neyi ifade etmektedir? Bilgi toplumu kavramı etrafında yürütülen tartışmalar ve bilgi toplumunun öne çıkan özellikleri nelerdir? Tüm bu sorulara cevaplar aramanın sonraki bölümlerde ele alınacak tartışmaların temel yapı taşlarını oluşturacağı düşünülmektedir.

1.1.1.1.1 Bilgi Toplumu Kavramı

Bilgi toplumu deyimi günlük yaşamda çoğu kez, “bilgi düzeyi yüksek toplum”, “bilginin temel ekonomik kaynak olduğu toplum”, “bilgisayar ve bilgi kullanımında ileri toplum”, “bilgisayarın her alanda yaygın olarak kullanıldığı toplum” anlamlarında kullanılmaktadır (Başbakanlık, 2002: 7).

Toplumların dönüşümünde teknolojik yeniliklerin önemli etkileri olmaktadır. Teknolojik yenilikler toplumların ekonomik, sosyal, politik ve kültürel yapılarını belirli bir süreç içerisinde değiştirmekte ve dönüştürmektedir (Basalla, 2004: 284). Nitekim, insanlığın teknolojik gelişim tarihinin saban, buhar makinesi ve bilgisayarın geliştirilmesi olgularının belirleyici olduğu üç toplum aşamasından geçtiği kabul edilmektedir (Aktan ve Tunç, 1998: 118-119). Bunlardan ilki, sabanın icadıyla başlayan ve insanlığın göçebe yaşamdan yerleşik düzene geçtiği, pazarın üretim bölgeleri ve yakın köylerle sınırlı olduğu ve ilk kamusal örgütlenmenin ortaya çıktığı “Tarım Toplumu”dur (Sarıbay, 1996: 146). İkincisi, buhar makinesinin icadıyla başlayan ve üretimin kitlesel hale geldiği, ekonomik, sosyal ve kültürel tüm alanlarda Fransız aydınlanmasının etkilediği modernleşme sürecinin ön plana çıktığı, işte uzmanlaşmanın ve pazarın fiziksel olarak erişilebilen her yer olduğu “Sanayi Toplumu”dur (Giddens, 2000: 328). Üçüncüsü ise, ilk bilgisayarın geliştirilmesiyle başlayan, bilginin ve nitelikli insanın merkezde yer aldığı ve pazarın sayısal ağlarla erişilebilen tüm dünya olduğu “Bilgi Toplumu”dur (Taşçı, 2007: 25).

Sosyal bilimciler 1960’larda ileri düzeyde sanayileşmiş ABD, Japonya ve Batı Avrupa gibi toplumlarda “bilgi ve iletişim teknolojileri” olarak adlandırılan yeni teknolojilerin ortaya çıkarak hızla gelişmesiyle meydana gelen değişmelerin sanayi toplumundan birçok yönden farklılıklar gösteren yeni bir yapı ortaya çıkardığını gözlemlemişler ve bu yeni yapıyı tanımlamak için çok sayıda yeni kavram ortaya atmışlardır (Törenli, 2004: 9-10). Bunların en meşhurları Alvin Toffler’in “Üçüncü Dalga”sı, Daniel Bell’in “Sanayi-Ötesi Toplum”u, Masuda ve Drucker’in “Bilgi Toplum”u kavramları olmuştur (Masuda, 1990; Drucker, 1995). İçlerinden “Bilgi Toplumu” kavramı ise 1990’lardan sonra daha çok benimsenmiş ve kullanılmıştır.

Bu yaklaşımlar, yeni toplumsal yapıyı adlandırmada ve tanımlamada sanayi toplumunun ekonomik, sosyal, siyasal, kültürel ve felsefî yapısını oluşturan “ulus-devlet”, “merkezi yönetim”, “temsili demokrasi”, “hiyerarşik yapılanma”, “fordist üretim”, “modernite”, “akıl” ve “pozitivist bilim” gibi geleneksel analiz, araç ve kavramlarının yetersiz kaldığı noktasında birleşmektedir (Al, 2007: 63-65). Yeni dönemde, üretim ilişkilerinin, tüketim alışkanlıklarının, örgütsel yapıların değişmiş olduğuna ve sermayenin küreselleştğine; fordist üretimden postfordist üretime, ulus-devletler dünyasından küreselleşmiş dünyaya, modernist düşünceden postmodernist düşünceye geçildiği dile getirilmektedir (Tekeli, 1999: 244; Kumar, 1999: 9).

Hatta, tüm bu değişmelerin “paradigma değişimi” olduğu (Bozkurt, 1996: 3); bu yeni dönemde, fordist paradigmanın yerini postfordist paradigma, modern paradigmanın yerini postmodern paradigma, ulusal paradigmanın yerini küreselleşme paradigması, refah devleti paradigmasının yerini özelleştirme paradigması, geleneksel kamu yönetimi paradigmasının yerini yeni kamu yönetimi-işletmesi paradigmasının aldığı değerlendirilmesi yapılmaktadır (Bilgiç, 2008: 29; Al, 2007: 65).

ABD’nin resmi belgelerine bakıldığında “bilgi toplumu” kavramının çok az kullanıldığı görülmektedir. ABD, çeşitli sosyo-kültürel nedenlerle “Ulusal/Küresel Bilgi Altyapısı”, “Bilgi Otoyolları” gibi kavramları daha çok kullanmaktadır. Avrupa Birliği (AB) ise 1994 yılından bu yana bilgi toplumu kavramını bu alandaki politikaların genel çerçevesi için kullanmaktadır (TÜBİTAK, 2002: 4).

1.1.1.1.2 Bilgi Toplumunun Özellikleri

Bilgi toplumunun temel özelliklerini şunlardır (Bozkurt, 1996: 3; Aktan ve Tunç, 1998: 119-129; Drucker, 1994: 14-18; Toffler, 1981: 34; Kumar, 1999: 78-81; Tekeli, 1994: 53; Bensghir, 1996: 7; Çoban, 1996: 34-45; Erkan, 1997: 72):

1. Ekonomik Yapıdaki Dönüşüm: Bilgi toplumunun en önemli özelliği mal ve eşya üretiminden hizmet üretimine doğru bir kaymanın görülmesidir. Dolayısıyla bilgi toplumunda hizmetler sektöründe çalışanların oranı, tarım ve sanayi sektörlerindeki istihdama göre çok daha fazladır. Bilgi toplumunda eğitim, sağlık, sosyal hizmetler gibi insani hizmetler ve bilgisayar, elektronik, biyokimya, yazılım, bilimsel AR-GE gibi mesleki hizmetler yoğunluk kazanmaktadır.

2. Yükselen Yeni Sınıflar: Sanayi toplumunda yarı vasıflı işçiler çalışan sınıf içinde en kalabalık grubu oluşturmaktaydılar. Bilgi toplumunda ise, teknik ve profesyonel sınıf, yani Drucker tarafından “bilgi işçisi” olarak nitelenen bilim adamları, teknisyenler, mühendisler, öğretmenler sayıca artmış ve toplumun kalbi konumuna yerleşmişlerdir. Buna bağlı olarak toplumda gücün yapısı da değişmiştir. Tarım toplumunda toprak sahipleri, sanayi toplumunda ise sermaye sahibi işverenler gücü ellerinde bulundurmaktayken oluşan yeni toplumda ise güç bilgi sınıfına geçmiştir.

3. Bilginin Artan Rolü: Sanayi toplumu, malların üretimi için makine ve insanların koordinasyonuna dayanmaktaydı. Yeni toplum ise bilgi etrafında örgütlenmektedir. Sanayi uygarlığının öncü isimlerinden Bacon’un yüzyıllar önce söylediği gibi “bilgi güçtür”, ancak, bilgi toplumunda bilgi aynı zamanda toplumun temel eksenini de oluşturmaktadır. Buna göre, tarım toplumunda toprak ve işgücü, sanayi toplumunda sermaye merkezi bir öneme sahip iken, bilgi toplumunda bilgi stratejik bir kaynak ve sermaye haline gelmiştir. Bu yeni toplumda teorik bilgiyi piyasada yeni ürün ve hizmetlere başarılı şekilde dönüştürenler ile eğitim ve AR-GE harcamalarına en çok yatırım yapan işletmeler ve toplumlar başarılı olacaktır.

4. Bilgi ve İletişim Teknolojileri: Sanayi toplumunun ortaya çıkmasında en önemli etken buhar makinesi, elektrik, içten yanmalı motor gibi enerji teknolojilerinin

bulunmasıdır. Bilgi ve iletişim teknolojilerinin ortaya çıkıp hızla gelişmesi de benzer bir etkiyi yeni oluşan toplumda oluşturmuş ve yüksek değerlere sahip ürünler ortaya koyma yeteneğine sahip olduklarından iktisadi gelişme açısından en fazla önem verilmesi gereken alan olarak görülmüşlerdir.

5. Örgütlü Toplumun Güçlenmesi ve Gönüllü Kuruluşların Etkinleşmesi: Bilgi toplumunda, ortak özellikler, değerler ve amaçlar ile ortak çıkarlara sahip kişilerin oluşturduğu sosyal gruplar teşkilatlanmış gruplar olarak sivil hayatta ağırlıklarını ve etkinliklerini göstereceklerdir. Bilgi toplumunda gönüllü kuruluşlar ön plana çıkacaktır. Toplum artık örgütlü bir toplum olacak ve sanayi toplumundaki temsili demokrasi yerini katılımcı demokrasiye bırakacaktır.

1.1.1.2 Bilgi Toplumunda Devlet ve Kamu Yönetimi

Bilgi toplumunda devlet ve kamu yönetimi konusunu, tezin ikinci alt hipotezinin tartışılmasına imkan verecek şekilde, önce tarihsel perspektifi içerisinde ele alıp günümüze taşıdıktan sonra, yapılacak olan tartışmalara ışık tutması bakımından yönetim ve e-devlet konularına yer verilecektir. Keza, elde edilecek veriler çerçevesinde ikinci hipotez değerlendirilecektir.

1.1.1.2.1 Tarihsel Arkaplan ve Bugün

Her toplum biçiminin dayandığı bir “geçim biçimi”, geliştirdiği bir “yaşam biçimi” ve yaşam biçimiyle uyumlu bir “düşün biçimi” ve dolayısıyla bunlarla da uyumlu bir “yönetim biçimi” söz konusudur (Şenel, 1995: 16). Nitekim, kamusal hayatın örgüt ve işlev olarak gelişmesinde, sanayi devriminin yapılandığı sanayi toplumu ve modern ulus-devlet anlayışı belirleyici olmuş, bu değişimler de siyasi, ekonomik ve sosyal şartları zorlamış ve yeni kurumların ortaya çıkmasına neden olmuştur (Şaylan, 1995: 26). Bu durum, kamu işlevlerinin tarihte görülmemiş bir şekilde artmasına ve genişlemesine, buna paralel olarak da kamusal örgütlerin büyümesine ve her alana nüfuz etmesine yol açmıştır (Bilgiç, 2008: 27; Toffler, 1981: 494). Örgütlenmedeki artış nedeniyle devletin iktidar alanı genişlemiş, etkinliği artmış ve her konuda söz sahibi olmuştur. Böylece “refah devleti” anlayışı ortaya çıkmıştır (Al, 2007: 117)

Sanayi toplumunda teknolojik gelişmeler mal ve hizmet üretimini merkezileştirmiş, sermaye belli ellerde toplanmaya başlamış ve bu merkezileşme eğilimi işletme yönetiminden kamu yönetimine ve hatta tüm topluma yayılmıştır (Toffler, 1981: 85-89). Merkezileşme düşüncesiyle yakından ilgili olarak bu dönemde ortaya çıkan Max Weber'in kavramsallaştırdığı “bürokrasi modeli”, genelde yönetim düşüncesini, özel de ise kamu yönetimi düşüncesini derinden etkilemiştir. “Geleneksel Kamu Yönetimi” olarak da anılan sanayi toplumu kamu yönetimi, yapı ve işleyiş olarak “Weberyen Bürokrasi Modeli” ne dayanmaktadır (Weber, 1996: 290-316).

1970’lerdeki refah devleti bunalımı ve bunu aşmaya yönelik yeni politikalar, bilgi ve iletişim teknolojilerindeki olağanüstü gelişmeler, üretim alanındaki büyük değişimler, Doğu Bloku’nun çökmesi, küreselleşme, liberalizm ve piyasanın artan gücü ve demokrasi ve insan haklarındaki gelişmeler ile yeni kamu yönetimi yaklaşımı eşzamanlı olgular olarak birbirlerini beslemiştir (Al, 2007: 82).

Sanayi devrimi, sanayi toplumunu ve ona uygun kamu yönetimi anlayışını ortaya çıkartırken, bilgi ve iletişim teknolojilerindeki gelişmeler de bilgi toplumunu ve ona uygun yönetim yapısını ortaya çıkartmıştır. Bu anlamda sanayi toplumunun genel zihniyet yapısını yansıtan modernizmin, her alanda evrensel, objektif akılcı ve ideal olana ulaşma çabası göstermesi; kamu yönetiminde ulus-devlet çerçevesinde akılcılığı, merkeziliği, bütünselliği ve hiyerarşik düzeni yansıtan bürokratik yapılanmayı getirmiştir. Buna karşılık bilgi toplumu zihniyet yapısını yansıtan postmodernizmin bütünselliğin yerine parçayı ve tekil öznelere koyması, merkezde toplanma ve bütünleşme yerine çoğulculuğu benimsemesi, genellik ve objektifliğin yerine görelilik ve subjektifliği getirmesi; kamu yönetiminde merkeziyetçilikten uzaklaşan, yerelliği, yerinden yönetimi, yatay örgütlenmeyi ve esnek uzmanlaşmayı ön plana çıkaran görev örgütlenmelerini, geçici ya da kendiliğinden oluşan yapılanmaları gündeme getirmiştir (Saran, 2004: 14-15).

Hem özel sektörde hem de kamu sektöründe, bilgi ve iletişim teknolojileri örgütlerin yapısını, işleyiş süreçlerini, hizmetlerin niteliğini, çalışma ilişkilerini, performansını ve değişimini derin bir şekilde etkilemiştir. Toplumsal yapının değişmesine yol

açarak belli bir süreç içinde üretim ilişkilerini ve organizasyon yapılarını yeniden yapılandırmıştır. Kamu hizmetlerinin işleyişinde görülen geleneksel bürokratik yapı çözülmüştür (Ergun ve Polatoğlu, 1992: 68; Al, 2007: 282).

Bilgi ve iletişim teknolojilerinden yönetimin bütün basamaklarında yararlanılmasıyla birlikte bilginin işlenme hızı, kullanabilirliği, kullanım alanları ve veri hacmi artmıştır. Bu da örgütlerin planlama, uygulama ve denetleme kapasitelerini büyük ölçüde geliştirmiştir (Balcı, 2008: 320; Kumar, 1999: 24; Tekeli, 1994: 46). Bilgi ve iletişim teknolojileri, kamu hizmetlerinin ucuz ve daha kolay sunulmasında önemli bir rol oynamış; ulaşım sisteminden, güvenlik sistemine, kütüphane sisteminden, banka sistemine kadar birçok alanda geleneksel hizmet yöntemlerini değiştirmiştir.

Yeni teknolojiler ve özellikle İnternet, zaman ve mekanı dönüştürmüş, hızı artırmış ve böylece coğrafya ve fiziki mekanın önemini azaltmıştır (Rahm, 1997: 72). Nitekim, işyeri kavramı geleneksel anlamını yitirmiştir. Hizmetler, hemen her yerde üretilebilmekte, dolayısıyla işin nerede yapıldığı önemsiz hale gelmektedir. Bu gün birçok hizmet evlerden yürütülebilir duruma gelmiştir. Kişisel bilgisayarlar sayesinde insanlar kendi kendilerinin patronu olma imkanı bulmuşlardır. Keza, yeni teknolojilerle birlikte, mesai anlayışı da değişmiş; online/tele-bankacılık, online/tele-alışveriş ve online/tele-eğitim sistemi hayatımıza girmiştir. Bu şekilde, 7/24 mantığıyla sunulan hizmetler gün geçtikçe artmıştır.

Diğer taraftan, bilgi ve iletişim teknolojilerinin yaygın olarak kullanılmaya başlanması, vatandaşların beklenti düzeylerini hem farklılaştırmış, hem de arttırmıştır. Aynı zamanda bu olgu vatandaşların oluşturulan kamu politikaları ile, kamu yöneticilerinin kararlarına daha fazla katılma imkanı sağlamıştır (Coşkun, 2008: 56).

Tüm bu gelişmeler nedeniyle bilgi toplumunun, kamu yönetimi anlayışında; vatandaş ve devlet arasındaki güç dağılımındaki eşitsizliğin ortadan kaldırılması, “temsili demokrasi”nin yerini “katılımcı demokrasi”nin ve “yönetişim”in alması, yönetimin vatandaş odaklı olması, yönetime egemen olan “gizlilik kültürü”nün yerini “açık” ve “hesap verebilir” yönetim anlayışına bırakması, merkeziyetçi yönetim yapısından

yerelleşmiş veya yerinden yönetimin önem kazandığı bir yönetim yapısına geçilmesi, kamu mal ve hizmet sunumlarında verimliliğin esas alınması, kimi kamu hizmetlerinin “özel sektör” ve “sivil toplum örgütleri”ne bırakılması yönünde bir değişime uğradığı ifade edilmektedir (Akyıldız, 2004: 447).

Keza, bilgi toplumunda devletin rolü ve sınırlarının yeniden sorgulandığı ve “yeni devlet” anlayışının geliştiği görülmektedir. Yeni devlet; siyasal sınırların ve ulusal egemenlik anlayışının eski katılığını kaybettiği, bölgesel ve uluslararası örgütlenmelerin önem kazandığı, küresel sermayenin çizdiği etkinlik alanı içinde mal ve hizmet ve dolayısıyla teknoloji ve bilgi akışının hızlandığı, bireysel tercihlerin ve alt kimliklerin ulusal kimlik yapısının standartlaştırılmış kalıplarına sığmadığı, merkeziyetçi plan disiplini ve kalkınma anlayışıyla belirlenen ilerlemeci hedeflerin bağlayıcılık ve etkileme güçlerinin zayıfladığı siyasal-yönetimsel bir zemin üzerinde oturmaktadır (Saran, 2004: 27). Bu zeminde yeşeren bilgi toplumu devleti, “Hukuka bağlı demokratik devlet”, “adem-i merkeziyetçi devlet”, “katılımcı devlet”, “açık-şeffaf devlet”, kamu istihdamında bilgi ve becerinin, uzmanlığın esas alındığı “meritokratik devlet”, “sınırlı-çerçeve devlet”, piyasayı düzenleyen ve gözetici “hakem devlet” özellikleri ile tebarüz etmiştir (Aktan, 2003: 92-117).

Bu süreçte, devletin daha etkili ve verimli bir işleyişe kavuşturulması amacıyla kamu hayatındaki müdahale ve etki alanının daraltılmasını temin etmek için “kamu yönetimi reformları” gündeme gelmiştir. Bu çerçevede kullanılan en önemli araçlardan birisi olan deregülasyon uygulamaları, öncelikle Batı Avrupa ve ABD’de, daha sonra da diğer ülkelerde yaygınlık kazanmıştır.¹

1980’lerden sonra hız kazanan bu eğilim, daha çok özelleştirme politikalarıyla kendisini göstermiştir. Devletin ekonomik alandaki ağırlığının azaltılmasına yönelik deregülasyon uygulamaları, posta, haberleşme, enerji, hava/demiryolu taşımacılığı,

¹ Deregülasyon, devletin sektörler üzerindeki hukuki düzenleme, kısıtlama ve kontrol etme yetkisinin kısıtlanması veya tamamen kaldırılmasıdır. Buna göre, devlet, yürüttüğü bazı kamusal faaliyetlerden, fiyat veya ücret denetiminden vazgeçer, sübvansiyonları kaldırır ve kamu tekellerinin tekel olma niteliği son bulur (Aksoy, 1995: 168). “Deregülasyon politikalarının temel nedeni kamu hizmetlerinde etkinlik ve verimlilik sağlamaktır. Daha önce devlet faaliyetleri arasında yer alan işlevlerin özel sektör rekabetine açılarak endüstriyel performansın artırılması hedeflenmektedir.” (Al, 2007: 160).

finans ve sigorta gibi temel sektörlerde faaliyet gösteren kamu işletmelerinin hızla özelleştirilmeleri sonucunu doğurmuştur (Aktan ve Vural, 2005: 54-55).

Yeni devletin tüm özellikleriyle ortaya çıkabilmesi için, 1980’lerdeki devletin toplumsal ve ekonomik alandaki rolünün azaltılmasıyla kendisini gösteren deregülasyon politikalarının ardından, 1990’lardan sonra regülasyon politikaları yeni reformlar olarak uygulamaya geçirildi. Bu çerçevede, öncelikle İngiltere gibi Batı Avrupa ülkelerinde ve bir süre sonra da Türkiye’de hız ve yaygınlık kazanan, ABD’de ise kamu yönetimi sisteminin öteden beri karakteristik kurumları arasında yer alan “düzenleyici kurullar”; kamu yönetiminin işleyişine hız ve etkinlik kazandırmak ve daha önce icracı rolü kaldırılan devlete aktif düzenleyicilik işlevi verilmesi için faaliyete geçirildiler (Saran, 2004: 31).

1.1.1.2.2 Yönetişim

Bilgi toplumu ve kamu yönetimi bağlamında yeni kamu yönetimi yaklaşımıyla ilgili olarak son yıllarda en sık kullanılan kavramlardan birisi de yönetişimdir. Yönetişim, “karşılıklı yönetim,” “etkileşim içinde yönetim” anlamına gelmektedir (Uçkan, 2003). Kavramsal olarak yönetişimin, özel sektör ile kamu kesimi arasındaki sınırların muğlaklaştığı, devlet otoritesi ve yaptırımlarına dayanmayan, çoğulcu yönetim biçimlerinin ve aktörlerinin etkileşimiyle ortaya çıkan yeni yönetim modeli olduğuna ilişkin genel bir kabul vardır (Coşkun, 2008: 68).

Yeni kamu yönetimi, yeni kamu-özel ortaklık formu oluşturmayı ve merkezi yönetim, yerel yönetimler, hükümet-dışı organizasyonlar ve özel sektör grupları ile işbirliği yapmayı öngörmektedir. Ulus-devletin otorite ve yetkilerini uluslararası kurumlar, yerel yönetimler, sektörler, bireylerle paylaşması gibi yönetim de sorumluluğunu ve yetkilerini, kendi dışındaki kurum, birey, grup ve örgütlerle paylaşmak durumundadır (Coşkun, 2008: 75).

Yönetişim, kamusal sorumluluk ve denetim anlayışına yepyeni bir yaklaşım getirmiştir. Bu yeni anlayışa göre, kamusal sorumluluk genişlemekte ve yönetilenler de yönetim sürecine dahil edilmektedir (Tekeli, 1999: 244). Yönetişim, gücün nasıl

kullanıldığını, kararların nasıl alındığını ve vatandaşların yönetim sürecine nasıl katıldığını belirleyen bir süreçtir. Bu durum, kamu yönetimi anlayışının, “kamunun yönetilmesi”nden “kamunun yönetmesi” anlayışına doğru evrilmesinin bir işareti olarak görülmektedir (Nohutçu ve Balcı, 2008: 19).

Yönetişim, siyasal katılma beklentilerini karşılayamayarak krize giren temsili demokratik sistem için alternatif çözüm üretmektedir. Yönetişim, modern yönetim ve siyaset anlayışının, kaybettiği temsil gücünü yeniden kazanmasında; yatay koordinasyona, yoğun bilgi akışı ve paylaşımına, yaygın iletişim altyapısına, siyasal-yönetimsel bütünlüğü oluşturan tüm tarafların açık katılımına dayalı mekanizmalarıyla uygun bir sistem çerçevesi ortaya koymaktadır (Saran, 2004: 24-25).

Bir de son yıllarda kamu yönetimi literatürüne giren “iyi yönetim” kavramı vardır. İyi yönetim, özellikle küreselleşme sürecinde önemleri artan Dünya Bankası, OECD, Birleşmiş Milletler (BM) ve IMF gibi uluslararası kuruluşların geliştirmekte olan ülkelerde yürüttükleri kalkınma programları, teknik ve mali yardım ve kredi ilişkileri çerçevesinde bu ülkelerin yönetim sistemlerinin değerlendirilmesine yönelik teknik bir terim olarak geliştirilmiştir. Bu kapsamda geliştirmekte olan ülkelerin kamu yönetimlerine, küresel değişim doğrultusunda iyileştirilmeleri için ulaşmaları gereken hedef olarak gösterilmektedir (Saran, 2004: 22-23).

1.1.1.2.3 E-Devlet

Gelişen bilgi ve iletişim teknolojileriyle birlikte vatandaş-devlet ilişkisi de yeni bir boyut kazanmıştır. İnternet, web teknolojileri ve e-posta gibi yeni araçlar devlet-vatandaş iletişimi ve etkileşimini geliştirmekte ve etkili kılmada önemli fırsatlar sunmaktadır. Elektronik ticaretin, klasik ticaret ve piyasa anlayışına nazaran gerek zaman ve gerekse maliyet açısından daha ekonomik, etkin ve hızlı olması, bu kavramın farklı bir boyutta kamu yönetimine uyarlanarak kamu hizmetlerinin dijital ortama aktarılmasını gündeme gelmiştir. Böylece hantallaşmış, gereğinden fazla büyümüş, yüksek maliyetle daha az iş yapabilir hale gelmiş olan kamu yönetiminin iyileştirilmesi çabalarına çare olacağı ümidiyle, “elektronik devlet (e-devlet)”

kavramı ve bununla birlikte e-vatandaş, e-demokrasi.. gibi bir takım yeni kavramlar ortaya çıkmıştır (Şahin ve Örselli, 2010).

Bilgi toplumu yönetim anlayışının önemli araçlarından birisi olan e-devlet, “devlet işlerinin elektronik ortamda yapılması”nı ifade etmektedir. Fakat, ifade edilmek istenen husus aslında daha derindir. E-Devlet, gerçek hayattaki devletin, teknoloji olanaklarını kullanarak çağın gereklerine uygun olarak daha şeffaf, vatandaş odaklı, daha ucuz ve daha iyi çalışan bir idari yapı oluşturmak için yeniden yapılandırılmasıdır. Dolayısıyla, aynı zamanda kamusal işleyişte ve bürokraside köklü bir anlayış ve işleyiş değişikliğini ifade etmektedir (Şahin ve Örselli, 2010).

İnternetin yönetimde yoğun olarak kullanılması, çağımızın demokrasi anlayışını da etkilemiştir. Sanayi toplumunda yönetime katılım, sınırlı düzeyde ve genellikle seçimlere katılıma endekslenmiş bir biçimde ele alınırken, bilgi toplumunda İnternetin yaygın kullanımı, bu anlayışı dönüşüme uğratacak yetenekleri potansiyel olarak taşımaktadır (Alkan ve Şimşek, 1998: 179).

Bilgi toplumu savunucuları, bireyin ve sivil toplumun, politikaların belirlenmesini etkileme ve böylelikle kendi geleceklerine sahip çıkma potansiyelinin, bilgi ve iletişim teknolojileri ve özellikle İnternet sayesinde ve e-demokrasi, e-seçim, e-yönetişim gibi yönetime katılım yöntemleriyle, her geçen gün arttığını belirtmektedir (Uçkan, 2003). Buna göre, İnternetin belki de en demokratikleştirici yönü, insanlara daha büyük bir iletişim özgürlüğü sağlaması ve gruplar halinde örgütlenme ve iletişimde bulunma yeteneklerini artırmasıdır (Castells ve İnce, 2006: 70).

Görüldüğü gibi, varacağı sonuç ve etkileri hala kestirilemeyen bilgi toplumu sürecinden kamu yönetimi de derinden etkilenmektedir. Bu bağlamda, sanayi devriminin konjonktürel yapılanmasına koşut olarak Weberian bürokrasinin, katı, hiyerarşik, merkezi ve yasal-ussal ilkelerine göre biçimlenmiş olan kamu yönetimi, küresel bilgi toplum ve ekonomisinin dinamik süreç, ilişki ve yenilikleri karşısında yetersiz ve çözümsüz kalmıştır. Kamu yönetimi ile ilintilendirilen “yeni”, “işletmecî”, “piyasa odaklı”, “rekabetçi”, “girişimci”, “postbürokratik” ya da

“postmodern” gibi değişik sıfat, açılım ve yaklaşımlar, model ve tartışmalar, kamu yönetimi aygıt ve disiplininin içinde bulunduğu bu krizden kurtulması için bulunmaya çalışılan çözüm girişimleri ve çabaları olarak görülebilir.

Bilgi ve iletişim teknolojileri sayesinde küreselleşme, ekonomi ve uluslararası ilişkilerde karşılıklı bağımlılıkların egemen olduğu bilgi ve iletişim devriminin yönetsel yapısı da işbirliği ve ortaklıklar ekseninde evrimleşmektedir. Bilgi toplumunun etkisiyle devlet ve toplum arasındaki işbölümünün hiyerarşik niteliği de değişmiştir. Keskin uluslararası rekabet ve küreselleşmeye karşı ayakta kalma mücadelesi veren devlet, bunun için önceden tekelinde bulundurduğu bir dizi işlev, yetki ve sorumluluğu bilgi ve iletişim teknolojisinin olanaklarıyla bilinçlenip güç talep eden sivil topluma aktarmıştır. Artık tüm siyasal ve toplumsal süreç, ilişki ve kararlar devlet, yerel yönetimler, özel sektör, STK’ları, meslek örgütleri, gönüllü kuruluşlar ve üniversiteler gibi aktörler arasında beraberce düzenleme, yönlendirme, üretim ve yönetim temelinde yapılandırılacaktır (Nohutçu ve Balcı, 2008: 19).

Tüm bu tabloda “yönetim”in klasik, yöneten ve yönetilen varsayımına dayanan içeriği boşalırken; konuyla ilgili ve karardan etkilenen tüm aktörlerin “birlikte”, “beraber”, “ortaklaşa”, “işbirliği” içerisinde kendilerini yönetmesi anlayışı doğmuş ve “yönetişim” olarak telaffuz edilmeye başlanmıştır. Sonuçta, sanayi toplumunun “kamunun yönetilmesi” olarak yapılanan “kamu yönetimi” anlayışı, bilgi toplumunun henüz tamamlanmamış olan dokusal gelişiminde “kamunun yönetmesi” biçiminde kavramsallaşıp kurumsallaşmaya başlamıştır (Nohutçu ve Balcı, 2008:19).

Bu süreçte bilgi toplumunda devletin rolü ve sınırları yeniden belirlenmiş, siyasal sınırlar ve ulusal egemenlik anlayışı eski katılığını kaybetmiş, küresel sermayenin çizdiği etkinlik alanı içinde mal ve hizmet, teknoloji ve bilgi akışı hızlanmış, bireysel tercihlerin ve alt kimliklerin önem kazandığı yeni devlet anlayışı gelişmiştir. Keza, bilgi toplumu devleti, hukuka bağlı demokratik, adem-i merkeziyetçi, katılımcı, açık-şeffaf, sınırlı-çerçeve ve hakem devlet olarak ortaya çıkmıştır. Keza, bu süreçte, devletin küçültülmesi ve daha etkili ve verimli bir işleyişe kavuşturulması amacıyla “kamu yönetimi reformları” gündeme gelmiştir. Bu çerçevede önce, daha çok

kendisini özelleştirme politikaları ile gösteren deregülasyon uygulamaları, daha sonra ise regülasyon politikaları ve “düzenleyici kurullar” devreye sokulmuştur.

Bu çerçevede, görülmektedir ki, İnternet içeriğinin devlet eli ile düzenlenmesi sorununun bir alt bağlamını da “bilgi toplumu ve devlet/kamu yönetimi” ilişki ve etkileşimi oluşturmaktadır. Buna göre, İnternetin başrol oynadığı “bilgi toplumu” olgusu “devleti/kamu yönetimi”ni dönüştürürken, “devlet/kamu yönetimi”, bilgi toplumu ile gündeme gelen İnternet gibi yeni sorun alanlarına ilişkin belirsizlik ve dönüşümlere yanıt ve çözümler üretme, gelişen kavram, yapı ve yaklaşımları doğasına uyarlamaya çalışmaktadır. Yani, karşılıklı etkileşime dayalı olarak işleyen bir süreç bulunmaktadır. Bu süreçte, İnternet ve İnternetin içerik düzenlemesine ilişkin konularla ilgili olarak ortaya çıkan yönetsel yaklaşımın, “yönetişim” modeliyle çalışan “üst kurullar” olduğu görülmektedir.

1.1.1.3 Bilgi Toplumu Kuramına Yöneltilen Eleştiriler

Yukarıda kuramsal çerçevesini kısaca belirlemeye çalıştığımız bilgi toplumu olgusuna ve bilgi toplumu kuramcılarına yönelik bazı eleştiriler bulunmaktadır.

1.1.1.3.1 Tüm Dünya Bilgi Toplumu Aşamasında Değil

Bilgi toplumu ile ilgili eleştirilerden birisi, dünyadaki mevcut duruma bakıldığında, dünyaya egemen durumda olan ülkelerin dışında büyük çoğunluğun bilgi toplumu aşamasında olmadığı konusundadır. Bilgi toplumu olmayı belirleyecek dönüşümlerin, tüm toplumlarda aynı oranda ve düzeyde işlemediği bir gerçektir. Toplumların belli bir bölümü, sanayi sonrası dönüşümleri etkin bir şekilde yaşarken, geri kalan büyük çoğunluğun, tarım, sanayi ve ileri sanayi toplumu aşamalarını yaşamakta oldukları görülmektedir.

Nitekim, bilgi toplumu aşamasında olmayan bu büyük çoğunluğun bir kısmı tarım, sanayi ve kısmen de bilgi toplumu aşamasını birlikte ve sıkıştırarak yaşarken, önemli bir kısmı da sanayi öncesi toplum aşamasında yaşam mücadelesi vermektedir. Keza, sanayi toplumu olmanın aşamalarını tamamlamış ülkeler kolay bir biçimde bilgi

toplumuna geçerken henüz sanayileşmemiş ülkeler ise bilgi toplumuna geçiş konusunda ciddi sorunlar yaşamaktadır. Azgelişmiş ve gelişmekte olan ülkeler, bilgi toplumunun bilişim altyapısına sahip olmadıkları gibi, personel, kurumsal ve maddi altyapıları yeterli seviyede değildir (Kocacık, 2003: 9; Çoban, 1996: 60). Bu nedenle, ancak küreselleşme bağlamında ele alındığında dünyanın bilgi toplumu aşamasında olduğunun iddia edilebileceği dile getirilmektedir (Uçkan vd., 2005: 84).

Diğer yandan, azgelişmiş ülkeler ile bilgi toplumu seviyesine ulaşmış ülkeler arasındaki farkın giderek arttığı da gözlemlenmektedir. Gelişmiş ülkelerde bilişim teknolojisi ile yaratılan "Kuantum Sıçraması" azgelişmiş ülkeler karşısında, gelişmişlik farkının daha da açılmasına sebep olmaktadır (Çoban, 1996: 60). Bilgi hizmetleri artık ileri teknoloji ve sermaye gerektiren alanlar olarak ortaya çıkmaktadır. Bu gerçek bize bilgi toplumu olan ileri teknoloji ülkeleri ile gelişmekte olan ülkeler arasındaki farkın daha da açılacağını göstermektedir (Yücel, 2010).

Hatta, geri kalmışlık ve az gelişmişlik kavramlarının, ülkelerin ekonomik yetersizlikten dolayı temel eğitim, sağlık, konut, bilim vb. sorunları çözemeyiş anlamı içerdiği düşünülürse, dünyanın 4/5'inin en azından yakın bir gelecekte bilgi toplumu kavramını kendileri adına kullanamayacakları açıktır. Bu ülkeler, büyük bir olasılıkla, bilgiden para kazanan değil, ona para harcayan buna karşın bilgiyi, sahip oldukları altyapısal sorunlar nedeniyle, birey ve toplum düzeyinde kullanamayan toplumlar olacaklardır (Yılmaz, 2006: 154).

1.1.1.3.2 Toplamların Tarihsel ve Yapısal Gerçekleri Farklı

Bilgi toplumu eleştirilerinden bir diğeri ise, bilgi toplumu kuramcılarının toplumların farklı tarihsel ve yapısal özelliklere sahip oldukları gerçeğini göz ardı etmeleridir.² Tek düze yaklaşımların kuşkusuz en büyük problemi ülkelere ait belirli yerel koşul ve özellikleri görmemesi ve herkes için geçerli olabilecek bir formül ürettiğine inanmasıdır

² Yücesan-Özdemir, bilgi toplumuna ilişkin gösterge ve indekslerin "Gelişmekte olan ülkelerin kendi iktisadi, toplumsal ve siyasi yapıları içinde ne kadar anlamlı oldukları ve gerçeklikleri ne derece kavrayabildikleri soruludur" derken, bu konuda kullanılan niceliksel yöntemlerin "her toplumsal formasyona ilişkin somut tarihsel ilişkileri ya da özgül sebepleri analizin dışına iterek, toplumlara tarihsiz şablonlarla bakılmasına sebep olmaktadır" demektedir. (Yücesan-Özdemir, 2008: 34).

(Akdenizli, 2011). Halbuki, birbirlerinden etkilenseler de toplumların tarihsel serüvenleri, yaşadıkları tecrübeler ve yapısal özellikleri kendilerine özgü ve farklıdır ve bu nedenle ortaya çıkan her oluşuma benzer tepkiler vermezler.³ Dolayısıyla, Batılı toplumların kendi tarihsel ve toplumsal dinamiklerinin sonucu olarak yaşadıkları tarım toplumu, sanayi ve bilgi toplumu aşamalarının ortaya çıkardığı dönüşümlerin tarih, kültür, değerler sistemi ve siyasal yapıları farklı diğer toplumlar için anlamları ve etkileri de farklı olmaktadır (Bilgiç, 2008: 38).

Nitekim, Batılı gelişmiş toplumların yaşadıkları bilgi toplumu modeli, “farklı gelişme ritmi ve toplumsal yapı özelliklerine sahip toplumlarda, model ile toplumsal gerçeklerin birebir örtüşmüyor olması” nedeniyle uyumsuzluklardan kaynaklanan sorunlara neden olmaktadır (Törenli, 2004: 13; Kocacık, 2003: 9). Bilgi toplumu aşamasında bulunan, bilgi ekonomisine geçmiş ve bu bağlamda küresel ekonomiye eklemlenmesini tamamlamış gelişmiş ülkelerde geliştirilip uygulanan yönetsel ve örgütsel süreç, model ve tekniklerin, gelişmekte olan veya az gelişmiş ülkelerde uygulanması, bu ülkelerin farklı tarihsel ve yapısal özelliklere sahip olmalarından ve özellikle ekonomik temelin oturmaması ve hatta hiç olmaması nedenleriyle tepeden inmece bir şekil almakta, sürekli sorun, zorluk ve sıkıntılar doğurmaktadır (Nohutçu ve Balcı, 2008: 20-21).

Konuyla ilgili olarak yapılan eleştirilerin diğer bir boyutu da, bilgi toplumu aşamasında bulunmayan topluluklar bağlamında konunun kültürel-ideolojik çağrışımlara açık bir niteliğe sahip olduğudur.⁴ Bu eleştiriye göre, günümüzde bireyler ve toplumlar, aynı zamanda bir ölçüt durumuna getirilen bilgi toplumu kavramına dayalı yeni özellikleri ile tanımlanmakta, gelişmişlik düzeyleri bu

³ “Kapitalizmin yeniden yapılanmasıyla enformasyonalizmin yayılması küresel ölçekte birbirinden ayrılmaz süreçlerse de, toplumlar, tarihleri, kültürleri ve kurumlarının özelliklerine bağlı olarak bu tür süreçlere farklı tepki vermişler, bu süreçlerde farklı tutumları benimsemişlerdir. Dolayısıyla, yeni sistemde her yerde toplumsal biçimlerin homojenliğini çağrıştıracak olan bir ‘enformasyonel toplum’dan bahsetmek, bir yerde uygunsuz olur.” (Castells, 2008: 24)

⁴ “Sanayileşmiş ülkelerin kendi özgül tarihi ve toplumsal tecrübelerinden geniş bir zaman dilimi içinde süzerek oluşturdukları-ve bu nedenle öznel, kültürel ve ideolojik boyutlarını içselleştirerek nispeten görünmez kılabilindikleri- kavram ve yaklaşımlar, aynı tecrübeleri yaşamamış başka toplumsal ortamlara, gecikmişlik, ‘geri kalmışlık’ telaşı içinde alelacele tercüme edilirken, bunların üstü örtülü olarak içlerinde taşıdıkları öznel, kültürel ve ideolojik yüklenimler açıkça ve kimi zaman çok kaba bir biçimde ortaya çıkmaktadır.” (Avcı, 1990: 46).

özelliklere sahip olma oranı ile belirlenmektedir. Bilim, eğitim, politika, yönetim vb. birçok alanda ve her düzeyde, anlam içeriği yeterince sorgulanmadan/kavranmadan kullanılan "bilgi toplumu" kavramı, bir yanıyla "slogan" ve "ideoloji"ye bir yanıyla da "teknolojik bir tehdit"e dönüştürülmüştür.⁵ Çağa adını verme iddiasındaki kavramın "slogan", "ideoloji" ve "tehdit" düzeyinde değerlendirilmesi, tehlikeli bir şekilde, tartışma zeminini bilimsellikten uzaklaştırmaktadır (Yılmaz, 2006: 148).

1.1.1.3.3 Kapitalizmde Geline Son Nokta: Bilgi Toplumu

Bugünün küresel dünyasından ve yaşanan gerçeklerden yola çıkan kimi yazarlar, bilgi toplumu sürecini, kapitalizmin dönemsel olarak kendisini yeniden yapılandırması süreci olarak açıklamaktadır. Buna göre, daha önce bazı krizlerin ardından olduğu gibi 1970'lerden sonra da kapitalizm, kendisini iktisadi, siyasi ve ideolojik yapılarda yeniden yapılandırmaktadır. Bilgi toplumu işte bu son yapılandırmanın adıdır (Yücesan-Özdemir, 2008: 15; Castells, 2008: 5-16).

Bilgi toplumu kuramına yönelik en köklü eleştiriyi ortaya koyan bu görüşe göre kapitalizm, ekonomi politik bir sistem olarak, toplumsal ortamın keşfedilmiş olanaklarını güncelleştirme açısından sona ermemiştir. Bilgi toplumu kavramsallaştırması, kapitalizmin içinde bulunduğu yeni kriz şartlarını aşmak için bilgi iletişim teknolojilerinin dönüştürücü potansiyelinin devreye sokulduğu yeni dönemi anlatmaktadır. Dolayısıyla bilgi toplumunu, yeni bir toplumsal dönem olarak değil, kapitalizmin krizini aşmak için bilgi iletişim teknolojilerinin desteğinde yeni politikaları ve uygulamaları uluslararası bir meşruluk şemsiyesi altında hayata geçirme eylemi olarak tanımlamak mümkündür (Törenli, 2004: 112).

Bu çerçevede bilgi toplumu, küreselleşen dünya ekonomisi içerisinde, genel olarak bilimin ve teknolojinin, özellikle de bilgi ve iletişim teknolojilerinin, gelişmiş

⁵ "Slogandır; çünkü, toplum; kendi üretmediği sistemleri bu söylemin içinde kalarak, ancak slogan düzeyinde anlatabiliyor. İdeolojidir; çünkü tarihsel, toplumsal, ekonomik ve kültürel değişimin tüm boyutlarını yeni bir bakış açısıyla değerlendirmekte ve çözümlemekte; ayrıca bu yaklaşımı, kabul edilmesi gereken 'doğru' olarak sunmaktadır. Bunun dışında, 'teknolojik tehdit'tir; çünkü 'bilgisayar'da somutlaşan yeni iletişim ve enformasyon teknolojilerine sahip olmayan ülke, toplum ve bireylerin 'geri kalmışlığa' mahkum olacağını öne sürmektedir." (Yılmaz, 2006: 148)

toplumların ticari-ekonomik rekabet güçlerini artırma hedeflerine ulaşması için daha çok olanak sağlamasına yönelik bir politikayı ifade etmektedir. Bu durum, gelişmiş ülkelere, merkezleri ülkelerinde bulunan çokuluslu şirketlerin önünü açmaya yarayan politikaları oluşturma ve uygulamaya koyma olanağı sunarken, azgelişmiş ülkeler açısından ekonomik kalkınma sorununun ‘bilgi toplumu olmakla’ aşılabileceği umuduyla küresel kapitalist sisteme eklenme sürecini işletmektedir (Yücesan-Özdemir, 2008: 23-24; Törenli, 2004: 111).

Benzer şekilde, Castells de kapitalizmin bugünkü konumuna gelmesinin, enformasyon teknolojilerindeki gelişmeler sayesinde gerçekleştiği ve ortaya çıkan yeni teknolojik paradigmanın, sosyo-ekonomik ilişkilerin temelini oluşturduğu düşüncesindedir. Bu devreyi tanımlamak üzere “Enformasyonel Kapitalizm” terimini kullanan yazar, kar, özel mülkiyet, piyasa ilkeleri gibi kapitalizme özgü ekonomik unsurların hala geçerli olduğu, öte yandan yenilerin sahip olduğu esneklik ve küresel erişim olanakları sayesinde önceki kapitalist dönemlere nazaran, daha az bağışlayıcı bir kapitalizmin varlığından söz etmektedir (Castells, 2008: 5-16). Keza, Suraz-Villa, günümüzün ekonomik yapısını tanımlamak için “teknokapitalizm” kavramını kullanmaktadır (marin, 2010).

1.1.2 Bilgi Toplumunun Sorunları

Bilgi toplumunu sadece faydaları açısından tek yönlü olarak değerlendirmek, bilgi toplumu olmanın gündeme getirdiği sorunları ve taşıdığı potansiyel riskleri ve tehlikeleri görmemize engel olabilecektir. Bu nedenle, bilgi toplumu olmanın maliyetlerinin neler olduğunun irdelenmesi gerekmektedir.

1.1.2.1 ‘Büyük Birader’ Ya Da ‘Gözetim Toplumu’ Korkusu

Günümüzde bilgi toplumu kavramı tartışılırken yeni teknolojilerin gelişim sürecine paralel olarak ağırlık kazanan modern gözetimin tehlikelerine dikkat çeken tüm kaynaklarda atıfta bulunulan bir eser Orwell’in meşhur ‘1984’ isimli kitabıdır. Bunun yanında Huxley’in ‘Cesur Yeni Dünya’ ve Zamyatin’in ‘Biz’ adlı kitapları da 50-60 yıl önce geleceğe dönük tahminleri içermeleri açısından dikkate değerdir. ‘1984’ ve

‘Biz’ insanın kişiliğinden uzaklaştırıldığı tamamen bürokratikleşmiş bir toplumu ele alırken, bu toplumlarda yer yer fiziki baskıya da varan ideolojik ve psikolojik bir yönlendirmeyi tasvir etmektedir. Huxley’in çalışmasında ise insanın bir tür makineye dönüştürülmeye çalışılması ele alınmaktadır. Zamyatin, ‘Biz’de insanların insan doğası gereği olan taleplerini yok etmek için uygulanan beyin operasyonlarından bahsederken, ‘Cesur Yeni Dünya’da çeşitli ilaçlar ve yapay biyolojik yöntemlerin uygulanması konu edilmektedir (Akin, 2006).

Orwell ise ‘1984’te, ‘Büyük Birader/Ağabey’ adındaki dev bir merkezi-bürokratik güç/organizasyon tarafından sürekli gözetlenip, baskı ve denetim altında tutulan bir toplumu son derece çarpıcı bir biçimde anlatmaktadır. Orwell, bu romanıyla sınırsız baskıyı ve beyin yıkamayı öne çıkarmakta ve devletin her şeyi denetim altında tuttuğu, en küçük bir aykırılığa ve bireyselliğe izin vermediği, resmi ideolojinin bütün tarih ve dili kendine göre kurguladığı bir toplum ütopyasından bahsetmektedir. Orwel’in çizdiği karanlık senaryoda, ‘Büyük Birader’ metaforuyla, vatandaşların düşüncelerinin dahi denetlendiği, totaliter bir topluma doğru gidilmesine dikkat çekilmektedir (Orwel, 1985).

Ancak gözetim konusunda en çarpıcı ve etraflı analizi, postmodern teorisinin en önemli isimlerinden Michel Foucault yapmıştır. Foucault’dan sonra gözetim sosyal teoride merkezi bir öneme sahip olmuştur. Foucault, modern toplumda gözetimi anlatmak için, Bantham’ın ‘Panopticon Hapishanesi’ metaforunu kullanmış ve gözetimi sadece örgütler açısından değil, toplumun genelinde daha geniş bir disiplin bağlamında ele almıştır. Foucault’ya göre, özgürlüğü keşfeden “Aydınlanma Çağı”, disiplinleri de keşfetmiş ve modern toplum bir anlamda “gözetim” ve “disiplin”in hakim olduğu bir toplum haline gelmiştir (Bozkurt, 2011)..

Foucault’un da son derece çarpıcı bir biçimde ortaya koyduğu, “bir veya daha çok kişinin iletişim ya da eyleminin sistematik olarak araştırılması ya da izlenmesi” (Bogonikolos) olan gözetim kavramı son dönemde, İnternet gibi enformasyon teknolojilerinin gelişim sürecine paralel olarak özel bir önem kazanmıştır. Bu sayede toplanan kişisel enformasyonun miktarı sürekli artarken, enformasyon teknolojileri,

potansiyel olarak olağanüstü kalabalık kitleleri, gözetimciler için, görünmeksizin ya da bilinmeksizin izlenebilir hale getirmiştir (Bozkurt, 2011).

Dolayısıyla, teknolojik gelişmelerin, toplumların giderek bir izleme ve gözetleme toplumu olmasına doğru evrimlenmesindeki rolü büyüktür. Bu durum, toplumları kitle iletişim araçları ve teknoloji aracılığıyla yönlendirme olgusu ve bilgisayarlar ve özellikle İnternet aracılığıyla kolayca manipüle etmek ve daha sıkı bir denetim altına almak isteyenlerin olabileceği endişesini beraberinde getirmektedir. Bu nedenle, söz konusu endişeleri de içerisine alan bir kavram olarak “gözetim toplumu/surveillance society” kavramı, insanoğlunun içinde bulunduğu bu dönemi tanımlamak için literatürde sıklıkla kullanılır olmuştur (Stanley and B. Steinhardt, 2003: 1).

Keza, bugün bilgi toplumunun fertleri kredi kartı harcamalarından, gelir transferine, parmak izinden işlediği suçlara, kütüphane kayıtlarından İnternet’te ziyaret ettiği web sitelerine, telefon görüşmelerine ve en uçta genetik şifrelerine kadar tam anlamıyla erişilebilir, dolayısıyla etkilenebilir, saldırılara maruz kalabilir ve gözetlenebilir konuma gelmiştir. Bu şekilde “Büyük Birader”in gözetimi altında sürdürülen bir yaşam, belki de, birçoklarınca yorumlandığı gibi özellikle Stalin dönemi Sovyet komünist düzeni ve onun toplumuna değil de, Amerikalıların deyimiyle “Yeni Dünya Düzeni” ve bilgi toplumuna özgüdür (Gültan, 2009). Özellikle ABD’ye yapılan 11 Eylül saldırılarından sonra güvenlik gerekçesiyle İnternet üzerinden gözetimin giderek yaygınlaşarak, adeta ‘küresel gözetim’ boyutuna gelmesi bu görüşü destekler niteliktedir. Nitekim, ABD diğer hükümetleri ve potansiyel suçluları kontrol edebilme hayaliyle “teknolojik jandarmalık” yapmayı kendisinden çevreye de ihraç etmiştir (Lyon and Höller, 1997).⁶

Keza, küresel gözetim metaforunun ulaştığı en uç nokta olarak, çok geniş bir kullanım alanı olan ECHOLON sisteminden bahsetmek yerinde olacaktır. Bütün dünya üzerindeki uydu tabanlı iletişimi izleyen beş devletin (ABD, İngiltere, Kanada, Avustralya ve Yeni Zelanda) gizli servislerinin ortaklaşa çalışması sonucu kurulan

⁶ Dünya üzerinde kullanılmakta olan tüm izleme sistemleri hakkında ayrıntılı bilgi için bkz. <http://www.fas.org/irp/world> (14.12.2009)

ECHELON, dünyanın çeşitli yerlerine konuşlandırılan antenler sayesinde, telefon görüşmeleri ve elektronik posta trafiği dahil olmak üzere tüm uydu tabanlı iletişimi gözetlemektedir. Sistem sayesinde elde edilen ham veriler özel yöntemlerle çözümlenerek iletişimin içeriği öğrenilmektedir. Sistemin ulusal güvenliği sağlamak amaçlı olarak kurulduğu söylenilmekle beraber, resmi, sivil tüm iletişimin kontrol edildiği ve ticari sırların ve diğer devletlere ait stratejik bilgilerin de elde edildiği, 1988’de Avrupa Parlamentosu’nun bir raporunda yer almıştır. ECHELON sisteminin dünya İnternet trafiğinin %90’ını kontrol ettiği belirtilmektedir. (European Parliament Temporary Committee on the ECHELON Interception System, 2001).

Bunun yanında verilerin merkezi bir sistem dahilinde izlenmesiyle kişiler hakkında çeşitli tahmin ve öngörülerde bulunmak amacını taşıyan bir başka teknik ise “veri madenciliği/data mining”dir. Veri madenciliği sisteminde siber uzayda kişilerin gerçekleştirdiği işlemlerden elde edilen tüm veriler bir programa yüklenerek kişi hakkındaki davranış eğilimleri, kısa ve uzun vadede gerçekleştirmesi muhtemel eylemlerin belirlenmesi gibi sonuçlara ulaşılmaya çalışılmaktadır (Beceni, 2004: 14). Nitekim, ABD tarafından geliştirilen “Carnivore ve Total Information Awareness” sistemleri, siber uzaydaki veri dolaşımını izleyerek kişiler hakkında bilgi toplamakta ve bu bilgiler tasnif edilerek kişinin suç işleme potansiyeli tespit edilmeye çalışılmaktadır (Stanley and Steinhardt, 2003: 12). Keza, günümüzde sosyal ağlar kişisel bilgi ve verilerin paylaşımını temin etmekte, akıllı telefonlar baz istasyonları, GPS ve kablosuz ağ bağlantıları yoluyla takip edilebilme ve bu yer bilgileri aracılığı ile birey hakkında hassas verilere ulaşılabilme imkanı sağlamaktadır.

Bilgi ve iletişim teknolojileri farklı kurum ve örgütlerin elinde insanlığın aleyhine de kullanılabilecek özelliktedir. Örneğin, bilgi toplumunun sunmuş olduğu imkan ve kolaylıklar vatandaşların özel hayatlarını denetim altına almak, sivil toplumu bastırmak isteyen hükümetlere de, suç işlemek üzere bilgi toplamak isteyen suç örgütlerine de benzer imkanları sunmaktadır (Erdoğan, 2010: 57). Nitekim, enformasyon teknolojisi toplumda sosyal iktidarın fiilen az sayıda karar alıcının elinde toplanmasına ve böylece egemen çıkar gruplarının siyasi sistem içindeki konumlarını pekiştirmelerine yol açabilmektedir. Demokratik ülkelerde dahi kitle

iletiřim aralarının tekellerin eline gemesi ve bylelikle kamuoyunun gdml olarak řekillendirilmesi mmkn olabilmektedir. Enformasyon teknolojisinin imkanlarına dayanarak, otoriter ve totaliter siyasi iktidar yapıları tesis edilebilir ve bu iktidarlar iletiřim araları sayesinde geniř toplum kesimlerinin maniplasyonunu ve denetimini daha rafine yntemlerle temin edebilmektedir (Erdoğan, 2010: 57-58).

Bu erevede Kongar'ın tespiti de nemlidir. Bir toplumun endstri devrimini yařaması nasıl onu zorunlu olarak demokrasiye deėil de, Almanya ve İtalya'da grldė gibi, ırkı ya da Rusya'da ve in'de grldė gibi sınıfsal diktatrlklere dnřmesine yol aıyorsa, aynı biimde iletiřim-biliřim devrimi de zorunlu olarak temel hak ve zgrlklerin geliřmesine deėil, tam tersine bunların denetlenmesine yol aan etkiler de yapabilir. Bu aıdan, bilgi aėında ilerleyen teknoloji, bireysel hak ve zgrlklerin geliřmesi ynnde kullanılabileceėi gibi kısıtlanması ynnde de kullanılabilir (Kongar, 2001: 39).

Diėer yandan, bilgi ve iletiřim teknolojisindeki geliřmelerin bilginin yeniden merkezileřmesine yol atıėı ve bilginin dev okuluslu řirketlerin karlarını arttırmada ve bireyler zerinde daha sıkı bir kontrol saėlamada kullanılacaėı endiřesine sahip olanlar bir hayli fazladır. Buna gre, biliřim teknolojisindeki geliřmeler zerk, zgn ve farklı kltrel oluřumlara imkan vermemekte, aksine dnya apında egemen, bařat ve tek bir kltrn oluřumuna katkıda bulunmaktadır (Hamelink, 1991: 21). Bilgi toplumu efsanesi biliřim devrimini bařlatan ve ynetenlerin ıkarlarına hizmet etmektedir (Trenli, 2009). Geniř kitleler iin biliřim teknolojileri ve bilgi toplumunun nemli bir vaadi bulunmamakta; bu insanlar bilgi toplumunda bilgisayar kontroll kaybedenler olarak kalmaya devam etmektedirler (Hamelink, 1991: 21).

1.1.2.2 Sayısal Uurum

Bilgi toplumu ile ilgili gndeme gelen konulardan birisi de “sayısal uurum” sorunudur. Bilgi ve iletiřim teknolojileri alanında lkeler arasındaki ve lkeler iindeki eřiřsizlik olgusu 1970'lerden bu yana tartıřılmakta ve “bilgi yoksulları/bilgi zenginleri” gibi kavramlarla ifade edilmektedir (TBİTAK, 2002:10). BM, G8,

OECD ve Dünya Bilgi Toplumu Zirvelerinde tartışılan ve çözüm bulunmaya çalışılan bu konu, önemini ve güncelliğini korumaktadır.

Günümüzde “sayısal bölünme” veya “sayısal uçurum” olarak adlandırılan, “coğrafi, sosyo-ekonomik koşulları farklı kurumlar ve bireylerin, bilgi ve haberleşme teknolojilerine erişim olanakları açısından eşit konumda olmayışları”nı ifade eden konu, gerek ülkelerin kendi içlerindeki bölgesel farklılıklardan, gerekse ülkeler arasındaki gelişmişlik düzeylerindeki farklılıklardan kaynaklanan eşitsizlikler nedeniyle sosyal açıdan endişe kaynağı haline gelmiştir (Başaran, 2005: 49).

Bu nedenle bugün, sayısal uçurum konusu, sadece uluslararası boyutuyla ve küresel eşitsizlik yönüyle değil, bilgi toplumu aşamasına ulaşmış bulunan ABD’den Avrupa’ya kadar en önemli sorunlardan birisidir. Sayısal uçurum, tüm dünya ölçeğinde ülkeler arasında iki kutuplu bir ayrıma neden olurken, bilgi toplumu olarak tanımlanan toplumlarda da iki parçalı bir toplumun ortaya çıkma tehlikesini beraberinde getirmektedir. Nitekim, bilişim devriminin gelişmiş olan ülkeler ile geri kalmış ve gelişmekte olan ülkeler arasındaki farkı gelişmiş ülkeler lehine daha da açtığı; geri kalmış ve gelişmekte olan ülkelerin toplumlarının üretilen katma değerden daha çok daha az pay aldığı dile getirilmektedir (TÜBİTAK, 2002: 10).

Sayısal uçurum konusu “elektronik sömürgecilik” olarak da ele alınmaktadır. Buna göre, bilgi zengini ile bilgi yoksulu dünyanın gelişmiş ve gelişmemiş bölgeleri arasında zamanla daha da derinleşen uçurum nedeniyle, giderek genişleyen bir kitle için, “küreselleşme” olgusu aslında, “yeni bir kolonileşme düzeni”, “bilgi toplumu” da, “kapitalist sömürünün devam ettiği bir yapı” olarak ortaya çıkmaktadır (Gültan, 2009). Fakat ilginç olan, küreselleşme sürecinin meydana getirdiği bu eşitsizlik ve adaletsizliğin yine bilgi ve iletişim teknolojileri eliyle ortadan kaldırılabileceği iddia edilmektedir (Yücesan-Özdemir, 2008: 20-21, 68-74).

1.1.2.3 Güvenlik Korkusu Ya Da Risk Toplumu

Bilgi toplumu öncesi geleneksel toplumlarda kötülüğün kaynağı olarak bilgi yoksunluğu veya bilgiye ulaşamamış olunması görülürdü. Oysa ki, ironik bir

şekilde bilgi toplumunda insanları tehlikeli durumlara sokan şeylerin çoğu bilgiden kaynaklanmaktadır. Yine ironik olarak daha fazla bağımsızlık güdüsü ile gelişen teknolojinin varlığı, insanın kişisel bağımsızlığını, mahremiyetini ve güvenliğini tehdit eden riskleri de beraberinde getirmektedir. Bilgi toplumunun aynı zamanda bir “Risk toplumu” olduğunu ifade eden kuramcılardan Beck ve Giddens, bilgi toplumlarında artık “tehlikenin kaynağının cehalet değil bilgi” olduğuna dikkat çekmekte ve bilimin sorunlara çözüm bulmaya çalışırken yeni sorun/risk alanları oluşturduğunu ifade etmektedir (Beck, 2002; Giddens, 1998). Teknoloji modern yaşamın karmaşıklığını azaltma konusunda kolaylıklar sağlarken, özgürlükler oluştururken, aynı zamanda bağımlılıklar, denetim ve kontrol mekanizmaları, yeni ihtiyaç alanları ve baskı araçları da meydana getirmeye de neden olmaktadır (TMMOB Elektrik Mühendisleri Odası, 2009: 29-30).

Bilim ve teknolojinin egemenliğinde ortaya çıkan risk ve tehlikeler adeta Frankenstein efsanelerini çağrıştırmaktadır. Mucidini devre dışı bırakarak egemenliğini ilan eden ve topluma büyük zararlar veren bir ucubenin anlatıldığı bu efsane, aslında bilimsel ve teknolojik gelişmelerin potansiyel olarak içlerinde barındırdıkları tehlikeye ve taşıdıkları risklerin boyutlarına işaret etmektedir. Nitekim, kontrol edilmesi son derece güç nükleer enerjinin, laboratuvar ortamlarında yapılan denemelerin, genetik mühendisliğindeki gelişmelerin, kimyasal ve biyolojik silahlar alanındaki teknolojik ilerlemelerin, bilişim alanındaki baş döndürücü gelişmelerin taşıdığı tehlike ve riskler, insan yaşamını ve doğal hayatı ciddi anlamda tehdit etme potansiyeline sahiptir.

Günümüz bilgi çağında, bilgi ve iletişim teknolojilerinde yaşanan gelişmelerin meydana getirdiği değişikliklerin yaşamımızın kalitesini nasıl etkilediği, birçok sosyal bilimci tarafından tartışma konusu yapılmaktadır. Dünya çapında sürdürülen bilimsel çalışmaların aydınlanmadan miras almış olduğu ilerlemeci doğası, yaşanan bu süreçlerin doğurduğu ya da taşıdığı riskleri çoğu kez tartışma dışı bırakmaya çalışsa da, bu gelişmelerin insani varoluşumuzun ontolojik temelleri ile ne derece uyumlu bir yapı içinde olduğu sorgulanmaktadır (Şan ve Hira, 2009).

Bu anlamda teknolojik ve bilimsel gelişmelerin, başka bir deyişle niceliksel gelişmelerin insanların varoluşsal duruşlarında ortaya çıkardığı tahribattan söz edilmektedir. Bir “mit” olarak sürekli pompalanan bilgi toplumu, maddi ve teknolojik gelişmenin insani gelişmeyi sağlayacağı varsayımına dayanmaktaydı. Oysaki teknolojik ilerleme ile gelen kitle kısımları ve küresel anlamda yaşanan insanlık trajedileri bunun hiçte öyle olmadığını göstermektedir. (Şan ve Hira, 2009).

Bilgi ve iletişim teknolojileri, genetik, tıp, astronomi, tarım, ekonomi vb. alanlarında yaşanan ilerlemeler gelişmeyi anlatmakta, fakat ekolojik riskler (eko-sistemin bozulması, bitki ve hayvan varlığının imhası, nehirlerin kirlenmesi, okyanus-deniz, hava kirliliği vb.), sosyal riskler (ailelerin dağılması, ferdiyetçilik, toplumsal yozlaşma, yalnızlık, yabancılaşıma, madde bağımlılığı, suç ve suçluluğun artması, terör, açlık ve kıtlık, işsizlik, gelir dağılımı bozukluğu vb.), teknolojik riskler (kitle imha silahları üretilmesi, manyetik kirlenme, özel hayatın gizliliğine tecavüzler vb.), kültürel riskler (kültür emperyalizmi, yerli toplum ve değerlerin yok oluşu vb.) günümüz sanayi sonrası toplumunun, aynı zamanda risk toplumuna da dönüştüğünün sinyallerini vermektedir (Öngören, 2005: 78-80).

Bugün dünyanın dört bir yanında, suç örgütleri, mafya tipi örgütlenmeler, zihinsel hiperaktiviteyi ve yasak arzuları kışkırtacak araçların yanı sıra, sofistike silahlardan insan bedenine dek uzanan bir yelpazede toplumların talep ettiği her türlü yasadışı ticareti sunarak küresel ve enformasyonel hale gelmiştir (Castells, 2008: 2).

Görülmektedir ki, insanoğlunun iyiliği, refahı, mutluluğu için olduğu kadar, tam tersi yönde de kullanılabilen teknolojik gelişmelerin hızına ayak uydurması hiç de kolay görünmeyen hukuki sistem eksikliği, varolan hukuk düzenlemelerinin de küresel çapta uygulanabilir olmayışı sonucunda, elektronik sahtekarlık, vandalizm, müstehcenlik, çocuk istismarı, mahremiyete saldırı, siber terörizm, ırkçılık ve şiddet gibi her geçen gün çeşitlenen bu çağa özgü suçlar ortaya çıkartmaktadır. Her türlü metin, görüntü, veri ve bilginin İnternet aracılığı ile denetimsiz biçimde akışı, küresel ağlara bağlı kitlelerin karşı karşıya kaldığı bahsi geçen tehlikeleri bertaraf edecek teknolojik çözümlerin de herkes tarafından etkin olarak kullanılamaması, hukukun

ise yeterince caydırıcı olamaması, bilgi ve iletişim teknolojilerine sahip kesimde, ciddi bireysel ve toplumsal sorunlara neden olmaktadır (Gültan, 2009).

1.1.2.4 Tüketim Toplumu ve Yabancılaşma

Bilgi toplumuyla ilgili gündeme gelen eleştiri konularından birisi de “tüketim toplumu” ve “yabancılaşma” olgusudur. Nitekim, sanayi toplumunda üretimin, sanayi sonrası toplumlarda ise tüketimin sembol olduğu gerçeğinden hareket eden sosyal bilimciler, tüketim toplumu ve yabancılaşma kavramlarıyla yaşanan değişimleri analiz etmeye çalışmışlardır (Şan ve Hira, 2009).

Tüketim toplumunda, kitle kültürü sunduğu bütün araç ve kolaylıklarla, bireysellik üzerindeki toplumsal baskıları güçlendirmekte ve bireyin direnme gücünü, modern toplumun atomize edici işleyişi içinde kendini koruma imkanını elinden almaktadır (Horkheimer, 1990:166). İnsan geçmiş dönemdeki baskı yöntemlerine ve pratiklerine oranla çok daha ince ve etkin yöntem ve pratiklerle cendere altında tutulmaktadır. Tüketim toplumu ve tüketim kültürü, bireyleri tüketime dayalı yaşam biçimlerini satın almaya zorlayan yanlış ve sahte ihtiyaçlar üretmektedir (Jameson, 1997: 104).

Diğer bir açıdan, "bilgi toplumu" kavramı, bugün “piyasa ekonomisi” bağlamında düşünüldüğünde, özünde paraya dönüşen her malın daha çok üretilmesine ancak bunun için de toplum tarafından daha çok tüketilmesine dayalıdır. Bu döngü, piyasa ekonomisinin egemen olduğu toplumun "tüketici toplum" olarak adlandırılmasına yol açmaktadır (Mattelart, 2004: 73-74). "Tüketici toplum", toplumu, sınırları her gün genişleyen biçimde tüketici yapmak için başta reklamlar olmak üzere çeşitli pazarlama teknikleriyle, üretilen ürünün alınması gerektiğine, onsuz yaşanamayacağına inandırılmasıyla oluşturulmaktadır. Bir süre sonra bu ürün insanı yönlendirir duruma gelmekte; bu yönlendirme, aynı zamanda, insanın, ürettiği ürüne, dolayısıyla kendisine yabancılaşması anlamına gelmektedir.

“İnsanın kendi özünden, ürününden, doğal ve toplumsal çevresinden koparak onların egemenliği altına girmesi” olarak tanımlanan (Tolan, 1980: 37-38) yabancılaşma olgusunu, bilgi ve iletişim teknolojilerinin sunduğu olanaklarla açıklayanlar da

bulunmaktadır. Buna göre, bilgi ve iletişim teknolojileri formel ilişkilerdeki kolaylığın yanında insanlar arasındaki sosyal ilişkilerde bir azalma ve topluma yabancılaşma, toplumdan kopma gibi sakıncaları da beraberinde getirmektedir (Yücel, 2010). Yüz yüze yürütülen insan ilişkileri yerini makine-insan ilişkisine, gerçek yaşam yerini sanal gerçeklik uygulamalarına bırakmaktadır. Zamanının büyük bölümünü bilgisayar karşısında geçiren insanların en belirgin yönü, içe kapanma ve kendini soyutlama olarak nitelenebilir (Başbakanlık, 2002: 270-271; Gültan, 2009). Araştırmalar, belli koşullar altında, İnternet kullanımının yalnızlığı, yabancılaşma duygularını hatta depresyonu derinleştirdiğini göstermektedir (Castells, 2008: 477).

Nitekim, Finkelkraut İnternetin geleceğiyle ilgili yorum yaparken televizyonu ve televizyonun geçirdiği değişimin önemine vurgu yapmaktadır. Buna göre, televizyon aslında insanları özgürleştirmemiş tam tersine onları bağımlı birer varlık yapmıştır. Sinemadan televizyona geçiş bireyi kendisine yabancılaştırmış, kendisini başka bir iradeye teslim etmiştir. Gücün verdiği sarhoşlukla televizyon seyircisi kendi arzularının kölesi, sınırsız ve keyfi gücünün tutsağı haline gelmiştir. İstekleriyle çevrelenen, kendi arzu ve sabırsızlıklarının hemen tatmin edilmesini isteyen, elinde televizyon kumandası olan birey aslında özgürleşmemiş, karşı koyamadığı sınırsız özgürlük duygularına tutsak edilmiştir. Yasaklanmış ve sınırlanmış olan kendi öz benliğini bulabilmesi dışında hiçbir şey onun için yasak olmamaktadır. Bu tutsaklık her geçen gün daha da ağırlaşmaktadır. Kanallar arasında zapping yapma gücüne bir de İnternette sörf yapma ve tıklama gücü eklenmiştir (Tarcan, 2005: 2-9).⁷

1.1.2.5 Bilgi Kirliliği ve Enformatik Cehalet

Bilgi toplumunun gündeme getirdiği sorunlardan birisi de “bilgi kirliliği” dir. Geniş anlamı ile bilgi öyle bir şey ki, yokluğu mutlaka kötü şeyler doğuruyor ama varlığı ve çokluğu da her zaman hayra dalalet etmiyor. Bu nedenle postmodern toplum bilgi yoksunluğu tehlikesine karşı geleceği bilgi teknolojilerinde görürken, başka bir tehlike ile karşılaşmaktadır: Bilgi fetişizmi (Kozanoğlu, 1997:106). Bilgi toplumunda

⁷ Sartori de benzer bir yaklaşımla dijital çağın rahatlığını uyuşturucunun sağladığı rahatlığa benzetir. (Sartori, 2004: 44)

kişiler bireysel bazda, aşırı bilgi yüklemesi ile karşı karşıya kalmakta, enformasyon denizinde boğulmama savaşı vermektedirler. Dolayısıyla, “doğru” ve “yararlı” enformasyona ulaşmak bilgi toplumu fertleri için çoğu zaman önemli bir sorun haline gelmektedir. Bu durum “bilgi kirlenmesi” kavramını gündeme getirmektedir.

Naisbitt, bu durumu, “enformasyon içinde yüzerken bilgi için açlıktan ölmek” olarak ifade etmekte, kontrol ve organize edilmeyen enformasyon kirlenmesi karmaşasının, bilgi işçisinin düşmanı haline geldiğini dile getirmektedir (Megatrends, 1984: 17). Postman, bilgisayar teknolojileri ile gelinen bu noktayı “bilgiye gark olmak” olarak nitelemektedir. Fakat üretim malzemesi ve tüketilen bir ürün olarak bilgi, bir atık haline gelmiştir ve bu haliyle bilgi artık insanların en temel sorunlarını cevaplamaktan acizdir (Postman, 2006: 84-85).

Post-modern düzende sesini duyurma olanakları artan birey ve kitleler, diğer taraftan, çokseslilikten kaynaklanan bilgi kirlenmesine de yol açabilen bu karmaşık ortamda etkin olmakta zorlanmaktadır. Çok sayıdaki dağınık, hatta çelişkili ve bütünsellikten yoksun bilgi karşısındaki bireyin birikimini düzenlemesi için harcadığı çaba ve zaman, gün geçtikçe artmakta, verimlilik ise, tam tersine, düşmektedir (Gültan, 2009).

Keza, İnternet barındırdığı 716.822.317 adet web sitesi (Netcraft, 2013), 252 milyon alan adı (Verisign, 2013), milyonlarca e-posta grupları, tartışma forumları, web sayfaları, sohbet odaları aracılığıyla kamuoyunun ‘her gün doğrulanmamış bilgilerle’ karşı karşıya kalması ve bunun sonucu olarak da ‘bilgi kirliliği’ne neden olduğu dile getirilmektedir (AREM, 2008: 6). İnternet ortamında önemli olan ile önemsiz olanın bir arada sergilenmesi, İnternetin bilgi çöplüğü olarak da değerlendirilmesine neden olmaktadır. Keza, önemli olanın önemsiz olandan, uygun olanın uygun olmayandan, faydalı olanın faydasız olandan bir biçimde ayrılmaması durumunda her şeyin aynı oranda ilgi çekici ve sıkıcı olacağı; dolayısıyla, kişinin kendini yeniden günümüz çağının kayıtsızlığında bulacağı ifade edilmektedir (Dreyfus, 2002: 110).

Bilgi ve iletişim teknolojileri, kişisel gelişim için gerekli olan tüm bilgileri kolayca erişilebilir kılmıştır. Bilgiye ulaşmak için sınır, kurum, zaman ve mekan kavramı

büyük oranda aşınmıştır. İnsanlar zamanlarının çoğunu, bilgi ve iletişim teknolojilerinin ürünü olan cihazların karşısında değerlendirilmektedir. Fakat buna rağmen içerikte büyük bir yozlaşma, anlayışta kısırlaşma yaşanmakta ve “enformatik cehalet” yaygınlaşmaktadır (Avcı, 1990: 71-75). Bilişim alanındaki yoğun gelişme ve ilerleme aynı oranda toplumsal ve bireysel bilgiyi sığlaştırma tehlikesine de kapı aralamaktadır. Bilgi bollaşmakta, anlayışlar ise daralmaktadır. Bilgi toplumunun gelecekte belki de karşılaşılabileceği en ciddi sorunların başında, bu sığlaşma, düzeysizleşme ve sıradanlaşma tehlikesi gelmektedir (Avcı, 1990: 83-91).

Bilgi ve iletişim teknolojilerinin gelişmesiyle enformasyon üretme, ulaşma, haberdar olma ve farkındalık oluşturma olanakları olabildiğince genişlemiş fakat, buna karşılık dünyada olup bitenleri sağlıklı bir şekilde anlayabilme ve yaşanan olayların sonuçlarına ve arkasındaki gerçeklere ulaşabilme noktasında ciddi bir körlük meydana gelmiştir. Enformasyon tüketimine ilişkin olarak ortaya çıkan bu durum “anestezi edilmiş bir bilme biçimi” olarak adlandırılmaktadır (Robins, 1999: 189).

Diğer yandan, mevcut kitle iletişim araçları bilerek veya bilmeyerek kitleleri ciddi konulardan uzaklaştırmaya, eğlenceye dönük bir anlayışa yöneltmeye çalışmaktadır. Sonuçta, edilgen bir çoğunluk ile bilgi teknolojisine egemen olan güçlü bir azınlık ortaya çıkmaktadır. Teknolojinin büyüğü dünyası egemen anlayışın kitleler üzerindeki örtük denetimini kamufle etmektedir (Robins, 1999: 156).

Görüldüğü gibi, Bilgi toplumu sunduğu bir çok imkan, fırsat ve faydaların yanında risk, tehdit ve sorunları da beraberinde getirmektedir. Buna mukabil, insan hayatında sağladığı kolaylık, rahat ve konforun insanı daha mutlu kılacağı beklentisi, teknolojik yeniliklere duyulan ilgi, sunmuş olduğu ekonomik kalkınma vaadi, tüketim için yeni ve çeşitli olanaklar sunması gibi nedenler yanında, bu beklenti ve vaadlerin ancak bilgi toplumu ile mümkün olacağına ve maddi ve teknolojik gelişmenin insani gelişmeyi de sağlayacağına dair düşünce, kanaat ve fikirlerin değişik iletişim ve haber araçları ile sürekli topluma pompalanması, bilgi toplumunu bir “mit” haline getirmektedir. Dolayısıyla, toplumlarda bilgi toplumuna ilişkin olarak “kurtarıcı” ve “kutsayıcı” bir algının oluşmasına neden olmaktadır.

Halbuki, bahsi geçen sorunlar bağlamında, 21. yüzyılın, çok enteresan gelişmelere sahne olabileceği, bilim ve teknolojinin son analizde insanlığa hizmet etmek yerine, onun sonunu hazırlayacak bir yapıya bürüneceği bir çağa dönüşmesi olasılığının bulunduğu söylenebilir. Dolayısıyla, bilgi toplumunu sadece faydaları açısından tek yönlü olarak değerlendirmek, bilgi toplumu olmanın gündeme getirdiği sorunları ve taşıdığı potansiyel riskleri ve tehlikeleri görmemize engel olabilecektir. Bu nedenle, bilgi toplumu olmanın maliyetlerinin neler olduğunun irdelenmesi gerekmektedir. Keza, oluşturulan imaj ve algı yerine, “olguyu” bütün gerçekliği ile görmeye, anlamaya ve kavramaya çalışmak, beraberinde getirdiği sorunlara doğru çözümler üretilmesine yönelik girişimlerin en temel şartı olarak görülmelidir.

1.1.3 Bilgi Toplumu ve İnternet

İnternet yönetimden siyasete, ekonomiden hukuka, aileden arkadaşlık ilişkilerine, iş ilişkilerine, insanların tutum, davranış ve alışkanlıklarına kadar toplumların sosyal, siyasal, ekonomik ve kültürel yapıları üzerinde olumlu veya olumsuz yönde önemli ve belirgin değişikliklere sebep olan bir olgu olarak önümüzde durmaktadır.

İnternetin sağladığı sanal ortamın dünyanın her yerinden milyonlarca kullanıcıyı coğrafi uzaklıkları yok sayan bir şekilde - ki Caincross bu durumu “mesafenin ölümü” olarak tanımlamaktadır (Caincross, 1997) - bir araya getirmesi sonucu, McLuhan’ın deyimiyle “Global bir köy”ün meydana geldiği söylenmektedir. Keza, İnternetin renk, ırk, milliyet ve dil farkı gözetmeksizin, çeşitli işaretler ve kısaltmalardan oluşan yeni bir anlaşma dili (Wingate, 2001: 26), yeni okuma alışkanlıkları (UCL, 2008) ve dolayısıyla, yeni bir “siber kültür” oluşturduğu belirtilmektedir (Bell, 2000: 92-101).

İnternetin meydana getirdiği özgün kültürel ortamın etkisi altında kalan kitlelerin ve bu kültürün etkisi altında doğan ve yetişen yeni neslin, farklı değer kümeleri oluşturdukları ve bu değer kümelerinin çatışmasının antropolojik, ekonomik, sosyolojik ve hukuksal sonuçlar doğurduğu; toplumsal etkileri olan her yeni değişimde farklı boyutlarda yaşanan bu etkileşimin İnternetin yapısı ve sunduğu

imkanlar özelinde değerlendirildiğinde paradigma dönüşümüne neden olacak kadar geniş ve derin izler bıraktığı dile getirilmektedir (Wise, 2000: 27).

Nitekim, meydana gelen değişimlerle ortaya çıkan yeni topluma “İnternet toplumu”, İnternet toplumunu oluşturan bu halka, net halkı “net citizen” veya “netizen” veya netdaş denilmektedir (Uğur ve Bilici, 1998: 448-496). Bu yeni toplum için “siber toplum” adlandırması da yapılmaktadır. Buna göre, İnternet kullanıcıları siber toplum mensubudurlar ve bir sanal gerçeklik alanı olan siber uzayda yaşamaktadırlar (Subaşı, 2005: 108).

O. Nihat Şen de İnternetin bilgi toplumuyla gündeme gelen bir olgu olmakla birlikte son 10-15 yıldır tek başına bir fenomen haline geldiğini ve bilgi toplumunun kalıplarını aştığını belirtmektedir. Zira, İnternet günümüzde hayatın merkezine yerleşmiş ve herşeyi şekillendiren bir güç haline gelmiştir. Dolayısıyla, artık bilgi toplumunun bir sonraki aşaması olarak İnternet toplumundan ve onun özellik ve sosyal etkilerinden bahsetmeli ve bu yeni olguyu anlamaya, çözümlemeye ve bu yeni döneme hazırlık yapmaya çalışmalıyız (O. N. Şen ile kişisel iletişim, 06.08.2013).

Fakat, bu durumu daha ziyade İnternetin popülerliği ve günlük hayattaki etkilerinin daha çok ve somut olmasına bağlamak gerekmektedir. Bu yanılsama bizi aldatmamalıdır; çünkü, konunun başlangıcı, nirengi noktası ve bağlamı bilgi toplumudur. Bu kapsamda İnternet, bilgi toplumunun en çok bilinen ve kullanılan, marka değeri en yüksek ürünü olarak düşünülmelidir. Bunun aksine, konunun ele alınışında ve yürütülen tartışmalarda bilgi toplumundan bağımsız olarak tek başına İnternet olgusunu merkeze koymanın, konunun ve sorunların özüne inmemek ve hatta hedefi iskalamak gibi bir sonuç doğuracağı muhtemeldir.

Yüzyılımızın en önemli buluşu ve günümüz bilgi toplumunun en önemli unsuru olarak kabul gören İnternet, birçok yeniliği ve kolaylığı hayatımıza getirmiş olmakla birlikte, neden olduğu ve olacağı değişimlerle insanlığa refah ve mutluluk noktasında katkıda mı bulunacak, yoksa insanları daha da mutsuz insanlar haline mi getirecek sorusunu da hatıra getirmektedir.

Bu bağlamda, daha önce bahsi geçen konu ve sorunlar da kısmen değinilmekle birlikte, önce İnternetin kullanım alanları ve sağladığı faydaları kısaca hatırladıktan sonra, doğrudan İnternet kaynaklı olan sorunların daha geniş olarak ele alınması, ilerleyen bölümlerde yapılacak tartışmalar için yararlı olacaktır.

1.1.3.1 İnternetin Kullanım Alanları ve Sağladığı Faydalar

İnternet'in, insanların hayatına kattığı olumlu katkıların oldukça fazla olduğu ve doğru kullanılması durumunda yaşamı birçok açıdan kolaylaştırdığı bir gerçektir. Başlangıçta haberleşmeyi kolaylaştırma özelliği ile ön plana çıkmış olsa da, artık bireylerin yaşamının her alanına girmiş ve ticaretten eğitime, sağlıktan siyasete tüm alanlarda etkisini artırmıştır. Bu bağlamda, İnternet kullanımının olumlu etkileri ve insan yaşamına getirdiği kolaylıklar genel olarak; İnternet'in bilgi ve eğitim amaçlı kullanımı sayesinde yaşam boyu öğrenime olanak sağlama, fikir ve bilgi alış verişini hızlandırmak, hayatın her alanında üretkenlik ve verimliliği arttırmak ve iletişimi kolaylaştırmak şeklinde sıralanabilir (Odabaşı, 2002: 8-9).

İnternetin kamu hizmetlerinde kullanılmaya başlamasıyla birlikte, kamu sektöründe verimlilik artmış ve devlet vatandaşına “bir tuş mesafesi” kadar yakın hale gelmiştir. İş dünyası, İnterneti etkin bir şekilde kullanarak zaman ve ekonomik yönden tasarruf sağlamaktadır. İnternetin, günlük yaşam, sosyal ilişkiler, çevre, sağlık ve eğitim gibi alanlarda getirdiği yenilik ve faydalar herkes tarafından kabul edilir hale gelmiştir.

Arama motorları, haber grupları, haber siteleri, e-posta, anında mesajlaşma, sohbet, bankacılık, eğitim, elektronik ticaret, elektronik yayıncılık gibi birçok servisin getirdiği avantajlar İnternet aracılığıyla hayatımıza girmiştir. Öte yandan insanlar bu teknoloji vasıtasıyla bilgiye daha kolay, ucuz ve hızlı bir şekilde erişebilme imkanına kavuşmuştur. Nitekim, Dünyadaki büyük kütüphanelere ulaşmak, farklı ülkelerde yaşayan ve değişik bilim dallarında araştırma yapan bilim insanlarının çalışmalarına erişmek bir tık mesafesi kadar yakınımıza gelmiştir. İnternet, pek çok yararlı bilgiye bir tuşa basarak ulaşılan dev bir kütüphane işlevini fazlasıyla yerine getiren bir platform görevi görmektedir.

İnternet ayrıca, kişilerin değişik platformlarda fikirlerini serbestçe söyleyebilme ortamı sağlayan demokrasi platformu olmuştur. Bu yönüyle İnternet, toplum yapısının çoğulcu ve katılımcı olmasını, kültürel çeşitlenmesini, hoşgörü ortamının gelişmesini ve insanlar arasında yaygınlaşmasını, kısaca değişik kültürlerin, dini ve ahlaki değerlerin birbirleri arasında kaynaşarak yeni boyutlar kazanmasını kaçınılmaz bir sonuç olarak karşımıza çıkarmaktadır. Bu nedenlerle siber uzay olarak bilinen İnternet alanına, “etkileşim uzayı” adını verenler de vardır(Subaşı, 2005:108).

Milyonlarca insan bu ortamda etkileşimde bulunarak yoğun bir bilgi paylaşımı yapmak suretiyle sosyalleşmektedir. Bu yoğun bilgi akışı ve paylaşımı İnternetin sosyal yönünü ortaya çıkarmaktadır. İnternet asosyal insanları daha aktif ve katılımcı bir ortama çekerek sosyalleştirmektedir. İnsanlar gerçek hayatta konuşamadıkları, paylaşamadıkları düşüncelerini, burada görülme ve tanınma riski taşımadığından dolayı rahatlıkla dile getirebilmektedir.

Özetle İnternetin haberleşme, bilgi paylaşımı, habercilik ve medya, tanıtım ve reklam, seyahat ve tatil, kamu hizmetleri, bankacılık, ticaret, eğlence, sosyal ilişkiler ve kültürler arası etkileşim, çevre, sağlık ve eğitim gibi günlük yaşamı ilgilendiren pek çok alanda getirdiği olumlu yenilikler ve faydalar bu gün herkes tarafından kabul edilmektedir. Gelecekte bunlara yenilerinin de ekleneceği beklenen bir durumdur.

1.1.3.2 İnternetle Gelen Sorunlar

İnternet, yaşadığımız gerçek dünyada mahiyetini pek fazla bilmediğimiz ve her geçen gün büyüyen sanal bir aleme, belki hiç kapanmayacak geniş kapılar açmıştır. Günümüz insanı merak, korku, endişe, heyecan ve şaşkınlık içinde bu sanal alemin kapısından içeriye bakmaya çalışmakta, çoğu zaman içeri dalarak el yordamıyla bir şeylere dokunmakta, amaçsızca esrarengiz yolculuklara çıkmaktadır(AREM,2008:5).

Dolayısıyla, İnternet her ne kadar hayatımıza birçok faydalı yenilikler getirmiş olsa da beraberinde bir takım olumsuzluklar ve sorunları da taşımıştır. Bu olumsuzluklar ve sorunlar en başta çocuklar, gençler ve aileler olmak üzere tüm toplum kesimlerini etkilemektedir. Gerçek hayatın içerisinde nasıl iyi-kötü, güzel-çirkin, doğru-yanlış,

faydalı-zararlı varsa, artık modern hayatın önemli bir parçası olan İnternet ortamı da bunların sanal dünyaya ait versiyonlarını barındırmaktadır.

Bu noktada Şen'in dikkat çektiği bir hususa da, içerik düzenlemesi fikrinin "İnternetin zararları neler" bakış açısından ortaya çıkması ve İnternetin olumsuz yönüne odaklanmasıdır. Şen'e göre, İnternetin "zararlı" ve "kötü bir şey" olarak algılanmasına neden olan bu bakış açısı aslında İnternete zarar vermekte, İnternetle ilgili kutuplaşmalara ve bazı insanların kategorik olarak İnternetten uzak kalmasına neden olmaktadır (O. N. Şen ile kişisel iletişim, 06.08.2013).

Halbuki, İnternetin yararları sakıncalarından çok daha fazla ve somuttur. Zararları ise daha az, soyut ve zamana yayılmıştır; genellikle de bilinçsiz kullanımdan kaynaklanmaktadır. İnternetin bu şekilde yarar-zarar düzlemine indirgenmesi İnternete yapılan büyük bir haksızlıktır. Nasıl, insanlar araç kullanmayı, trafiğe çıkmayı tüm risk ve olumsuzluklarına rağmen benimsemiş ve hayatlarından bir parça haline getirmişlerse, İnternet de aynı yaklaşım ile ele alınmalıdır. Yani, toplumda herkesin kabullendiği diğer husularda olduğu gibi İnternet konusunda da bu yarar-zarar indirgemeciliğinden vazgeçilip, İnternet hayatın vazgeçilmez bir parçası olarak kabul edilmelidir. Zaten İnternet, biz isteyelim veya istemeyelim hayatın her alanına girmiş ve ailemizin afacan, haylaz bir çocuğu olarak hanelerimizde yerini almıştır (O. N. Şen ile kişisel iletişim, 06.08.2013).

Bu çerçevede İnternetle birlikte gündeme gelen sorunları, İnternette yer alan yasadışı ve zararlı içerikler, güvenlik ve mahremiyet sorunları ile İnternetin sebep olduğu toplumsal sorunlar olarak tasnif ederek ele almak mümkündür.

1.1.3.2.1 İnternette Zararlı ve Sakıncalı İçerik Sorunu

Girilen yazılı ve görsel her türlü bilgi ve veri İnternet içeriğini oluşturmaktadır ve bunların önemli bir kısmı istenmeyen sakıncalı içeriklerdir. Bu tür içeriklerin başlıcalarını; pornografi ve çocuk pornografisi, fuhuşa aracılık, ırkçılık, ayrımcılık, kumar oynamaya ve uyuşturucu kullanmaya teşvik, şiddet, vahşet, nefret ve intihara yönlendirme içerikleri ile telif hakkı ihlallerine ait içerikler şeklinde sıralayabiliriz.

1.1.3.2.1.1 Pornografi ve Çocuk Pornografisi İçerikleri

Günümüzde pornografi ve bilhassa çocuk pornografisi materyalleri tüm dünyada çok hızlı bir şekilde artmakta, çoğaltılmakta ve paylaşılmaktadır. Bu artışta dijital teknolojilerin ve özellikle İnternetin rolü büyüktür. Pornografinin, İnternette özgürce yer alması ve sınırsızca paylaşılabilmesi tüm dünyada eleştiri konusu yapılmakta ve bu tür içeriklerle mücadele edilmesinin gerekliliği tartışılmaktadır. Buna karşılık bazı kesimler de bu tür içeriklerin sınırlandırılmasının “İnternet özgürlüğü” ve “İnternette ifade hürriyeti” bağlamında değerlendirilmesi gerektiğini iddia etmektedir.

1.1.3.2.1.1.1 Pornografik İçerikler

Pornografik içerik, sosyal hayatı pek çok açıdan olumsuz yönde etkilemesi özelliği ile İnternetin getirdiği en önemli olumsuzluklardan birisidir. Günümüzde yeni teknolojiler pornografinin doğasını değiştirmiştir. Daha önce basılı pornografik materyaller revaçtayken son dönemde büyük çoğunluğu İnternet ortamına taşınmış olan dijital pornografik materyaller ön plana çıkmıştır.⁸

Dijital kameralar ve fotoğraf makineleri, kameralı cep telefonları kolay ve ucuz yoldan eskimeyen ve bozulmayan görüntüler üretmektedir. Bunun dışında, dijital grafik programlar iki görüntüyü birleştirme veya fotoğrafları bozarak ve değiştirerek yeni görüntüler elde etmek suretiyle aslında pornografik olmayan fotoğrafları kolayca pornografik hale getirilebilmektedir. Keza, sözde (pseudo) pornografi denilen, gerçek dışı, bilgisayar ile üretilmiş kişileri kullanarak bilgisayar ortamında pornografi olayı canlandırılabilmekte ve görüntülerde, bu kişilerin arka planındaki her şey gerçek dünya nesneleri bile olabilmektedir (Uzunay ve Koçak, 2005: 107-108). Bütün bunlara İnternetin takip edilemezlik ve sınırları aşma özelliği de eklenince pornografi, üretim ve tüketim boyutlarıyla, hiç olmadığı kadar yaygın bir sorun olarak karşımıza çıkmaktadır (Polat, 2006).

⁸ Nitekim son dönemde basılı pornografik yayın satışlarında büyük düşüşler gözlenmiştir. Penthouse Dergisi'nin 1980'lerde yıllık 3,5 milyon satış trendi varken, yıllar geçtikçe bu trend 850 bine kadar düşmüştür. Playboy Dergisi, yıllık 5,3 milyon dolar kar rakamlarından 46,6 milyon dolara varan zararlara gerilemiştir (Uzunay ve Koçak, 2005: 108).

Pornografinin bu yaygınlığı, İnternet sayesinde kolay ulaşılabilir olmasından kaynaklanmaktadır (Ropelato, 2012). İnternet pornografiye erişimi kolaylaştırarak, pek çok kişi için günlük yaşamda karşılığı olmayan bazı güdülerin, sanal dünya kullanılarak gerçekleştirilmesini sağlamaktadır (Yıldız, 2003: 2). Bunun yanında, günümüzde, pek çok ülke, sadece çocuk pornografisini suç olarak değerlendirirken, yetişkin pornografisini ya suç olarak kabul etmemekte ya da çok az cezalar uygulamaktadır. Bu durumda, İnternet, gençler ve çocuklar için pornografiyle karşılaşmada ilk adres olmaktadır (AREM, 2008: 72).

Sosyal dokuyu zedeleyen, ahlaki yapıyı bozan ve hukuksal ve adli sorunlara neden olan “pornografi” günümüz dünyasında büyük bir tehdit haline gelmiştir. Birçok İnternet sitesinde, pornografik içeriğe sahip yerli ve yabancı dokümanlar, broşürler ve filmler bulmak mümkündür. Ayrıca, bu sitelerin adres gösterdiği sohbet odalarında da sürekli pornografi konuşulmakta, genç erkek ve kızlara promosyonlar ve hediyeler verilmek suretiyle birbirleriyle tanışmaları sağlanmakta ve pornografi piyasasına çekilmeye çalışılmaktadır (AREM, 2008: 72-73).

Bugün İnternetin pornografi endüstrisini önemli ölçüde teşvik ettiği; web siteleri, chat kanalları, fotoğraf ve metin olmak üzere en büyük ve zengin içerikli pornografi koleksiyonunu kullanıcılara sunduğu bilinmektedir. Nitekim, Uluslararası Çalışma Örgütü ve UNICEF’in 2008 yılı tahminlerinden yola çıkan bazı araştırmalara göre dünya genelinde pornografi sektöründe bir çeşit cinsel köle olarak çalışan veya çalıştırılan 27 milyon erkek, kadın ve çocuk bulunmaktadır (Bouché, 2009: 3).

İnternet Filter Software Review’in hazırlamış olduğu 2006 yılı İnternet pornografisi istatistiklerine göre, 27,4’ı Çin’e, 25,73’ü Güney Kore’ye, 19.99’u Japonya’ya ve 13.33’ü ABD’ye ait olmak üzere yetişkin porno piyasasının cirosu 97 milyar dolardır. Tüm kullanıcıların %42,7’si pornografik içerik görüntülemektedir. İnternet ortamında tüm web sitelerinin %12’sini oluşturan 4,2 milyon pornografik web sitesi, 420 milyon pornografik web sayfası bulunduğu tahmin edilmektedir. %12’sini oluşturduğu İnternet pornosu için her saniye 3.000 \$’dan fazla para harcanmaktadır. Her saniye 28.258 kişi porno izlemektedir. Günlük pornografik arama motoru isteği

68 milyon civarındadır ve bu rakam tüm aramaların %25'ine karşılık gelmektedir (Internet Filter Software Review, 2006). Tüm dünyada İnternette porno arama oranının 2013 yılında neredeyse yüzde yüze yaklaştığı ifade edilmektedir (Par, 2013).

Aynı istatistiğe göre, İnternette indirilen materyalin %35'i pornografik içeriklidir. Her gün 2,5 milyar civarında pornografik içerikli e-posta gönderilmektedir. Tüm dünyada sanal pornografi meraklıların 1/3'ü kadındır. Porno siteleri en çok pazar günleri ziyaret edilmektedir. Avrupa, ABD ve Uzak Doğu'da 18-24 yaş arası kullanıcı erkeklerin %70'i ayda en az bir kere İnternette porno izlemektedir. Aynı coğrafyalarda erkeklerin %20'si, kadınlarinsa %13'ü işyerinde zaman zaman porno izlediklerini kabul etmektedirler (Internet Filter Software Review, 2006).

Optenet tarafından 2010 yılında 4 milyon web sayfası üzerinde yapılan bir araştırma sonucuna göre, pornografinin, İnternet'in toplam içeriğinin %37'sini oluşturduğu belirtilmiştir (Optenet, 2010). İnternetin toplam içeriği içinde pornografinin 2006 yılında yayınlanan istatistiklerde tahmini %12 iken 2010 yılında %37 olarak bulunması dikkat çekicidir. Yıllar içinde bu tür içeriğin hızla arttığı görülmektedir. Nitekim, 2010 yılının ilk çeyreğinde bu tür içerik bulunan web sayfalarının oranında %17'lik bir artış gözlenmiştir. Yine, bu araştırmaya göre, 24 yaş altı erkek kullanıcıların %70'i bu tür web sayfalarına girmektedir (Optenet, 2010).

WorldTracker'in kullanıcıların arama motorlarında sorguladıkları sözcüklerin listelendiği rapora göre en çok arama yapılan 200 anahtar sözcüğün 82'si pornografi ile ilişkilidir (TheWordTracker Report, 2012). İngiltere'de yapılan bir araştırmada İnternet kullanıcılarının %43'ünün pornografik içerik görüntülediği, bunların %10'unun ise bu içeriğe bağımlı olduğu tespit edilmiştir (Haberturk, 19.01.2010).

IBM'in bir raporuna göre, pornografi ve erotizm türü yetişkin (adult) içerik üreten ilk beş ülkenin oranları şu şekildedir: 1. ABD %53,1, 2. Almanya %16,2, 3. Hollanda %5,5, 4. Güney Kore %4,5, 5. Kanada %4,3 (IBM, 2008: 44).⁹ Pornografik içerikleri

⁹ Ameriken porno endüstrisinin merkezi, "Pornywood" diye tanınan San Fernando Valley'dir. Pornywood'daki ikiyüz film stüdyosu, yılda onbin kadar film üretmektedirler.(Caydı, 2010).

sunucularında barındıran ülkelerin oranları ise şöyledir: ABD %60, İngiltere %7 ve Almanya %1 (Roadtogracy, 13.08.2013).

Ayrıca, pornografik içerikli web sitelerinin büyük bölümü kötü amaçlı yazılımlar içerdikleri için kullanıcılarını mağdur etmektedir. Nitekim, International Secure System Lab tarafından gerçekleştirilen bir araştırmaya göre, incelenen 35 bin pornografik içerikli alan adının %90'ı ücretsiz web sitelerinden oluşmakta ve bu alan adlarını kullanan 269 bin web sitesinin %3,23'ü istenmeyen casus yazılımlar ve virüs gibi tuzaklarla donatılmış bulunmaktadır. Diğer yandan, uzmanların test amaçlı kurdukları ve ücretsiz içerikler sağladıkları 2 adet müstehcen siteye gelen 49 bin kişinin 20 bininde ciddi açıklar içeren bilgisayar ve tarayıcı ayarlarına rastlanılmıştır (BBC, 11.06.2010). Bu türden açıklar pornografik içerikli web siteleri üzerinden gerçekleştirilen dolandırıcılık eylemlerini artırmaktadır. Çünkü, bu web sitelerine giren kişilerin bilgisayarları yeterli güvenlik önlemlerine sahip değilse, fark edilmeden yüklenen programlar ile kişisel verilere erişilebilmektedir (Güvenliweb, 2012).

1.1.3.2.1.1.2 Çocuk Pornografisi İçerikleri

Çocuk pornografisi, “Çocuğun cinsel davranışı ya da organları üzerinde odaklanan yazılı ve işitsel gereçler de dahil olmak üzere, çocukların cinsel istismarını göstermenin ya da teşvik etmenin her türlü yolu” olarak tanımlanmaktadır (Özkanlı ve Özkanlı, 2006: 118). BM Çocuk Hakları Sözleşmesi'nin 25.05.2000 tarihinde imzalanan ek protokolünde ise çocuk pornografisi, “Çocuğun gerçekte veya taklit suretiyle bariz cinsel faaliyetlerde bulunur şekilde herhangi bir yolla teşhir edilmesi veya çocuğun cinsel uzuvlarının, ağırlıklı olarak cinsel amaç güden bir şekilde gösterilmesidir.” (Çocukhakları, 2012).

Başlangıçta lokal olarak nadiren görülen çocuk pornografisi İnternetin yaygınlaşmasıyla dünyanın her tarafına yayılmıştır. İnternet, çocuk pornografisi ticaretine küresel bir kimlik kazandırmış, akıl almaz bir hızla gelişmesine neden olmuş ve bir suç tipi olarak uluslararası alanda dünyayı tehdit eden önemli sorunlardan birisi haline gelmiştir (Uzunay ve Koçak, 2005:97-98). Keza, Avustralya

Adalet ve Gümrük Bakanlığı ülkede ele geçirelen çocuk pornografisi materyallerinin %85'inin İnternet aracılığıyla dağıtılmakta olduğunu açıklamıştır (Ellison, 2003).

Çocuklar, İnternette pornografik bir meta olarak 1986'dan beri kullanılmaktadır ve bugün, resimlerin (imaj) oluşturulması, kaydedilmesi, kopyalanması, dağıtım ve pazarlama gibi pek çok işlem İnternet üzerinden gerçekleşmektedir. İnternet, çocuk pornocuları ve tacirlerine, yeni kurbanlar ve materyaller bulma, bu işle uğraşan diğer kişilere ulaşma gibi konularda İnternet sayfaları, haber grupları, e-posta iletileri ve sohbet odaları ile erişim noktasında büyük kolaylıklar sağlamaktadır. Ayrıca, tespit edilme riskini en aza indirmek amacıyla, çocuk pornograficileri arasında değiş tokuş işlemleri için bire-bir (peer-to-peer) bağlantı yönteminin de tercih edildiği görülmektedir. Bu tür bağlantı yöntemlerinde istemciler merkezi bir sunucuya değil de birbirlerine bağlanmaktadır (Uzunay ve Koçak, 2005: 108).

Uzmanlar, çocuk pornografisi izleyenlerin ilk başta yetişkin, daha sonra hayvan ve en son çocuk pornografisine yöneldiklerini bildirmektedir (Par, 2013; Takvim, 02.06.2010).¹⁰ Bazen çok küçük yaştaki çocukları hatta bebekleri içeren, acımasızca ırza geçme, cinsel kölelik, hayvanlarla birlikte cinsel ilişki ve cinsel tacizin bütün çeşitlerinin yer aldığı görüntülerin varlığı çocuk pornografisinin iğrenç yüzünü ortaya koymaktadır (Uzunay ve Koçak, 2005: 105).

Çocuk pornografisine ilişkin materyallerin ve bu içerikteki fikir, fantezi ve görüş aktarımında bulunmak gibi sanal alanda gerçekleştirilen uygulamaların, çocuklara karşı işlenen cinsel suçları beslemekte, teşvik etmekte ve kolaylaştırmakta önemli bir rol oynadığı genel olarak kabul gören bir görüştür (Akıncı, 2001: 12). Çünkü bu tür içeriklere ilgi duyan yetişkinler çoğu zaman bunları izlemekle yetinmemekte, normal hayatta da bu davranışın akislerini sürdürmektedir (CYBERTIP, 2009: 66).

¹⁰ “Psikiyatrlar bağımlılık yaptığını da söylerler. Porno sektörünü bu kadar alengirli hale getiren şey, insanların gelenek ya da toplum tarafından konulmuş bulunan “sınırları” aşmaya duydukları tekinsiz merak ve dürtüdür. Yasak dürtüleri körükler denir; doğru, ama yasak kalktığı anda şehvetle yeni yasaklar arayan da aynı dürtülerdir. Her sınır aşımı, tatmin çıtasını biraz daha yükseltir ve daha “yasak” olanın peşine düşürür. Artık sırada ne varsa.” (Karaca, 2010)

Yapılan arařtırmalar, çocuk pornografisi materyalleri alan/satan ve bulunduran kiřilerin yaklaşık %80'inin bizzat kendisinin de aktif olarak çocuklara cinsel istismar ve řiddet uyguladıklarını göstermektedir. Dolayısıyla, çocuk pornografisi ve cinsel istismarı, lke, sınır, ırk, cinsiyet ve yař farkı gözetmeksizin, tüm dünya çocuklarını tehdit eden, çocukların cinsel řiddete maruz kalmalarına ve ticari meta haline gelmesine sebep olan ciddi bir sorundur (Uzunay ve Koçak, 2005: 106,109).

Telefono Arcobaleno'nun arařtırmasına göre, büyük bir pazar ve sektör haline gelen çocuk pornografisine olan ilgi ve tüketici yönelimi her geçen yıl hızla artış göstermektedir. Çocuk istismarı materyalleri ve bunlarla ilgili web sitelerinin oranı 2003'ten bu yana 4 kat artmıştır. 1997'den itibaren İnternetteki çocuk pornografisi fotoğraflarının sayısı ise %1.500 artış göstermiştir. İsteyen herkes İnternette ücretsiz olarak veya kredi kartını kullanarak arzu ettiğı yař, ırk ve fiziksel özellikleri de belirterek çocuklara ait resim ve video görüntülerine sahip olabilmektedir (Telefonoarcobaleno, 2009; Yeniaktüel, 2006).

Genellikle organize suç örgütleri tarafından uyuşturucu ve çocuk fuhřu ile birlikte yapıldığı belirtilen çocuk pornografisinin, İnternette geldiğı noktanın dehřet verici olduğı görölmektedir. Bugün 100 bini aşkın çocuk pornografisi sitesi bulunduğı, 2 milyon çocuğun bu sektörde seks kölesi olarak kullanıldığı, online suistimale uğrayan çocukların sayısının günde 20 bini aşmakta olduğı, bu sektörün yıllık cirosunun 80-90 milyar dolara ulařtığı tahmin edilmektedir. Sektörün 2004 yılında bilinen geliri 20 milyar dolar idi (Bouché, 2009: 3; CNNTURK, 2006; Yeniaktüel, 2006). Bu sektörün en büyük üretim merkezi Almanya, dağıtım merkezi Hollanda ile İngiltere ve en büyük pazarı ise ABD'dir.¹¹

2008 yılında, 20 milyar çevrimiçi hareketin, 36.149 çocuğa ait 1 milyon 700 bin adet istismar ve çocuk pornografisi görüntüsünün dolařımına sebep olduğı tespit edilmiştir. Bu çocuklardan % 42'sinin 7 yař altı ve % 77'sinin 9 yař altı olduğı,

¹¹ Çocuk pornografisi materyallerinin %73.2'si Avrupadan, %20.1'i ABD'nden servis edilmektedir. Bu içeriğın %39.63'ü Hollanda'dan, %13.44'ü Almanya'dan, %12.96'sı Rusya'dan, %3.83'ü Kıbrıs'tan kullanıma sunulmaktadır. Bu materyallerin kullanım oranları ise řöyledir: ABD %22.9, Almanya %16.6, İngiltere %6.9, Fransa %6.4, Rusya %5.2, İtalya %4.8 (Telefonoarcobaleno, 2011a).

%19'unun 3 yaş altı olduğu belirlenmiştir (Telefonoarcobaleno, 2009 ve 2011b). Prof. Dr. Esin Küntay, yapılmış olan araştırmaların bebeklerin bile pornografik malzemeye konu edildiğini belirtmektedir (i-cozum, 2011). Konunun diğer bir trajik yönü ise, İnternette yer alan pornografik malzemelere konu edilmiş veya cinsel istismara maruz kalmış çocukların ancak %1 ve hatta daha azı tespit edilip bulunabilmekte ve rehabilite edilebilmektedir (Telefonoarcobaleno, 2009).

INHOPE'un yayınladığı Rapora göre, 2009 yılında ihbarlarla tespit edilen 24.047 çocuk pornografisi ve cinsel istismarı konulu web adresindeki içeriklerin %77'sinde kız çocukları, %11'inde erkek çocukları, %12'sinde hem erkek hem kız çocukların kullanıldığı görülmüştür. Bu içeriklerdeki çocukların %4'ü bebeklik çağında, %71'i ergenlik öncesi yaşlarda, %25'i de ergenlik çağındadır (INHOPE, 2010: 15-17).

Kanada'daki Cybertip İnternet İhbar Merkezi'nin, kendisine bu tür içerikli gelen ihbarları analiz ederek 2009 yılında yayınladığı bir rapora göre, 16 bin olaydaki verilerin incelenmesinden görüntülerde yer alan çocukların %82'sinin 12 yaşından küçük olduğu tespit edilmiştir. Bunların %35'inden fazlasında çocuklara tecavüze rastlanılmıştır. Görüntülerin %77'sinde 8 yaşından küçük çocuklara ait fotoğrafların bulunduğu ve bunların da %69'unda 8 yaş altı çocuklara ekstrem taciz ve tecavüzlerin yer aldığı görülmüştür. Tüm görüntülerin %83'ünde kız çocuklarının kullanıldığı tespit edilmiştir (CYBERTIP, 2009: 39-51).

Raporda, çocukların cinsel istismarı içeriklerinin son derece pahalı olması nedeniyle dünyada giderek artan bir lüks tüketim haline geldiği ve daha çok zengin ve eğitimli bir müşteri kitlesinin olduğu vurgulanmaktadır. Milyarlarca dolarlık gelirler söz konusu olunca bazı ülkeler bu tür içeriklerle mücadelede kafa karışıklığı yaşamakta ve cılız tedbirlerle konuyu geçiştirmektedir. Bu tür içeriğe sahip siteler genellikle ticari web siteleridir ve çoğunlukla üyelik sistemi ile çalışmaktadırlar. Araştırmada bu sitelerde 27 değişik ödeme türüne rastlanmıştır. Bunların %55'i kredi kartı ile ödeme kabul ederken % 85'i üyelik aidatı almaktadır. %6'sı adet fiyatları 2000 doları bulan DVD'ler satmaktadır (CYBERTIP, 2009: 63-64). Rapora göre, çocukların cinsel istismarı içeriklerine yer veren 12.700 web sitesinin %50'si ABD'de, %20'si

Rusya’da, %9’u Kanada’da, %4’ü Japonya’da, %4’ü ise Güney Kore’de olmak üzere toplam 60 ülkedeki sunucularda barındırılmaktadır (CYBERTIP, 2009: 61).

Raporda sektörün milyar dolarla ifade edilen ticari büyüklüğünden dolayı söz konusu web sitelerin erişilebilir kalmak için büyük çaba gösterdikleri belirtilmektedir. Cybertip bu konuda bir test yapmış ve bu tür içeriklere sahip bir web sitesinin 48 saatte 16 farklı ülkedeki 212 farklı IP adresi üzerinde bir döngü gerçekleştirdiğini tespit etmiştir (CYBERTIP, 2009: 61-62). Görüldüğü gibi çocuk pornografisi sektörü büyük paralar kazandığı bu kirli işi kolay kolay bırakacağı benzememektedir. Dolayısıyla bu alanda çok ciddi ve profesyonel mücadele gerekmektedir.

Raporda bu çerçevede alan adlarının dağıtımında da bazı köklü değişikliklere gitmek gerektiği ve yeni standartlara ihtiyaç olduğu ifade edilmektedir. Buna göre, alan adı alınırken isim ve adres doğrulaması yapılmalı ve sürekli IP değiştiren alan adlarının tespit edilip, ihbar merkezleri ile işbirliği yaparak İSS’lerin bu sitelere hizmeti kesilmelidir (CYBERTIP, 2009: 67). Raporda ayrıca ele geçirilmiş zombi bilgisayarların çocukların cinsel istismarı içeriklerinin dağıtımında sahibinden habersiz bir şekilde kullanıldığından bahsedilmektedir (CYBERTIP, 2009: 69).

İngiltere’de çocuk pornografisi ile mücadele eden IWF adlı STK, yayınladığı bir raporunda ilginç ayrıntılara yer vermektedir. Rapora göre, İnternet ortamında çocukların cinsel istismarı içeriklerini pazarlayan şimdiye kadar tespit edilen 715 farklı organizasyon vardır ve bunların 321’i halen aktiftir. Bunlardan 10 tanesi sürekli yeni içerik üretmektedir ve İnternet piyasasında bu tür içerikleri pazarlayan web sitelerinin yaklaşık yarısı bu organizasyona aittir (IWF, 2010).

Keza, bu tür içeriklerin dağıtımında artık ağırlıklı olarak bedava barınma sağlayan servisler, sosyal ağlar, fotoğraf paylaşım siteleri ve ele geçirilmiş web siteleri kullanılmaktadır. Dağıtıcılar sürekli bir biçimde dağıtım ağlarını ülkeden ülkeye, yer sağlayıcı firmadan diğer yer sağlayıcı firmaya taşımakta ve yakalanmamaya çalışmaktadır. Dağıtıcılar yer sağlayıcı hizmetini daha karmaşık sistemleri olan Kuzey Amerika, Avrupa ve Rusya gibi daha hızlı ve ucuz ülkelerden almaktadır

(IWF, 2010). Raporda çocukların cinsel istismarı içeriklerinin %72'sinde 0-10 yaş arası çocukların ciddi anlamda şiddet gördükleri; bu içeriklerin %44'ünde ise bu çocukların cinsel işkence ve vahşete maruz kaldıkları belirtilmektedir (IWF, 2010).

Dünya ölçeğinde çocuk istismarına karşı mücadele yürüten uluslararası "Save The Children" Örgütü de dünyada milyonlarca çocuğun fuhuş amaçlı olarak istismar edildiğine dikkat çekmektedir. Bunların dışında cinsel istismar ve cinsel köleliğe maruz bırakılan çocukların ise bu sayıyı daha da artırdığını belirtilmektedir (Redbarnet, 2013). Örgüt, İnternet ortamındaki çocukların cinsel istismarı içeriklerinin asıl kaynağının gerçek hayat ve dünyanın sorunlu bölgeleri olduğuna inanmakta ve bu durum düzeltilmeden İnternet ortamındaki durumun da düzelmeyeceğini dile getirmektedir (Savethechildren, 2013).

Yapılan araştırmalar çocuk pornografisi, çocuk fahişeliği ve çocuk seks turizmi arasında birbirini üreten, büyüten ve destekleyen yakın bir ilişkinin olduğunu ortaya koymaktadır (Çam, 2003: 63). Çocuk pornografisi içeriklerinin barındırılması için, yasal problemlerle karşılaşmamak amacıyla nispeten daha fakir ve bu konularla ilgili yasal düzenlemeleri bulunmayan ülkeler seçilirken, fuhuş ve porno için kullanılan çocukların daha çok dünyanın sosyal ve siyasal çalkantıların yoğunlukta olduğu ve fakir bölümlerinde yaşayan mağdurlardan oluştuğu görülmektedir. Bu nedenle kaynak kurutulmadan İnternetteki bu tür içerikle mücadelenin ne kadar etkili bir çözüm olduğu sorusu gündeme getirilmektedir (INHOPE, 2012b).

Nitekim, çocuk pornografisi, çocuk fahişeliği ve çocuk seks turizmi konusunda Sri Lanka, Tayvan, Singapur, Tayland, Dominik Cumhuriyeti ve Filipinler önemli merkezler haline gelmiştir. Bu ülkelerdeki iç savaşlar, siyasi ve sosyal krizler, ekonomik güçlükler sahipsiz sokak çocuklarını, yoksul ailelerin çocuklarını ve özürlü çocukların önemli bir kısmını pornografi sektörüne malzeme yapmaktadır.¹²

¹² Stockholm'de, çocukların ticari amaçlı cinsel istismarına karşı yapılan uluslararası nitelikli kongrede (A World Congress Against Sexual Exploitation of Children and Adolescents) sunulan çocuk fahişeliğine ilişkin raporlarda aktarılan veriler oldukça çarpıcıdır. Raporlarda, Filipinler'de 6 yaşındaki çocukların 6 \$'a motosiklet sürücüleriyle cinsel ilişkiye girdikleri; Bombay'da yüzlerce çocuğun genelevlerde kafesler içinde tutulduğu, sokaklarda 12 yaşındaki çocukların 50 cent karşılığında yarım

Çocuk fahişeliği ile çocuk pornografisi üretimi arasında sıkı bir ilişki olduğu görülmektedir. John Hopkins Üniversitesi'nin Koruma Projesi kapsamında yaptığı çalışmalara ve Human Rights Watch'ın elde ettiği verilere göre, Hindistan'da 200 bini Nepal'de olmak üzere toplam 1 milyon 14 yaş altı çocuğun seks kölesi olarak çalıştırıldığı, Sri Lanka'da yaşları 6 ila 14 arasında değişen 10 bin çocuğun geneleve düştüğü, 800 bin dolayında Taylandlı çocuğun fahişelik için satıldığı, 1991-97 arasında Komboçyalı 15 bin kızın seks kölesi yapıldığı; Filipinlerde 60 bin, Brezilya'da 300 bin, ABD'de 100 ile 300 bin arasında değişen 17 yaş altı çocuk fahişenin bulunduğu tespit edilmiştir (Uzunay ve Koçak, 2005: 105; Çam, 2003: 64).

Benzer şekilde, çocuk pornografisi sektörünün, çocuk seks turizmiyle birlikte daha da yaygınlaştığı ve genişlediği görülmektedir. Zengin ve gelişmişlik düzeyi yüksek ülkelerden çocuk fuhuşu yapılan/yaptırılan az gelişmiş veya fakir ülkelerdeki merkezlere çocuk seks turizmi yapılmakta ve bu bir sektör olarak giderek gelişmektedir. Öyle ki, bu tür seyahatlerin yaygın görüldüğü ülkelerde hükümetler konuyla ilgili bazı idari ve cezai tedbirler almak zorunda kalmakta ve bu konuda vatandaşlarından ihbar vb. yöntemlerle yardım talebinde bulunmaktadırlar. Örneğin, Hollanda'da sadece çocuk seks turizmi konusundaki ihbarları kabul eden "Meldkindersekstoerisme" adında müstakil bir İnternet ihbar merkezi faaliyet göstermektedir (Meldkindersekstoerisme, 2013).

Diğer yandan, konunun bir de insan kaçakçılığı boyutu bulunmaktadır. İnsan kaçakçılığına kurban gidenlerin %80'ini kadınlar, %50'sini çocukların oluşturduğu, bunların %70'inin cinsel sömürü kurbanı olduğu belirtilmektedir. ABD Hükümetinin tahminlerine göre her yıl ABD'de 14.500-17.500 insan kaçırılmaktadır. Adalet Bakanlığı ile NCMEC (Ulusal Kayıp ve İstismara Uğramış Çocuklar Merkezi) adlı STK, pornografinin cinsel sömürü amaçlı insan kaçakçılığını artırdığını dile

saatliğine ilişkiye girdikleri; Sri Lanka sahillerindeki evlerin erkek çocukların turistlerle birlikte oldukları önemli mekanlar olduğu; Amsterdam'da *shov-window* fahişeliğinde ağırlıklı olarak 14 yaş altı çocukların çalıştırıldığı; New York'ta 15 yaşındaki kız çocuklarının 60\$'a yetişkinlerle ilişkiye girdikleri; Afrika'nın pek çok ülkesinde ise hemen her mekanda (otobüs durakları, tren istasyonları, barlar, parklar, kumsallar vs.) çocukların çok az bir para, yemek, şeker, okul kitapları hatta diskoteğe giriş bileti karşılığında satıldıkları belirtilmektedir (Çam, 2003: 64).

getirmektedir. Yakalanan birçok insan kaçakçısında pornografi üretmek ve satmak için kullanılan kamera gibi elektronik gereçler bulunmaktadır (McGinnis, 2011).

Görüldüğü gibi, çocukların cinsel istismarı ve çocuk pornografisi küresel ölçekte önemli bir güncel sorun haline gelmiştir. Buna mukabil çocuk pornografisine karşı yürütülen ulusal ve uluslararası mücadelenin önünde bazı engeller vardır. Çocuk pornografisinin tanımına ilişkin farklı anlayışlar, ülkelerin kanunlarında çocuk yaşı konusunda farklılıkların bulunması,¹³ yetişkin ile çocuk pornografisi arasında net bir ayrıma gidilememesi, ülkeler arasındaki yasal, sosyal ve kültürel farklılıklar ve ortak işbirliğinin sağlanamaması gibi nedenler bunların başlıcalarıdır.¹⁴

1.1.3.2.1.1.3 İnternette Pornografi ve İfade Hürriyeti

Demokratik toplumlarda düşünce ve ifade özgürlüğünün ayrılmaz bir parçası iletişim özgürlüğüdür. Günümüzde düşünceyi ifade etmenin en etkili ve yaygın araçlarından birisi de kuşkusuz İnternettir. Bu kapsamda, haber, bilgi ve düşüncelerin İnternet aracılığıyla kitlelere ulaştırılması özgürlüğü olarak ifade edebileceğimiz “İnternet özgürlüğü”, iletişim özgürlüğünün ve dolayısıyla düşünce ve ifade özgürlüğünün en önemli unsuru haline gelmiştir (Sınar, 2001: 47-48).

AİHS 10. maddesi “ifade özgürlüğü”nü açıklamıştır. Maddenin 1. fıkrasıyla herkesin haber, bilgi, görüş ve düşünce alma, bunları iletip yayma hakkı güvence altına alınırken,¹⁵ 2. fıkra ile, bu özgürlüğün ne zaman, nasıl ve hangi koşullarda

¹³ Her devlet iç hukukunda farklı yaşları çocuk olarak kabul etmektedir. Örneğin, Çin 14, Singapur 16 yaşın altındakileri çocuk olarak nitelendirmektedir. Devletlerin çocukların cinsel istismarına ilişkin iç hukuk düzenlemeleri ve ilgili çocukluk yaşı rakamları için bkz. **Sexual Offences Laws-Countries**, <http://www.interpol.int/Public/Children/SexualAbuse/NationalLaws/Default.asp> (23.11.2012).

¹⁴ Örneğin, çocuk pornografisi kapsamında bazı tanımlar, çocuğu temsil eden her türlü görsel ve sesli materyali içerirken, bazı tanımlara göre resimler, çizimler ve çizgi filmler çocuk pornografisi kapsamına alınmamakta, görüntü veya imajda mutlaka gerçek bir çocuğun bulunması gerekliliği öngörülmektedir. Bu durum, içerisinde gerçek bir çocuğun bulunmadığı yapay imajların ve çocuk şeklinde yapay maketlerin (pseudo-child) çocuk pornografisi olarak kabul edilmesini engellemektedir. Bu da çocuk pornografisi suçunun sınırlarının, tam olarak belirlenememesi anlamına gelmekte ve çocuk pornograficilerinin işini oldukça kolaylaştırmaktadır (Uzunay ve Koçak, 2005: 102, 106-107).

¹⁵ “Herkes ifade özgürlüğü hakkına sahiptir. Bu hak, kamu makamlarının müdahalesi olmaksızın ve ülke sınırları gözetilmeksizin, kanaat özgürlüğünü ve haber ve görüş alma ve verme özgürlüğünü de kapsar. Bu madde, Devletlerin radyo, televizyon ve sinema işletmelerini bir izin rejimine tabi tutmalarına engel değildir.”(Anayasa Mahkemesi, 2011).

sınırlandırılabilceğı belirtilmektedir. Burada zikredilen sınırlandırma konularından birisi de “genel ahlakın korunması”dır.¹⁶

AİHM ise, ifade özgürlüğünün ihlali iddiaları karşısında 2. fıkradaki sınırlama ölçütlerine uygun müdahale olup olmadığını saptamak için şu ölçütleri esas almaktadır: 1) Sınırlama veya müdahale için mevzuat olup olmadığı, 2) Sınırlamanın meşru bir amacının bulunup bulunmadığı, 3) Sınırlamanın demokratik bir toplum için gerekli olup olmadığı (Birtek, 2011).

Nitekim, AİHM bazı davalarda “ifade özgürlüğü”nün “genel ahlak” gerekçesiyle sınırlandırılabilceğine ilişkin kararlar vermiştir. Bunlardan birisi 1971 yılında İngiltere’de yaşanan Handyside olayıdır. Richard Handyside isimli İngiliz yayıncının yayınladığı “Küçük Kırmızı Ders Kitabı” adlı eserin Savcılık tarafından müstehcen bulunarak yayının durdurulması ve toplatılmasından sonra iç hukuk yollarının tüketilmesini müteakip konu AİHM’nin önüne gelmiştir. Mahkeme, “genel ahlakın korunması” için “ifade özgürlüğü”nü sınırlandıran ilgili ülkenin yargı kararını yerinde görerek yapılan işlemi haklı bulmuştur.¹⁷

AİHM’in konuyla ilgili bir diğer kararı da yine İngiltere’de 1999’da vuku bulan Perrin Olayıdır. Olay, Müstehcen Yayınlar Birimi’nde görevli bir polis memurunun İnternette vücutları pislikle kaplı insanlar ve daha başka pornografik görüntülerle karşılaşması üzerine ortaya çıkmıştır. Polis memuru, yaptığı araştırma sonucu Hove’da yaşayan Stephane L. Perrin’i yakalamış, konu yargıya taşınmış ve Perrin 30 ay hapse mahkum edilmiştir. Perrin, kararın ifade özgürlüğünü ihlal ettiğini, halen İnternette bu tür içeriklere ulaşılabilceğini, başvuru tedbirin orantısız olduğunu; filtreleme, erişimin engellenmesi ve evde aile tarafından alınacak bazı tedbirlerle

¹⁶ “Görev ve sorumluluklar da yükleyen bu özgürlüklerin kullanılması, yasayla öngörülen ve demokratik bir toplumda ulusal güvenliğin, toprak bütünlüğünün veya kamu güvenliğinin korunması, kamu düzeninin sağlanması ve suç işlenmesinin önlenmesi, sağlığın veya ahlakın, başkalarının şöhret ve haklarının korunması, gizli bilgilerin yayılmasının önlenmesi veya yargı erkinin yetki ve tarafsızlığının güvence altına alınması için gerekli olan bazı formaliteler, koşullar, sınırlamalar veya yaptırımlara tabi tutulabilir.” (Anayasa Mahkemesi, 2011).

¹⁷ AİHM Kararı ve Raporu için bkz. <http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-57499>; <http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-73423> (30.04.2011)

engeleme gibi daha iyi yöntemlerin bulunduğunu gerekçe göstererek temyize başvurmuş ancak bu talebi reddedilmiştir (Altınay, 2011: 86-87).

AİHM dava konusu somut olayda müdahalenin ahlakın ve başkalarının haklarının korunması meşru amacını güttüğünü, ahlakın korunması açısından devletlere tanınan geniş takdir hakkının aşılmadığını, belirtilen materyale serbestçe ulaşılabilmesini ve bireylerin ahlaki gelişimine zarar verecek nitelikte olduğunu belirterek İngiliz Mahkemelerinin verdiği kararı yerinde bulmuştur (Altınay, 2011: 86).

Keza, pornografiye erişim özgürlüğünün ifade özgürlüğü kapsamında değerlendirilmesinin mümkün olamayacağı birçok kişi tarafından ifade edilmektedir. Örneğin, bunun mantıksal ve ahlaki temelsizliğine vurgu yapan Whittle, pornografiyi özgür ifade ve pornocuları sanatçı olarak görenlerin büyük resmi gözden kaçırdıklarına dikkat çekmektedir. Whittle şöyle demektedir: “Kadınların ve çocukların objeleştirilmesi ve sömürülmesini haklılaştıracak ne olabilir? Özgür ifadeyi müstehcenliğin rasyonali olarak görmek, silah taşıma hakkını silahlı soygunun meşruiyeti olarak görmek kadar anlamsızdır.” (Whittle, 1997: 83).

Yine Apple’ın kurucusu dahi isim Steve Jobs, yetişkin pornosunu ifade özgürlüğü olarak görenlerin safında yer almamıştır. Bilakis bu kadar kolay ulaşılabilen pornografiden kendi üç çocuğu başta olmak üzere bütün çocukların uzak tutulmasını ve korunmasını istemiştir. Jobs, pornografinin ulaşamadığı özgür alanlar olmasının da özgürlüğün bir parçası olduğunu savunmuştur. Bu yaklaşım, porno özgürlük müdür diye tartışılırken dünyanın çoktan porno izlememenin de bir özgürlük olduğu hususunu tartışmaya başladığını göstermektedir (Özdemir, 2011).

Tıpkı sigara tüketiminin kişisel bir tercih olmakla beraber, toplum sağlığına zararlı olduğunun herkes tarafından kabul edilmesi gibi, sosyal dokuya zarar veren ve toplum sağlığını ilgilendiren pornografi konusu kişisel özgürlükler kapsamında değerlendirilmemelidir. “Ben müstehcen görüntüleri en kolay şekilde izlemek istiyorum, istemeyen bu tür İnternet sitelerine girmesin” demek gerçekçi ve insafli olmayacağı gibi, toplumun aleyhine bir özgürlük arayışının makul görülmesi de

mümkün değildir. Nasıl her sigara içen kanser olmamasına rağmen, ‘Dumansız hava sahası’ uygulaması toplumun çok büyük bir kesimi tarafından kabul görüyorsa; herkesin zarar görmediğini söylemek, pornografinin düzenlemelere konu olması gereği ve gerçeğini değiştirmemelidir (Altınay, 2011: 89).

Nitekim pornografi, İslamiyet, Hristiyanlık ve Yahudilik gibi büyük dinler başta olmak üzere neredeyse bütün dinlerce ve feminizm gibi düşünce akımları tarafından da tasvip edilmemektedir. Benzer şekilde dünyada yaşayan toplumların büyük bir çoğunluğunun örf, adet ve gelenekler gibi yazılı olmayan toplumsal kuralları açısından da uygun bulunmayan pornografi, çağımızın en büyük sosyal sorunlarından birisi olarak kabul edilmektedir.

Konunun fazlaca gündeme getirilmeyen bir yönü daha bulunmaktadır. Günümüzde porno işi, sadece film üreticilerini ve dağıtıcılarını içeren değil, aynı zamanda, bankaları, yazılım üreticilerini, kredi kartı firmalarını, İnternet sağlayıcıları, kablolu yayıncılık yapan şirketleri ve otel zincirlerini de içini alan ve zincirleme olarak birbirine bağlı, trilyon dolarlık büyük bir endüstri durumundadır.¹⁸ Bu endüstri, toplumsal maliyeti ne olursa olsun, daha çok kazanmak ve kar elde etmek için var gücü ile çalışmakta ve pornografinin yayılmasının önündeki toplumsal, kültürel ve yasal tüm engelleri aşmaya, dirençleri kırmaya çaba sarfetmektedir.¹⁹

Bu nedenle porno endüstrisi, bir yandan kendi pazarını oluşturan teknolojilerin ortaya çıkmasına ve gelişmesine yardımcı olurken; diğer yandan, pornoyla ilgili toplumda olumlu bir imajın oluşturulması, popüler kültüre entegrasyonu, kamu otoriteleri ve toplumca olağan ve normal görülmesi, yasal güvenceler elde etmesi yönünde çok yönlü ve ciddi çalışmalar yapmaktadır (Dines, 2011).

¹⁸ Örneğin, Holiday Inn, Hilton, Sheraton, Radisson, Hyatt and Marriott gibi büyük otellerin, müşterilerine sundukları pornografik filmler yayınlanan paralı televizyon kanallarından elde ettikleri gelirin 2007 yılı rakamlarına göre 500 milyon doları geçtiği dile getirilmektedir (Dines, 2011).

¹⁹ Porno üreticilerinin ve ticaretini yapanların konuya yaklaşımlarını yansıtmaları bakımından, pornografi konusuyla ilgili çalışmalarıyla tanınan ABD’li sosyolog Prof. Dr. Gail Dines’in, “Bana güvenin; yüzlerce pornocuyla mülakat yaptım ve onları heyecanlandıran şeyin sadece ‘kar’ olduğunu gördüm... Kimse gelecekte neyle karşılaşacağımızı bilmiyor. Fakat porno sektörü daha marjinal daha şok edici şeyler arıyor.” ifadesi oldukça anlamlıdır. (Guardian, 02.07.2010).

Nitekim porno, yakın bir zamana kadar, toplumdan - özellikle çocuklardan - özenle uzak tutulan, sözünü bile etmekten utanılan bir konuyken, 1960'larda başlayan, 'Cinselliğin baskılardan kurtulup özgürleşmesi' ve “zararsız yetişkin eğlencesi” söyleminin bir devamı olarak ve özellikle 1970'lerden sonra entelektüel bakımdan da "savunulabilir bir şey" haline gelmiştir. Zamanla, en başta ticari nedenlerle, dünyada pornoya tolerans artarak devam etmiştir. Sektörün girişimleri ile ve yaygın medyanın pornografiyi cazip hale getiren yayınlarıyla bugünün dünyasında vardığı yer, bir tür 'benimsenme' ve kısmen saygınlık kazanma aşamasıdır. Bugün artık, özellikle Batılı toplumlarda evde porno bulundurmamak şık ve modern sayılıyor. Eskiden porno oyuncular, anonim kişiler olarak yaşarken bugün porno 'star'larından söz edilebiliyor ve saygın gazeteler porno oyuncularıyla söyleşiler yapıyorlar. Burada en vahim olan ise, pornografiyi topluma mal etmeye yönelik böylesi aleni girişimlere gelen tepkilerin cılızlığıdır. Konu, medyada sadece bir magazin haberi olarak algılanıyor (Bouché, 2009: 5, 8; Caydı, 2010). Gelinek nokta şu ki, bugün artık pornografi toplumların birçoğunda kabullenilmiş; “olağan” ve hatta “gerekli” olarak görülmeye başlanmıştır. Herkes küresel seks endüstrisinin sömürücü uygulamalarının hedefi haline gelmiştir; ya üretici tarafında ya da tüketici olarak (Bouché, 2009: 9).

Pornografi sektörünün “benimsenme” ve “kabul görme”ye ilişkin yapmış olduğu söz konusu çalışmaların mücadele alanlarından birisinin de İnternet pornografisi alanı olduğunu söylemek mümkündür. Nitekim, pornografi sektörü bugün, pornografik içeriklerin İnternet ortamında serbestçe barınabilir, bulunabilir ve paylaşılabilir olması için konuyu “İnternet özgürlüğü” ve “ifade özgürlüğü” bağlamına ve alanına çekmeye çalışmaktadır. Sektör, bir kısım sansür konusunda hasas olan özgürlükçü çevreleri de yanına alarak, pornografiye serbestçe erişim konusunu “İnternet özgürlüğü” ve “ifade özgürlüğü” kapsamında savunma eğilimindedir. Bu stratejiye, aynı zamanda çocuk pornografisine de bu yolla bir özgürlük alanı açmaya çalışan çocuk pornografisi sektörünün de destek vermesi muhtemeldir. Bu nedenle, bazı ülkelerin pornografik içeriklere erişimi engelleyen veya sınırlandıran uygulamaları, pornografi sektörünün gayretleri ile “Sansüre Hayır”, “Pornoya Özgürlük”, “Pornoma Dokunma” kampanyalarıyla karşılık bulabilmektedir.

Bu stratejiyi ve kampanyaları çocuk pornografisine serbestlik getirilmesini savunan kişi ve grupların desteklemelerini kendilerinden beklenen bir davranış olarak görmek gerekmektedir. Çünkü, bu çevrelerin de benzer strateji ve yaklaşımlarla çocukların bir seks objesi olarak görülmesinin ve kullanılmasının kişisel bir tercih ve özgürlük konusu olduğunu, bunun doğal, olağan ve normal karşılanması gerektiğini savunarak, çocuk pornografisinin serbest bırakılmasını sağlamaya çalıştıklarına da rastlanılmaktadır. Dolayısıyla bu çevrelerin, yetişkin pornografisi konusundaki toplumsal direncin ve muhalefetin “özgürlük” argümanı ile kırılması ve izale edilmesini, hedeflerine ulaşmak için bir kazanım olarak görmeleri doğaldır.

Nitekim, pedofili hastaları, bir yandan kendilerini saflığı seven olarak adlandırıp, çocuklara yaklaşımlarını saflığa ve temizliğe duyulan en üst düzey sevgi olarak tanımlayarak masumiyet görüntüsü oluşturmaya çalışırken (Çetinkaya, 2006); diğer yandan da bu patolojik vakayı, bir yetişkinin cinsel ilgisi, kişisel tercihi ve kendini ifade biçimi olduğu savıyla “yasallaştırma ve normalleştirme”ye çaba göstermektedir (O’Connell, 1999). Bu bağlamda çocuk pornosunu da bireysel özgürlük çerçevesinde bir tür tercih ve “haz hakkı” biçiminde ortaya koymaya ve konunun düşünce ve ifade özgürlüğü bağlamında ele alınmasını sağlamaya gayret göstermektedirler. Çocuklara yönelik cinsel ilgi ve davranışların giderek yaygınlaştığı ve kabul gördüğünü ileri sürerek bunu meşrulaştırmak ve haklılaştırmak istemektedirler (Çam, 2003: 65). Keza, yakın bir zamana kadar nasıl eşcinsellik bir sapkınlık olarak görülürken bugün bir bireysel tercih ve özgürlük konusu olarak kabul ediliyor ise, zaman içinde kendilerinin de bu kapsamda değerlendirilip kabul görececeklerini hesaplamaktadırlar (Lütfi Güvener ile kişisel iletişim, 24.07.2013).

Nitekim, Hollanda ve İsveç gibi bazı ülkelerde çocuk pornografisinin yasallaşması gerektiğini savunan bazı siyasi oluşumlar dikkat çekmektedir. Örneğin Hollanda’da 2006 yılında pedofililer tarafından kurulan Komşuluk Aşk, Özgürlük ve Çeşitlilik Partisi (Partij voor Naastenliefde, Vrijheid en Diversiteit-PNVD), çocuk tacizinin suç olmaktan çıkartılmasını, çocukların rızalarının alınması şartı ile pedofililerle birlikte olma hakkının verilmesini, hayvanlarla seksin legalleşmesini, çocuk ve hayvan

pornografisinin yasal hale getirilmesini ve televizyondan yayınının serbest bırakılmasını savunmuştur (Wikipedia, 2013).

Pedofili alanındaki tabuları yıkmak istediğini açıklayan PNVD'nin kapatılmasına yönelik olarak "Soelaas" adlı bir grubun başvurusuyla açılan davayı karara bağlayan mahkeme ifade, toplanma ve örgütlenme özgürlüğünü hatırlatarak “Onlar sadece moral değerleri ifade etmek istiyorlar. Ortada bir partiyi kapatmaya yetecek kadar delil yok” gerekçesiyle talebi reddetmiştir. Nihayet, 14 Mart 2010 tarihinde PNVD kendi kararıyla partiyi feshetmiştir (Hürriyet, 17.07. 2006).

Benzer şekilde, İsveç'te ortaya çıkıp Avrupa genelinde örgütlenen ve yakın dönemde Almanya ve Fransa gibi bazı ülkelerde önemli siyasi başarılar elde eden ve özellikle İnternette sansüre karşı mücadele veren Korsan Parti (Pirate Party)'nin fikir babası ve kurucusu İsveçli Rick Falkvinge'nin çocuk pornografisiyle ilgili açıklamaları Avrupa'da tartışmalara yol açmıştır. Falkvinge kişisel blogunda “yürürlükteki yasaların tüm genç kuşağı cinsel suçlu olarak damgaladığı ve şimdiye kadar çocuk pornosuyla mücadele başlığı altında atılan tüm adımların sansür ve İnternet yasaklarından ibaret olduğu” yorumunu yapmış ve bu nedenle çocuk pornografisinin yeniden yasal hale getirilmesi için yapılacak mücadeleyi de ifade özgürlüğüyle eşit tuttuğunu belirtmiştir (Wikipedia, 2012a; Milliyet, 10.09.2012).

1.1.3.2.1.2 Şiddet, Vahşet, Nefret ve İntihara Yönlendirme İçerikleri

İnternette görülen şiddet, vahşet, nefret ve intihara yönlendirme konulu içerikler diğer sakıncalı ve zararlı içerik türlerindendir. Şiddeti ve saldırganlığı özendirme, intihara teşvik etme, ırk, cinsiyet ve din temelli ayrımcılık ve nefreti kışkırtma gibi içerikleri ile İnternet, özellikle çocukların ve gençlerin gerçeklik sınırlarını zorlamalarına ve yanlış model oluşturmalarına, kendilerine ve yaşadıkları topluma zarar verecek düşünce, tutum ve davranışlara yönelmelerine neden olmaktadır.

İnternet ortamında bulunan bu tür içerikler, merak eden, öğrenmeye ve keşfetmeye çalışan, eğlenmek isteyen herkes için ve özellikle bunun yanında risk almayı seven, kurallara uymaktan hoşlanmayan, hayat hakkında yeterince tecrübesi bulunmayan ve

karar verme yeteneđi fazla gelişmemiş çocuklar ve gençler için tehlikeli mecralara yönelme konusunda tehdit oluşturmaktadır. Dolayısıyla, İnternet sitelerinin ve sohbet ortamlarının çocuklara ve gençlere aşılamaaya çalıştığı “aykırı yaşama” ve “şiddet” kültürüne yönelik çabaların etkisinde kalabilmektedir (Tarhan, 2012: 105).

Günümüzde, dünyanın çeşitli bölgelerinde yaşanan kavgalar, çatışmalar, işkence olayları, savaş suçlularının infazı veya suç veya terör örgütlerince yapılan infazlar gibi olayların görüntülerinin İnternette kolay bir şekilde yayınlanabilmesi ve bu sitelerin en çok ziyaret edilen siteler arasında yer alması kaygı verici bir duruma gelmiştir. Öyle ki, İnternette, işkence, kavga, vahşet ve şiddet konulu hazırlanan siteler, özellikle gençlerin ve çocukların en çok ziyaret ettiği içerikler arasındadır. Nitekim, İnternette, son zamanlarda popüler olan, görüntü paylaşım sitelerinde (Yahoo Video, Youtube Video, Msn Video gibi) gençler ve çocuklar, en çok kavga, nefret ve şiddet içerikli görüntüleri izlemektedir. Keza, genç ve çocuklar tarafından hazırlanmış şiddet içerikli görüntülerin de, görüntü paylaşım sitelerine en çok paylaşılan görüntüler arasında yer alması dikkat çekicidir (AREM, 2008: 60).

Aynı şekilde İnternet, şiddetle birlikte ayrımcılığı, ayrımcılığa dayalı nefreti ve bu yöndeki çeşitli tehlikeleri de beraberinde getirmektedir. Günümüzde, ırkçılık, yabancı düşmanlığı, etnesite, cinsiyet, din, dil, mezhep gibi pek çok ayrımcılık türleri İnternette yer bulmaktadır. Bu tarz içerikler ve ırkçı, yabancı düşmanı web sitelerinin sayısı her geçen gün hızla artmaktadır. Pek çok ülke bu ve benzeri konularda “Nefret Suçları” adı verilen yasaları uygulayarak mücadele etmektedir (AREM, 2008: 59). Fakat, farklı yasal düzenlemeler sorunuyla burada da karşılaşmakta; bazı ülkelerde bu içerikler suç kabul edilirken bazılarında fiili bir eyleme dönüşmeden suç kabul edilmemektedir (INHOPE, 2012a).

Sayıları azımsanmayacak düzeydeki intihara yönlendirme siteleri de, tüm dünyayı tehdit eden bir olumsuzluk olarak görülmektedir. İnternet sitelerinde yer alan bazı bilgiler adeta intihara özendirme gayesiyle hazırlanmakta ve özellikle gençleri hedef almaktadır. Örneğın, bazı İnternet sitelerinde gençleri intihara özendirici yazılar yayınlanmakta veya intihara teşvik eden türden satanist içerikler barındırılmaktadır.

Bu siteler intihar etmek isteyip de cesaret edemeyenlere öneriler sunarak, intihara eğilimli kişileri etkileyebilmektedir. İnternette kısa bir arama yaparak kolayca ulaşılan bu sitelerde nasıl intihar edileceği aşamalı olarak anlatılmaktadır.

Yapılan bir araştırmada arama motorlarının intiharla ilgili psikolojik yardım bilgilerinden çok intiharı teşvik eden bilgiler içerdiği tespit edilmiştir. Bristol, Oxford ve Manchester Üniversitelerinden araştırmacılar Google, Yahoo, MSN ve Ask gibi arama motorlarında intiharla ilgili kelimeleri taramışlar ve sonuçların çoğunluğunda intiharı önleme konusunda bilgi vermekten ziyade intihar yöntemleri, hız, kesinlik ve acı miktarı gibi bilgileri içerdiği görülmüştür (Kaya, 2010: 90).

Özellikle sohbet odaları ve forumlar gibi kimliğin kolayca gizlenebildiği ve kişiler ile anlık iletişimin mümkün olduğu ortamlarda bu tür girişimler yoğunluk kazanmaktadır.²⁰ Sohbet odalarında kişiler intihar için birebir teşvik edilebilmekte, intihar etmiş olanlar kahramanlar olarak sunulabilmekte ve intihar tüm sıkıntılar için bir çözüm yöntemi olarak pazarlanabilmektedir.

Diğer yandan İnternet üzerinden gerçekleştirilen intihar akitleri ve toplu intihar olaylarına da rastlanılmaktadır. Bu tip durumlarda iki veya daha fazla kişi belirli zaman ve yerde intihar etmek üzere anlaşmakta ve zamanı gelince birlikte intihar etmektedir. Bunun bir örneği 2004'de Japonya'da gerçekleşmiştir. İnternette tanışan yedisi bir grupta, ikisi başka bir grupta dokuz kişi aynı anda intihar etmiştir. Yapılan araştırmalarda intihar edenlerin İnternette tanıştıkları ve bu fikri intihar yöntemleri hakkında bilgi veren web sitelerinden edindikleri belirlenmiştir (Kaya, 2010: 90).

İntihara yönlendirme İnternette her zaman açıkça gerçekleştirilmemekte, dolaylı yöntemler kullanılarak erişim engelleme yöntemleri çok kolay aşılabilmektedir. Bu tür mesajlar bazen bir edebi metnin bazen de bir videonun içine eklenmekte veya içerik aldatmacası tekniği kullanılabilmektedir. Bu nedenle, içeriğin intihara teşvik ettiğinin tespit edilmesi çoğu zaman bireysel engelleme yöntemiyle, ancak bir insan

²⁰ Örneğin Amerika'da 19 yaşında bir genç kendisini 1.500 kişi web kamerası ile canlı olarak izlerken intihar etmiştir (Telegraph, 2008)

tarafından değerlendirilmesi sonucunda ortaya çıkabilmektedir. Otomatik içerik engelleme sistemleri bu konuda çaresiz kalabilmektedir. Diğer yandan, video paylaşım siteleri zararlı içeriği engellemek için çeşitli yöntemler kullansa da bu tür sitelere milyonlarca videonun eşzamanlı olarak yüklenmesi tüm videoların site yöneticileri tarafından takibini neredeyse imkansız kılmaktadır (Kaya, 2010: 91).

1.1.3.2.1.3 Kumar / Bahis ve Uyuşturucuya Yönlendirici İçerikler

İnternet her yaş grubundan kullanıcıları, özellikle çocukları ve gençleri kumar, bahis ve şans oyunları oynamaya teşvik etme, uyuşturucu ve uyarıcı madde satışı ve bu maddeleri kullanmaya yönlendirme gibi pek çok zararlı faaliyetlerin hızlı bir şekilde yayılmasına ve artmasına da imkan sağlamaktadır.

Kumar bilinen ve belgelenmiş bir sorun olsa da, İnternet, kumarın daha çok yayılmasına ve erişilebilir olmasına kolaylık sağlamaktadır. Kumar bağımlılarının kurtulması ve bağımlılığın tekrar ortaya çıkmasının engellenmesi İnternet kumarıyla daha zor hale gelmiştir. İnternet erişimi olan herkes için çevrimiçi veya sanal casinolar tüm gün açıktır. İnternet kumarı için gerekli olan tek şey geçerli bir kredi kartının olmasıdır. Gençler ve çocuklar da dahil, buna sahip olan herkes, İnternet yardımıyla kumar oynanan ya da bahis yürütülen sitelerle karşılaşmakta ve erişim kolaylaşmaktadır (Ocak, 2012: 31).

Bu nedenle, İnternet üzerinden oynanan kumar, bahis ve şans oyunları büyük paraların döndüğü devasa bir sektör haline gelmiştir. Kumar ve bahis bağımlıları başta olmak üzere insanlar, günümüzde sayılarının on binlerce olduğu telaffuz edilen İnternet sayfaları aracılığıyla kumara, bahise ve şans oyunları oynamaya teşvik edilmektedir. Nitekim, günde onbir milyon üyenin oyun oynadığı, Facebook'un geliştirdiği ve 200 milyon üyesi ile dünyanın en büyük oyun platformu olan Teksas Hold'em Poker adlı kumar oyunu bunun bir örneğidir (Medyahayat, 2010).

Diğer yandan, İnternette yer alan online kumarhaneler genellikle denetimin az olduğu ve vergi cennetleri olarak da bilinen okyanus adalarından hizmet vermektedir. Örneğin, 68 bin nüfuslu Antigua ve Barbuda ada devletinde online kumarhane sayısı

119'u bulunmakta ve bu kumarhanelerde adanın nüfusunun %7'sine karşılık gelen yaklaşık 5 bin kişi istihdam edilmektedir (Goldsmith ve Wu, 2006: 172).

Bu şekilde online kumarhaneler hukuki sorumluluktan kaçtıkları gibi vergi ve kara para aklama denetimlerinden kendilerini kurtarmaktadırlar. Online kumar sitelerine kolay erişilebilir olması, İnternet üzerinden yüklü miktarlarda para transferinin gerçekleştirilebilmesi ve oyunların anonim olarak oynanması bu sitelerin kara para aklanması için kullanıldığı yönündeki şüpheleri artırmaktadır (Çağlar, 2011: 81). Diğer yandan, online kumarhanelerin yatırım giderleri normal kumarhanelere göre daha az olduğu için çok daha yüksek oranlarda ikramiye dağıtabilmektedir. Bu da cazibelerinin artırmasına neden olmaktadır (Kaya, 2010: 113).

Aynı şekilde, sanal ortamda suç takibinin zor olması sebebiyle uyuşturucu ve uyarıcı madde kaçakçıları, pazarlanma, satış ve üretimin her aşamasında İnterneti kullanmaktadır (AREM, 2008: 69). Uluslararası Narkotik Kontrol Kurulu'nun 2011 yılı raporuna göre, tüm dünyada uyuşturucu madde satışları büyük ölçüde İnternet ya da cep telefonları aracılığıyla yapılmaktadır. Özellikle sosyal medya uyuşturucu ve yasa dışı ilaç satışlarının yeni mecrası haline gelmiştir (INCP, 2011). Bazı İnternet siteleri uyuşturucu ve uyarıcı madde türleri, üretim teknikleri ve üretim için hammaddelerin nasıl temin edilebileceğine ilişkin bilgilere yer verirken, bazıları da kişileri uyuşturucu ve uyarıcı madde kullanmaya alenen özendirecek sohbet odaları, forum, video vb. içerikler sunmaktadır. Bu şekliyle İnternet, hem uyuşturucu ve uyarıcı maddeler hakkında bilgi veren bir aygıt hem de suç failleri arasında iletişimi sağlayan bir araç olarak kullanılmaktadır (Kaya, 2010: 100).

1.1.3.2.1.4 Telif Hakkı İhlallerine Ait İçerikler

İnternette görülen en önemli içerik sorunlardan birisi de telif hakkı ihlalleridir. Fikir ve sanat eserlerinin izinsiz kullanımı İnternette en çok rastlanan içerik sorunlarındanıdır. Bilimsel ve edebi eserlerin izinsiz yayımı ve dağıtımı, bilgisayar programları, bilimsel ve teknik nitelikteki fotoğraflar, haritalar, planlar, projeler, krokiler, resimler, maketler, mimarlık ve şehircilik tasarımları, sahne tasarımları vb.

bu kategoride sayılabilir. Müzik eserlerin yasaya aykırı yayın ve dağıtım sorunu da bu çerçevede gündeme gelmektedir. Güzel Sanat eserleri ve sinema eserleri de sıkça İnternet üzerinde yasa dışı olarak dağıtım yapılabilen ürünler olarak karşımıza çıkmaktadır (Salcı ve Güneş, 2010). Teknolojinin gelişimiyle birlikte kopyalama, kayıt ve taklit gibi eylemler kolaylaşmış, fikri mülkiyet haklarına tecavüz de artmıştır. İnternetin yaygınlaşmasıyla, telif haklarına yönelik sorunlar, ticari ve hukuksal boyutları ile en karmaşık meselelerden birisi haline gelmiştir.

Elektronik ortamda üretilen veya bu ortama taşınabilen herhangi bir özgün bilgi, ürün veya sanat eseri başlangıçta yüksek maliyetle üretilmekte fakat, çoğu zaman bir kez üretildikten sonra tekrar üretimi veya kopyalanması ve başkalarıyla paylaşılması kolaylıkla yapılabilmektedir. Fiziksel varlığı olan ürünlerden farklı olarak, bu tür ürünlerin, orjinalinin korunması zor ve hatta başka kişilerin bunlara ulaşması ve kullanması halinde uygun bedeli almak güç olabilmekte, genellikle de hiç alınamamaktadır (Mason, 1986). Bu durum sonunda fikir eserleri üretmek için emek ve zamanlarını veren hak sahipleri harcadıkları emek ve zamanın karşılığını alamamaktadır. Bir taraftan yaşamını bu işi yaparak devam ettiren kişiler çalışmaları karşılığında hak ettiği kazancı elde edemezken, öte yandan ise adalet duygusu ve erdemi zedelenmektedir (Dedeoğlu, 2006: 24-36).

1.1.3.2.2 İnternette Güvenlik ve Mahremiyet İhlali Sorunu

Hızla gelişen ve yaygınlaşan İnternetin denetimden uzak yapısı, İnterneti, illegal pek çok iş ve oluşumun yeni buluşma alanı yaparak güvenlik sorunlarına neden olurken, kişisel mahremiyet ihlallerinin de en önemli aracı haline getirmektedir.

1.1.3.2.2.1 İnternette Güvenlik Sorunu

İnternet, bilişim suçları olarak adlandırılan bilgisayar sistemlerine ve servislerine yetkisiz erişim, bilgisayar sabotajı, bilgisayar yoluyla sahtecilik ve dolandırıcılık, yazılımların izinsiz kullanımı, telekom hizmetleri hırsızlığı, bilgisayar sistemlerinin suç örgütleri tarafından kullanılması, tehdit ve gasp gibi suç çeşitlerinin hayatımıza girmesine sebep olmuştur (Şen, 2003).

Siber ortam, etraflıca bilinmediği ve tedbir alınmadığı zaman tehlikeli olabilmekte, kritik bilgilere siber suçlular tarafından kolayca ulaşılabilir. Bu durumda, bir işletme söz konusu olduğunda zarar, bir birey söz konusu olduğunda ise hak kaybı ortaya çıkmakta, bir devlet söz konusu olduğunda sonuç felaket olabilmektedir (Bayındır vd., 2009: 609).

İnternet, insanlığa hizmet etmenin yanında suçlulara yardım eden bir iletişim aygıtına dönüşmüştür. Şehirlerin uydu görüntülerinin ve fotoğraflı haritalarının yer aldığı uygulamalar, suç örgütleri ve teröristlerce de kullanılmakta; iletişim ve paylaşım için hazırlanan sohbet siteleri, iletişim programları ve sosyal ağlar, suçluların yakalanmadan birbirleriyle haberleşmeleri ya da propaganda yapmalarına imkan sağlamaktadır. Bugün terörist gruplar hazırlamış oldukları binlerce İnternet sitesinde broşür, dergi, gazete ve kitaplar yayınlamakta; bu yayınlarda polis takibinden nasıl kurtulacaklarından, bomba, bakteriyolojik ve radyoaktif silah yapımı ve kullanımına kadar bir dizi konu detaylı olarak anlatılmaktadır (Yamaç, 2003: 109).

Teknolojik gelişme, terörün de siber ortama taşınmasına yardımcı olmuş, suç, kabuk değiştirerek kendini siber ortamda göstermiştir (Atıcı ve Gümüş, 2006). İnternet, suç örgütleri, terör grupları ve ayrılıkçı güçler için organize olma, eğitim, iletişim ve propaganda, yardım ve bağış toplama aracı olarak kullanılabilmektedir (Aydın, 2007). Terör örgütleri İnterneti sanal propaganda, eleman kazanma, örgüt üyelerinin ve sempatanların eğitilmesi, eylem hazırlıkları, eylem emirlerinin verilmesi gibi birçok alanda kullanılmaktadır (AREM, 2008: 64-67). Alvin Toffler'ın "İçinde bulunduğumuz yüzyılda teröristlerin bir klavye ile bir bombadan çok daha tehlikeli olacağı" kehaneti gerçekleşmiş gibidir (Toffler, 1992: 148).

İnternet teröristlere uluslararası niteliğe kavuşma imkanı sağlamaktadır. Böylece, dünyanın farklı yerlerindeki teröristler İnternet üzerinden haberleşip koordine olarak bulundukları yerden binlerce mil ötede ortak eylemler yapabilmektedir. İnternet üzerinde yürütülen faaliyetler hem daha ucuza mal edilebilmekte hem de failler şifreli haberleşme ve anonimleştiren programlar kullanma gibi değişik tekniklerle kimliklerini rahatlıkla gizleyebilmektedir. Peru'daki Tubac Amaru, Kolombiya'daki

The Revolutionary Armed Forces of Colombia, Peru'daki Shining Path, El Kaide, Hindistan'daki Harkat-ül-Ansar ve ülkemizi hedef alan PKK terör örgütleri İnterneti kendi faaliyetleri için yoğun olarak kullanan örgütlere örnektir (Özcan, 2006).

Yine, İnternetin sağlamış olduğu imkanlarla ulusal veya uluslararası suç örgütleri, ekonomik, politik veya askeri amaçlarla siber saldırılar gerçekleştirebilmektedir. Hedef seçilen şahıs, şirket, kurum veya örgütlerin bilgi sistemlerine veya iletişim altyapılarına yapılan bu planlı ve koordineli saldırılar, web sayfalarının ele geçirilmesi, hizmet dışı bırakma saldırıları, karşı propaganda, gizlilik dereceli bilgilerin ele geçirilmesi veya enerji, iletişim, finans, güvenlik altyapısı gibi kritik sistemlere yönelik saldırılar şeklinde olabilmektedir (Alkan, 2012).

Son dönemde siber saldırıların siber savaflara dönüştüğü görülmektedir. Ülkeler siber savaşlar için hem savunma hem de saldırı amaçlı olarak siber ordular kurmakta ve kullanmaktadır. ABD, Rusya, Çin, İsrail, İngiltere, İran ve Kuzey Kore bu konuda önemli hazırlıkları olan ülkelerdir. Bu devletler aynı zamanda, uluslararası suçlara karışmadan devlet olarak yapamayacakları bu türden işleri, taşeron hackerler ya da taşeron organizasyonlar tarafından da gerçekleştirebilmektedir (Alkan, 2012). Bu nedenle günümüzde siber güvenlik, siber saldırılar ve siber savaşlar konusu bütün dünyayı çok yakından ilgilendiren önemli gündem maddelerinden birisi olmuştur.

Siber saldırıların ülkelere yüklediği ekonomik maliyetler giderek artmaktadır. Örneğin, yılda 100 binden fazla siber saldırının yaşandığı ABD'de bu saldırıların ülke ekonomisine maliyeti tahmini olarak 100 milyar dolardır. ABD siber savunma konusuna 2002'de 2,7 milyar dolar, 2003'de 4,2 milyar dolar harcamıştır. ABD'nin 2012'deki harcaması ise günlük 12 milyon dolar civarındadır. Keza, 2011'de siber saldırıların İngiltere'ye maliyeti 27 milyar pound olmuştur (Alkan, 2012).

Siber güvenlikle ilgili dikkat çeken konulardan birisi de küresel İnternet firmaları ve bunların kullanımları çok yaygın olan ürünleridir. Özellikle popüler arama motorlarının aynı zamanda iyi birer casus yazılımı oldukları ve bu ürünlerin yaygın olarak kullanıldığı ülkeler açısından riskler ve tehlikeler taşıdığı dile getirilmektedir.

Nitekim, “Google” bu yönüyle mercek altındadır. “Google”ı kontrol altında tutan ABD’nin bu yolla dünyanın bütün bilgisini topladığına dikkat çekilmektedir. Keza, resmi yazışmalarda dahi Yahoo ve Gmail gibi yabancı menşeli mail adreslerinin kullanması çok ciddi güvenlik riskleri oluşturmaktadır (Alkan, 2012).

Benzer bir tehlike ise, söz konusu firmaların ürettiği antivirüs yazılımlardır. Zira, bu antivirüslerin güncellemeler esnasında bilgisayara otomatik olarak aktardığı verilerin mahiyetleri kullanıcı tarafından bilinmemektedir (Demirkan, 2010). Ülkelerin bu sorunu güvenlik meselesi olmaktan çıkarmaları için kendi milli yazılımlarını geliştirmeleri gerekmektedir. Nitekim Almanya, Fransa, Rusya ve Çin Microsoft’un üretmiş olduğu yazılımları gizli bir takım şifreler taşıdığı düşüncesiyle kullanmamaktadır (Ersanel, 2001: 49).

İnternet ortamında cömertçe paylaşılan bilgiler, bu ortamın kötü niyetli kullanıcıları tarafından dolandırıcılık amaçlı kullanılabilir. İnternette sosyal medyanın yanında yoğun olarak kullanılmakta olan sosyal paylaşım ağları ve burada isteyerek ya da istemeden paylaşılan kişisel bilgilerin, verilerin kötü niyetli kişiler tarafından kullanılması insanların mağduriyetine sebep olmaktadır. Özellikle, düşünmeden paylaşılan ev ve iş adresi, telefon ve TC kimlik numaraları, anne kızlık soyadı ve güvenlik kodu bilgileri, kredi kartı numaraları, özel hayata ilişkin resimler ve diğer kişisel bilgilerin kötü niyetli kişilerce elde edilmesi mümkün olmaktadır.

Microsoft ve Harris Interactive firması tarafından yapılan bir araştırma kullanıcıların çevrimiçi güvenlik endişelerinin giderek artmakta olduğunu göstermektedir. Buna göre; Amerikalı yetişkinlerin %62’si çevrimiçi güvenlik konularında endişe duymaktadır. Bunların, %48’i kişisel bilgilerin siber suçlularca kullanılabileceğinden korktukları için çevrimiçi ortamlarda şahsi bilgileri vermekten, %37’si kişisel bilgileri vermek gerektiği için çevrimiçi alışverişten çekinmektedir. %36’sı kredi kartı bilgilerini çevrimiçi ortamlarda vermek istememektedir (Staysafeonline, 2010).

İnternet bağlantısına sahip bilgisayarların güvenlik önlemlerinin yetersiz olması veya yetersiz kalması nedeniyle, gelebilecek başlıca dijital tehlikeleri casus yazılımlar,

bilgisayar virüsleri, solucanlar (spam), truva atları (trojenler), phishing (oltalama), botnetler olarak sıralanabilir (Bayzan, 2011: 41).

1.1.3.2.2.2 İnternette Mahremiyet Sorunu

Mahremiyet, uluslararası insan hakları hukukunda temel bir insan hakkı olarak açık bir şekilde tanınmış ve korunması gereken bir temel hak olarak belirtilmiştir. Evrensel İnsan Hakları Bildirgesi'nin 12. maddesi “Kimsenin özel yaşamına, ailesine konutuna ya da haberleşmesine keyfi olarak karışamaz, şeref ve adına saldırılamaz. Herkesin bu gibi karışma ve saldırılara karşı yasa tarafından korunmaya hakkı vardır.” demektedir (TBMM, 2011).

AIHS, "mahremiyet" kelimesini zikretmemekle birlikte “Özel ve aile hayatına saygı hakkı” başlığı altında konuyu düzenlemektedir. Buna göre “Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir” diyerek özel hayata, meskene ve haberleşmeye saygı hakkını deklare etmektedir. 2. kısmında ise bu hakkın kullanılmasına bir kamu makamının müdahalesinin, ancak yasayla belirlenme ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda söz konusu olabileceğini belirtmiştir (Anayasa, 2011).

Diğer yandan, İnternet'in insan hakları ile ilişkili olduğu üç spesifik alanın olduğu ifade edilmektedir; bilgi özgürlüğü, ifade özgürlüğü ve mahremiyet. Paradoksal bir şekilde İnternet'in kullanıcılarına sağladığı özgürlük aynı zamanda bu haklara yönelik tehdidin de sebebi olmuştur. İnternet'in suiistimal edilmesinden ise iki büyük tehdit doğmaktadır; ifade hürriyetine karşı hükümet sansürü ve mahremiyetin ihlali. Mahremiyetin ihlali ise iki şekilde ortaya çıkmaktadır; hükümet veya iş dünyasınca toplanan kişisel verilerin istismarı ve bireysel haberleşmeye izinsiz giriş (Foley, 1999: 35-41). Bu son cümledeki “hükümeti” hem yaşanan “ülkenin hükümeti” hem de “diğer ülkelerin hükümetleri”, aynı şekilde “iş dünyası” ifadesini de “tüm dünyada bu alanda iş yapanlar” olarak genişleterek anlamak daha doğru olacaktır.

Devletler, yukarıda belirtilen güvenlik riskleri ve tehditlerini gerekçe göstererek İnterneti özellikle kontrol altına almayı, kişilerin telefon ve İnternet iletişimini takip etmeyi, dinlemeyi ve izlemeyi istemektedir. İnternetin kontrol edilmesi ise, bu defa kişisel hakların ve mahremiyetlerin ihlali konusunun sorunlu hale gelmesi sonucunu doğurmaktadır. Geline bu nokta, bilgi toplumunun en önemli tartışma konularından birisi olan özgürlük / güvenlik paradoksu sorununu ortaya çıkarmaktadır.

Devlet güvenliğini koruma ile bireylerin mahremiyetini koruma arasındaki çatışma aslında yeni değildir, ancak gelişen teknoloji ve özellikle İnternet teknolojisi devlete bireyler hakkındaki özel bilgilere eskisinden daha çok ulaşma imkanı sağlamıştır. Bu yüzden bilgi toplumunda ulusal güvenliği korumak ile mahremiyetin korunması daha sık karşı karşıya gelmekte ve mahremiyet ihlalleri daha çok vuku bulmaktadır (Diffie & Landau, 1998: 125). Keza, İnternette yapılan her türlü iş ve işlemin elektronik iz bırakması ve kullanıcıların özel alanına giren haberleşme, bilgi, belge, doküman ve işlemlerin başkalarının ulaşılabilir ve denetlenebilir olmasından kaynaklanan mahremiyet ihlalleri giderek daha da önemli bir sorun haline gelmektedir.

Elektronik yazışma ve görüşmeler, arama motorlarında yaptığımız aramalar, okunan ve araştırılan haber ve konular, takip edilen bloglar, ilişki içinde olunan kişiler, bankacılık işlemleri vs. gibi her türlü mahrem bilgilerin başkalarının eline geçme ve kontrol edilme riski vardır. Zira, tüm bu iş ve işlemler elektronik bir iz bırakmakta ve birer kopyaları bağlı bulundukları hostinglerde saklanabilmektedir. Bu, aslında bilinmedik bir durum değildir, e-postalar, cep telefonuna gelen SMS’ler silindiğinde de, hizmet sağlayıcının arşivinde veriler olarak yerini almaktadır. Aksi takdirde, hakaret içeren e-postasını posta kutusundan silen faillerin bulunması, Youtube’a hukuka aykırı içerikler (video, fotoğraf vb.) yükleyen ve daha sonra bunları kaldıran kimselere erişilmesi mümkün olamazdı (Evcı, 2010).

Nitekim, Facebook ‘Gizlilik Politikası’ sayfasında, kişisel mesajlar dahil Facebook’a giren bilgilerin kullanıcı tarafından silinse dahi arşivlerde tutulduğu açıklanmakta ve bu bilgilerin, servisin takdimi için zorunlu olması, hukuken istenmesi ve kullanıcının izni olması halinde 3. kişilerle paylaşılacağı belirtilmektedir. Buna göre, verilen

bilgiler artık sitenin kullanımına geçmekte, istense de kayıtlardan silinmemekte ve belirtilen durumlarda 3. kişilerle paylaşılabilir (Facebook, 2010).²¹

Bu çerçevede, İnternetin doğum yeri, merkezi ve büyük oranda hakimi olan ABD'nin güvenlik gerekçesi ile istihbari amaçlı olarak kişilerin özel bilgilerine ulaşma konusunda ciddi çalışmalar yaptığı bilinmektedir. Hatta, İnternette hizmet veren, ana serverları ve hostingleri ABD'de bulunan ABD menşeli birçok büyük şirketin (Microsoft, Facebook gibi), ABD istihbarat örgütleri ile işbirliği içinde bulunduğu sıkça dile getirilmektedir. Facebook'un 'Gizlilik Politikası' sayfasında, "Facebook'u kullanmakla, kişisel verilerinizin ABD'ne transferi ile özel işleme tabi tutulmasına izin vermiş olursunuz" (Facebook, 2010)²² ifadesi de bu kuşkuyu güçlendirmekte, hatta, Facebook'un ABD gizli servislerinin eseri olduğu konusundaki düşüncenin çok da paranoyakça olmadığını göstermektedir (Evcı, 2010).

1.1.3.2.3 İnternetin Sebep Olduğu Toplumsal Sorunlar

İnternet, bireysel ve toplumsal hayata getirdiği birçok kolaylığın yanında, gerek bireyleri, gerek bireylerin oluşturduğu aile yapısını, gerekse çocuk ve gençleri olumsuz yönde etkileyecek özellikleri de içerisinde barındırmaktadır. Bu kapsamda, İnternetin aile ile çocuklar ve gençler üzerindeki etkileri yanında, bilgisayar ve İnternet bağımlılığı ile genç nüfus tarafından yoğun ilgi gören sosyal ağlar ve etkileri üzerinde durulması gereken konular arasında yer almaktadır.

1.1.3.2.3.1 İnternetin Aile Üzerindeki Olumsuz Etkileri

Bilişim devriminin toplumun temel taşı olan aile kurumu için önemli tehlike ve tehditler oluşturduğu; aile düzenin bozulması yönünde negatif bir etkisinin olduğu

²¹ Söz konusu bilgilerin benzer şekilde Microsoft tarafından da kaydedildiği ve paylaşıldığına ilişkin olarak bkz. Füsun S.Nebil, "İnternet'teki İletişim Takip Edilebiliyor mu? Nasıl ?", 05.02.2009, <http://www.turk.internet.com/portal/yazi yaz.php?yaziid=23072>

²² Facebook'un sahibi Zuckerberg'in "Kişisel mahremiyet duygusunun artık sona ermekte olduğunu ve kişisel mahremiyetin artık bir sosyal norm olmaktan çıktığını" iddia etmesi ilginçtir (Haber7, 01.12.2010).

sıkça dile getirilmektedir (Laudon & Laudon, 1996: 160). Bu olumsuzluklar bütün olarak aileyi etkilediği gibi, ayrı ayrı çocukları veya eşleri de tesiri altına almaktadır.

İnternetin aile üzerindeki olumsuz etkileri, aşırı kullanımı durumunda aile içi ilişkilere ve iletişime vermiş olduğu zarar, eşler arasında “aldatma”yı kolaylaştırması ve boşanmaların artmasına neden olması ve barındırdığı zararlı ve sakıncalı içeriklerin genel olarak tüm aile bireylerini olumsuz yönde etkilemesi şeklinde üç noktada değerlendirilebilir.

İlk olarak, İnternetin aile içi iletişimi olumsuz yönde etkilemesiyle bazı sorunlara neden olduğu görülmektedir. Aileyi güçlü kılan ve ortaya çıkan sorunları çözmede avantajlı kılan, aile bireyleri arasındaki yakın ve sıcak ilişkiler ile yardımlaşma ve dayanışma ortamı oluşturmaktadır. Aile fertlerinin İnternet kullanım sürelerinin artması, ailenin birbirleri ile geçirdikleri zamanın azalmasına ve aile çevresinden uzaklaşmaya neden olduğu gibi yüz yüze iletişime de engel olmaktadır.

Günümüzde İnternet, anne ve babaların olduğu gibi çocukların da her birinin dünyaya açılan ayrı bir penceresi olmuştur. İnternet, neredeyse anne, baba ve çocuklardan oluşan çekirdek ailenin tanımını değiştirmiş ve ailenin vazgeçilmez yeni bir ferdi olarak aileye katılmıştır. Bu nedenle artık İnternet için “ailemizin ve evimizin afacan çocuğu” (Alan, 2012: 2), evlere de “online hane” (Bensghir ve Altınok, 2005: 4) denilmektedir.

Nitekim, yapılan çalışmalarda, İnternet kullanımının artışı ile aile ilişkilerinde bozulma ve sosyal çevrenin azalması arasında bir ilişki bulunmuştur. Araştırmacılar özellikle ergenlerde olmak üzere İnternetin uzun süreli olmayan kullanımlarının bile, yalnızlık ve depresyonu arttırdığını saptamışlardır (Kraut vd., 1998: 1017-31).

Southern California Üniversitesi'nde yapılan çalışmada, 2 bin kişilik bir grubu inceleyen araştırmacılar, 2000 yılıyla karşılaştırdıklarında, 2008 yılında insanların aileleriyle daha az vakit geçirdiğini tespit etmişlerdir. İnternet kaynaklı olarak aileleriyle daha az vakit geçirenlerin oranının 2000 yılından 2008 yılına kadar 3 kat arttığı gözlenmiştir. İnternet ile geçirilen zaman nedeniyle aile fertleri arasında gün

geçtikçe daha fazla kopukluk yaşandığı görülmektedir. Araştırma, maddi olanakları daha iyi olan ve İnternet kullanımını zenginleştiren donanımlara daha fazla sahip olan ailelerde aile içi ilişkilerin daha az maddi olanağı olan ailelere göre daha kötü olduğunu göstermiştir. Özellikle kadınlar, İnternet kullanan aile fertleri tarafından ihmal edildiklerini hissettiklerini belirtmişlerdir (Center for the Digital Future, 2008).

Bazı durumlarda ise, özellikle aile içi iletişim kurmayı başaramayan bireylerin kendilerini sanal ortamda ifade etmeleri ve arkadaşlık kurmaları daha kolay olmaktadır. Bu iletişim çoğu zaman duygusal bir bağa ve daha sonra da bağımlılığa dönüşmektedir. Aynı evi paylaşan bireyler birbirleri ile konuşamayacak, hatta yan yana gelemeyecek bir duruma gelmektedirler.²³

İkinci olarak, İnternetin neden olduğu, aile bütünlüğünü tehdit eden ve boşanmaların ortaya çıkmasına sebep olan yaygın sosyal sorunların bir diğeri ‘aldatma’ olgusudur. İnternetteki sohbet siteleri ve anlık görüntülü yazışmalar eşler açısından birçok olumsuz sonuçların ortaya çıkmasına zemin hazırlamaktadır. Eşyle yüzeysel tartışmalar yapıp problem yaşayan birçok kadın ve erkek, İnternet üzerinden tanıştıkları kişilerle bu mecralarda problemlerini paylaşmaktadır. Bu paylaşımlar karşı cinsleri birbirlerine yakınlştırarak yeni bir ilişkiye ortam hazırlamakta ve “aldatma” olarak ifade edilen bir başka soruna kaynaklık etmektedir. Aldatma ise çoğu zaman aile kurumunun yıkılmasına neden olmaktadır (Turan, 2008: 23-24, 67-68). Aldatma kadın ve erkek açısından farklılıklar gösterebilmektedir. Erkeklerde cinsel aldatma ağırlıklı davranışlar görülürken, kadınlarda duygusal aldatma ön plana çıkmaktadır (Hürriyet, 25.12.2009).²⁴

²³ Nitekim, Pennsylvania Üniversitesi mezuniyet töreninde konuşan Google'un CEO'su Eric Schmidt, teknolojinin gelişimi ve İnternet nedeniyle insan ilişkilerinin her geçen gün sekteye uğradığını söyleyerek, “Dijital yaşamı bir kenara bırakın biraz analog yaşayın. Sanal dünyadan uzaklaşıp gerçek insan ilişkilerine yönelin. Bilgisayarlarınızı kapatın insan olun” demiştir (Huffingtonpost, 2009).

²⁴ Kiliselerdeki günah çıkarma kulübelerinde papazlara yapılan itiraflardaki verilerden yola çıkarak yapılan bir araştırma erkeklerin işlediği günahlarda liste başında şehvet düşkünlüğünün, kadınlarda ise kibrin yer aldığını ortaya koymuştur. Kadın ve erkeklere ait bu özelliklerin İnternet ortamında da kendini yansıttığı; erkeklerin sanal muhabbette konuyu hızla cinselliğe getirirken, kadınların kendilerini övmekten veya övülmeğe hoşlandıkları görülmüştür.(Gazetavatan, 21.02.2009).

Sosyal paylaşım sitelerinin artması ve büyük bir kitle tarafından kullanılıyor olması boşanma davaları üzerinde önemli rol oynamaktadır. Bu tür sosyal paylaşım sitelerinin ikili ilişkilerde kıskançlık, güvensizlik, aldatma ve yeni cinsel arayışlara kapı araladığı görülmektedir (Özsoy, 2010: 7-77). Kanada’lı bilim adamlarının yaptıkları 17-24 yaş aralığındaki erkek ve kadınların katıldığı bir araştırmaya göre, özellikle sosyal paylaşım siteleri yoluyla gençler eşlerini veya birliktelik yaşadığı kişileri İnternette izleme eğilimi göstermektedir. Araştırmada bu durumun süreklilik arz ettiği, zamanla alışkanlığa dönüştüğü ve böylece daha fazla kıskançlık oluşturabilecek bilgi ve görsel malzemeye ulaşıldığı görülmüştür(Haber7,13.8.2009).

Bir araştırmada, 2009 yılında hazırlanan her beş boşanma dilekçesinden birinde Facebook adının geçtiği belirlenmiştir (Çehrelî, 22.12.2009). Eski arkadaşları buluşturan ve yenilerini bulmaya yarayan sitenin evlilikteki sorunları artırdığını belirten uzmanlar, eşlerin birbirlerini Facebook'ta kaçamak yapmakla veya Facebook'a dalıp birbirlerini unutmakla suçladıklarını dile getirmektedir (Zaman, 23.12.2009).

Üçüncü olarak, İnternet aile fertlerinin birbirleriyle ilişkilerini, istenmeyen içeriklerle muhatap olma açısından da olumsuz yönde etkilemektedir. Bu çerçevede İnternette karşılaşılan zararlı içerikler aile için tehlike oluşturmaktadır. Özellikle pornografik içerik tüm toplumun ahlaki temellerini derinden sarstığı gibi, toplumun temel taşı olan aile kurumu için de önemli bir tehdit haline gelmiştir (Eberstadt, 2010).

Dünyada pornografi içerikli sitelerin oldukça fazla olması, arama motorlarında pornografik site arama sıklığının fazlalığı, İnternetin bireyleri yeni cinsel arayışlara ittiğini göstermektedir. Pornografik olguyu izleyen erkekler eşlerini daha az heyecan verici bulmakta ve gördükleri içeriklerin aynısını eşlerinden beklemektedirler. Bu durum aile içi huzursuzlukların artmasına, evliliklerin riske girmesine ve boşanmalara neden olmaktadır (Weeks, 2010).

Araştırmalar, İnternet pornografisinin artan boşanma davalarının sebeplerinden birisi olduğunu göstermektedir. 2003 yılında, ABD’de boşanma avukatı ve savcılarıyla

yapılan bir ankette, katılımcıların %62'si İnternetin boşanmalarda etkili olduğunu ve boşanma vakalarının %56'sının eşlerden birinin pornografik İnternet sitelerine olan takıntılı ilgisinden kaynaklandığını belirtmişlerdir (Paul, 2004).

Pornografinin erkeklere zarar verdiği, bu zarar nedeniyle erkeklerin de kadınlara zarar verdiği dile getirilmektedir. Şöyle ki; pornografi erkeklerin kadın üzerinde kurmayı tahayyül ettikleri iktidar ve tahakküm arzusunu sömürmekte, zevk kölesi, hizmetçi, kurban rolünden hoşlanan kadın prototipleri ortaya koyarak, gerçek hayat ve kadın gerçeği hakkında yanlış bir algıya kapılmalarına sebebiyet vermektedir. Pornografi kadınların kendilerine kötü davranılmasından, şiddetten, tecavüze uğramaktan, aşağılanmaktan aslında gizliden gizliye "memnun olduklarına" dair hastalıklı düşünceler uyandırmaktadır (Karaca, 2010).

Nitekim, pornografik filmlerin %88'inin kadına şiddet içerdiğini belirten Prof. Dines, pornografi sektördeki ve izleyicilerdeki yükselme trendini bir "sağlık problemi" olarak nitelendirmekte ve günümüzde erkeklerin vahşi bir porno kültürü üzerine yetişmekte olduğuna dikkat çekmektedir. Yaptığı araştırmalar, pornografik görüntü ve resimlerin yeni neslin cinselliğini ve kadınlara karşı tutumunu çok ciddi bir şekilde etkilendiğini, pornografinin bu denli hakimiyet sağlamasının erkeğin duyarsızlaşmasına sebep olduğunu; bu nedenle de erkeklerin daha sert, daha korkunç ve kadının onurunu daha çok kırıcı görüntüler aramaya başladığını göstermektedir. Öyle ki, erkeklerin bu denli acımasız görüntülere olan ilgisi pornografi endüstrisini dahi şaşırtmaktadır. Dines, bu görüntüleri izleme yaşının 11'e kadar düştüğünü ve erkeklerin ne kadar erken pornografiyle tanışırsa, gerçek hayatta kadınlarla ilişkilerinde o kadar çok problem yaşadıklarını belirtmektedir (Guardian, 2.7.2010).

Gail Dines'e göre; "Eğer siyah ırktan olanlar veya Yahudiler, filmlerle, kitle halinde (o filmlerdeki kadınlar gibi) bu derece aşağılansalardı, bu filmlere itiraz ve protesto da çok büyük olurdu. Kimse de bu filmlerin, 'fantazi' olduğundan falan bahsetmezdi. Tam tersine, bunun ne olduğunu açıkça söylerdi, yani: Irkçılık ve Yahudi düşmanlığı". Burada "anlaşılamaz" görünen, ABD gibi insan haklarının mucidi bir ülkede kadının nasıl olup da bu derece aşağılanabilmesidir (Caydı, 2010).

Kadın-erkek ilişkilerinde duygulara hiç yer vermeyen pornonun kadın doğasına yabancı olduğu üzerinde ısrarla duran kadın aktivistler, pornoya karşı yürüttükleri mücadeleyle, aslında erkeklerin ruhunu kurtarmaya çalıştıklarını söylüyorlar. Çünkü pornonun asıl büyük ruhsal zararı erkeklere verdiği görülmektedir. Hayatın en mahrem alanlarının bile bu derece ticari mal/meta haline getirilmesi, en başta insan mutluluğunun temel faktörleri olan sevgi ve aşka karşı büyük bir saldırı anlamı taşımaktadır. Yeni porno, kadınları tarihte hiç olmadığı ölçüde aşağılamakta, cinselliği, sevgisiz ve aşksız bir şiddet pratiğine indirgemektedir (Caydı, 2010).

Pornografi kültürünün sadece erkekleri değil, kadınları da etkilediğini belirten Denis, pornografinin kadının, kendi vücuduna, cinselliğine ve ilişkilerine bakışını da değiştirdiğini, pornografik resimlerin yaygın kültüre girmesi oranında kadınlar ve kızların insani statülerinden uzaklaşarak, seks objesi haline dönüştüklerini; bu durumun, kızların cinsel kimlikleri üzerinde ciddi tahribatlar oluşturduğunu ifade etmektedir (Caydı, 2010). Yani, “porno satıyor, ama maliyeti ölçülemeyecek kadar yüksek. En yüksek bedeli de maalesef kadınlar ödüyor” (Stoner,2010; Henes, 2011).

Öte yandan, pornografi bağımlılığının hastalık olarak mütalaa edildiği bilinmektedir. Kronik bağımlılık, depresyon ve mutsuzluğu da beraberinde getirmektedir. Bağımlı olan kişiler istemedikleri halde pornografik sitelere girmekten kendilerini alamamaktadır. Bu durum, bağımlı kişinin normal bir ilişkiden korkmasına ve gerçek mutluluk sebebi olan aşkın ölmesine yol açmaktadır (Eberstadt, 2010).

Nitekim, bazı batılı ülkelerde de pornografinin kadınlara yönelik cinsel şiddeti artırdığı ve çocuklara zarar verdiği için bu tür görüntülerin İnternette indirilmesinin yasaklanması konusu tartışılmaktadır. En son İzlanda’da yetişkinlerin kredi kartlarıyla porno sitelerden görüntü indirmelerine engel olmak da dahil, İnternete bağlı cihazlar aracılığıyla pornografik içeriklere ulaşmanın önüne geçecek filtrelemeye ilişkin tedbirlerin yer aldığı bir yasa taslağı parlamontaya sunulmuştur. Taslağı hazırlayan İçişleri Bakanı Jonasson, İnternet pornosunun kadınlara karşı cinsel şiddeti artırdığını ve erken yaşta erotik videoları izlemeye başlayan çocuklarda uzun süreli bozukluklara yol açtığını savunmaktadır (Ahaber, 2013).

1.1.3.2.3.2 İnternetin Çocuklar Ve Gençler Üzerindeki Olumsuz Etkileri

Günümüzde çocuklar ve gençler, bilgisayar ve İnternet'in etkileşim ve iletişim isteyen kısımlarında en çok yer alan aktörlerdir. Bu açıdan bakıldığında toplumun bu kesimleri, teknolojiyi iyi kullanan ve onu ileriye taşıyacak etkenlerin başında gelmektedir. Bu çerçevede, bir sosyalleşme, eğlence, kendilerine yeni alanlar oluşturma aracı olarak İnternet, en çok çocuklar ve gençler tarafından ilgiyle karşılanmakta ve yoğun olarak kullanılmaktadır. Bu nedenle çocuklar ve gençler İnternet kaynaklı risk ve tehlikelerin de en çok tehdit ettiği toplumsal kesimdir.

Bu risklerin bir kısmı güvenlikle ilgili ve teknik boyutludur. Örneğin, indirdikleri bir oyun programında virüs, casus yazılım gibi kötücül yazılımlar bilgisayara bulaşabilir ve bunlar çok çeşitli tekniklerle bilgisayara ve kullanıcılarına zarar verebilir. Ya da kendisine veya ailesine ait kimlik, adres, kredi kartı vb. özel bilgileri paylaşarak İnternet dolandırıcılarına malzeme verebilir (Canbek ve Sağıroğlu, 2007a).

İnternet ortamının çocuklar ve gençlere verebilecekleri zararların diğer önemli bir kısmı ise fiziksel, sosyal ve psikolojik boyutludur. Bu kapsamda çocuklar ve gençler İnternet ortamında pornografi ve cinsel istismarla, şiddet, vahşet, siber zorbalık ve ırkçılık içerikleriyle karşılaşabilmekte, sosyal ağlar, dijital oyunlar ve bağımlılıkla ilgili sorunlar yaşayabilmektedir.

1.1.3.2.3.2.1 Cinsel İstismar ve Pornografi Sorunu

İnternetin çocuklar ve gençler üzerindeki olumsuzluklarının başında çocukların pornografik görüntülere maruz kalması ve cinsel istismarı gelmektedir. İnternette pornografik yayınların sınırsız olması, kolay erişilebilmesi ve denetimin zor olması gibi nedenlerle erken yaşlarda pornografik görüntülere ve cinsel istismara maruz kalan çocukların, seks objesi haline gelmesi duygusal ve cinsel gelişimlerini olumsuz yönde etkilemekte ve telafisi zor travmalar oluşturmaktadır.

Uzmanlara göre pornografi, modern çağ çocuklarının karşılaştığı önemli bir problemdir (Eberstadt, 2010). Çocukların pornografi ile erken yaşta tanışması erken

uyarılmaya neden olmakta, dolayısıyla “erken ergenlik” başlamaktadır. Uzmanlar, özellikle genç kızların ergen olma yaşının 9’a kadar düşmesi ve ilk ilişki yaşının 14’e kadar gerilemesinde erken uyarılmanın etkisi olduğunu dile getirmektedir. Gördükleri karşısında korkup içine kapanan çocukların yanında merak edip müptela olanların da bulunduğunu; cinselliği zamansız ve yanlış şekilde öğrenen çocukların eğer kontrol edilmezlerse ileriki yaşlarda daha farklı toplumsal sorunlara sebep olduklarını da ifade etmektedirler (Aksiyon, 2011).

Pornografi ile tanışan çocukların kısa sürede pornografi bağımlısı haline gelmeleri de mümkündür. Nitekim, Masters and Johnson Kliniği direktörü, 14-15 yaşlarında İnternet pornografisi bağımlısı çocuklar gördüğünü söylemektedir. Direktör, pornografi bağımlısı birçok erkek çocuğun tedavisiyle uğraştığını ve İnternette önce böyle bir şeyle hiç karşılaşmadığını dile getirmektedir (Eberstadt, 2010).

Çocuğa yönelik cinsel istismar “Psiko-sosyal gelişimini henüz tamamlamamış ve yaşı küçük olan bir çocuğun yetişkin tarafından cinsel uyarıcı olarak kullanılması” şeklinde tanımlanmakta ve sözel, dokunma, teşhircilik, röntgencilik, çocuğu pornografide veya fuhuşta kullanma veya bu görüntüleri izlemesini sağlama gibi farklı türlerinden bahsedilmektedir (Ahmet ve Çağlar Özkanlı, 2006: 117-133).

“Yetişkin bir kimsenin çocukları cinsel açıdan çekici bulması ve onlara cinsel eğilim duyması olarak” tanımlanan pedofili (paedophile) ise, çocukların İnternet’i özgürce kullanmaya başlamalarıyla yaygınlaşan ve artık ismini sıkça duyduğumuz psikoseksüel bir rahatsızlıktır. Pedofiller, İnternet vasıtasıyla kimliklerinin ortaya çıkması endişesi taşımadan sosyal ağlarda ya da oyun sitelerinde yaşlarını ve cinsiyetlerini değiştirerek çocukları kandırmakta ve onların masum ve temiz dünyalarında derin yaralar açmaktadırlar (Uzunay ve Koçak, 2005: 108).

İnternette cinsel istismara uğramanın ise, diğer cinsel istismar tiplerinde olduğu gibi, travma sonrası stres bozukluğu, depresyon, cinselliğin reddedilmesi, gelişigüzel cinsel ilişkiye girme, cinsel kimlik sorunları, alkol ya da uyuşturucu bağımlılığı,

psikopatik eğilimler, tekrarlayan intihar girişimleri ve kendine zarar verici fiziksel davranışlar gibi kısa ve uzun vadeli sonuçları olabilmektedir (Alıkaşifoğlu, 2012).

Pedofil hastaları ve bunların İnternette oluşturdukları sosyal gruplar ve grupların üye sayıları sürekli ve hızlı bir biçimde artmaktadır. Bu grupların üyeleri elde ettikleri her türlü CSAM (Child Sexual Abuse Material-Çocukların Cinsel İstismarı Materyalleri)'ı kişisel hazları için tüm grup üyeleri ile paylaşmaktadırlar. Grup üyeleri yakalanmamak için bu tür içeriklerin dağıtımında en ileri teknolojiler ve kriptoloji kullanmaktadırlar. Bu durum söz konusu kişi ve grupların tespiti ve yakalanmasını son derece zorlaştırmaktadır (INHOPE, 2012b).

İnternet ortamında giderek büyüyen diğer bir sorun da “grooming”dir. Grooming, İnternette kendini çocuk olarak tanıtip cinsel haz amacıyla çocukları hedef alan yetişkinlerin bu hedefe ulaşmak için yaptıkları faaliyetlerine verilen genel bir addır. Pedofiller çevrimiçi ortamda kendini çocuk olarak tanıtip çocuklarla arkadaşlık kurmakta, uzun süre çocuğun güvenini kazanmaya çalışmakta ve bunu sağladıktan sonra da karşısındaki çocuğa yavaş yavaş yetişkin pornosu ve CSAM göndermeye başlamaktadır. Pedofiller bu şekilde hem çocuğun bu duruma tepkisini ve ilgisini anlamaya çalışmakta, hem de çocuğu bu içeriklere baktığı için suçluluk psikolojisine sokarak durumu ebeveynlerine ve öğretmenine anlatmasını ve korunmak için yardım almasını önlemeyi amaçlamaktadır. Pedofiller daha ileri aşamalarda, çocuğu gerçek hayatta buluşmaya, tanışmaya çağırmakta ve sonrasında çocuğu sapkın cinsel emellerine alet etmektedir. Bu süreçlerin çoğu ne yazık ki çocukların cinsel istismarı, tecavüze uğraması, kaçırılması ve hatta ölümü ile sonuçlanmaktadır. Keza, sohbet servisleri ve sosyal ağların yaygınlaşması tüm dünyada grooming olaylarının sayısında patlamaya neden olmuştur (INHOPE, 2012c).

Nitekim, Prof. Dr. Dines, çocuk istismarını içeren görüntülerin son yıllarda artış gösterdiğini, körpe kızların yaşlı erkeklerle ilişki halindeki görüntülerinin yer aldığı legal İnternet sitelerinin olduğunu belirterek, cezaevlerinde çocuk istismarcılarıyla yaptığı röportajlarda suçluların cevapları karşısında şoka girdiğini aktarıyor; “Her zamanki görüntülerden çok sıkılmıştık. Artık taze ve yeni şeyler arıyorduk. Ergenlik

çağına gelmemiş çocukları istismar düşüncesi bizi başta korkuttuysa da, 6 ay içinde her birimiz tecavüz suçuyla içeri girdik.” (Guardian, 02.07.2010).

İnternet güvenlik firması Symantec’in araştırmasında, 7-14 yaş arasındaki çocukların arama motorlarında aradığı anahtar sözcüklerden ilk üç sırayı YouTube, Google ve Facebook alırken, ardından “sex” ve “porno kelimelerinin geldiği tespit edilmiştir. Yine aynı araştırmada çocukların %80’inin porno ile ilk defa ödev için araştırma yaparken karşılaştığına değinilmektedir (Earlyinterventionteam, 2010). WASPA (Mobil Uygulama Hizmet Sağlayıcıları Derneği), tarafından yapılan araştırma, 8-16 yaşlar arası gençlerin %90’ına yakınının porno içerikler görüntülediklerini, kızların %22’si, erkeklerin ise %20’si kendilerinin çektiği, uygunsuz fotoğraflarını bir porno sitede bulduklarını ortaya koymuştur (Çehreli, 04.10.2011).

Internet Filter Software Review’ın 2006 yılı İnternet Pornografisi istatistiklerine göre, günde 116 bin arama ‘child pornography’ sözcükleriyle yapılmaktadır. İnternette ilk kez pornografiye maruz kalma yaşı ortalama 11’dir. Yaşları 8-16 arası çocukların %90’ı -çoğu ev ödevi yaparken- online pornografiye karşılaşmaktadır (Internet Filter Software Review, 2006).

Bitdefender Güvenlik Firması tarafından 2012’de dünya genelinde 19 bin ebevyin ile yapılan bir araştırmaya göre, çocukların 6 yaşından itibaren İnternette porno izlemeye ve 8 yaşından itibaren de İnternette flört etmeye başladığını ortaya koymuştur. Analize dahil çocukların %2’sinin sadece 5 yaşında iken İnternette arkadaşlarıyla sohbete ve anında mesajlaşmaya başladığı tespit edilmiştir (Bitdefender, 2011). Keza, ABD’de üniversite öğrencilerine yapılan bir araştırmada ise, erkeklerin %93’ünün ve kızların %62’sinin 18 yaşından önce İnternette pornografiye tanıştığı görülmüştür (Covenanteyes, 2013).

İngiltere’de yapılan bir araştırmada ise, İnternette gezinen çocukların %57’si çevrimiçi pornografiye rastladığını, %38’i başka bir şey yaparken önüne pornografik içerikli reklamın çıkıverdiğini, %36’sı başka bir şey ararken bir porno sitesine kazara girdiğini, %25’i ise pornografik mesaj sağınağına yakalandığını, %22’si şiddet ve

korku içeren bir siteye rastladığını, %9'u düşmanca ve nefret dolu bir siteyle karşılaştığını belirtmiştir (Canbek ve Sağıroğlu, 2007b: 35).

Başka bir araştırmada, pornografik sitelerin 2/3'ünde yetişkin içeriğe ilişkin herhangi bir ikaz bulunmadığı, diğerlerinin %75'inin ise yaş kontrollerinden önceki ana sayfalarında müstehcen görseller barındırdığı, sadece %3'ünün yaş kontrollerinden sonra bu tür materyallere ulaşılmasına izin verildiği görülmüştür. Öte yandan, ergenler arasında bir hayli popüler olan İnternet bağlantılı cep telefonlarında da bu tür içeriklere karşı etkin filtreleme sistemleri bulunmadığı tespit edilmiştir (Eberstadt, 2010). Keza, Kaiser Family Foundation 2002 raporunda ise, yaşları 15 ile 17 arası olan gençlerin %70'i pornografik içeriklerin onlar istemeden karşısına çıktığını ve bu gençlerin %23'ü de bu olayın sıklıkla tekrarlandığını belirtmişlerdir (Kff, 2002).

ITU'nin Çocukların Online Korunması (COP) İnisiyatifi'nin yayınladığı broşürde yer verdiği çeşitli araştırmaların özet sonuçlarına göre, İnternet kullanımının artışına paralel olarak İnternet üzerindeki tehlikeler de artmakta ve bunlardan olumsuz etkilenenlerinin başında çocuklar gibi korunmaya muhtaç gruplar gelmektedir. Broşürde yer verilen bazı araştırma sonuçları ise şöyledir (ITU Cop-brochure, 2009):

- Her yıl, İnternet kullanıcısı her 5 çocuktan 1'i İnternet saldırganlarının veya pedofili hastalarının tacizine uğramaktadır.
- ABD'de genç kızların %86'sı ailelerinin bilgisi dışında sanal sohbet odalarını kullanırken, bunların %30'u bu ortamlarda tacize uğramaktadır. Tacize uğrayanların sadece %7'si bu durumu ailelerine söylemektedir.
- Ailelerin %92'si çocukların İnternet kullanımı ile ilgili kurallar belirlediklerini söylerken çocukların %34'ü kural olmadığını belirtmektedir.
- Fransa'da, çocukların % 72'si yalnız başlarına İnternet sörfü yapmaktadır. Ailelerin %85'i ebeveyn kontrol yazılımlarından haberdar olmasına rağmen sadece % 30'u böyle bir programı çocuklarının bilgisayarına kurmuştur.
- İngiltere'de, yaşları 9 ile 19 arası kullanıcıların %57'si çevrimiçi pornografi gördüklerini, %46'sı vermemeleri gereken bilgileri başkalarına verdiklerini ve %33'ü çevrimiçi ortamlarda kandırıldığını belirtmektedir.

- Çin’de, çocukların %44’ü çevrimiçi ortamda yabancıların kendilerine yakınlık kurmaya çalıştıklarını söylerken %41’i yabancı biriyle cinsellik veya rahatsız edici başka bir konu hakkında konuştuklarını ifade etmektedir.

Norton Online Family Report’un 2009 yılında 14 ülkede gerçekleştirdiği araştırma sonuçları ise şöyledir (Güvenliweb, 2009):

- Dünya genelinde, çocuklar günde ortalama olarak 1,6 saatten fazla süreyi İnternet başında geçiriyorlar. Bu, haftada yaklaşık 11,4 saat etmektedir.
- Çocukların %41’i, İnternette tanımadıkları kişilerin kendilerini sosyal paylaşım sitelerine eklemek istediklerini, %33’ü bilgisayarına virüs bulaştığını, %25’i şiddet ya da müstehcen görüntülerle karşılaştıklarını, %10’u İnternette tanımadıkları birinin kendisiyle gerçek hayatta tanışmak istediğini söylemektedir.
- Çocukların 2/3’ü İnternet ortamında olumsuz bir deneyim yaşamış olmalarına rağmen, ailelerin sadece %45’i bunun farkındadır.
- Yetişkinlerin %44’ü, ailelerin çocukların İnternetteki faaliyetlerini tamamıyla kontrol etmeleri gerektiğini düşünüyor. Bu oran, Kanada ve Amerika’da %61’e yükselmektedir. Ailelerin %40’ı çocuklarının İnternet ortamında her zaman ne yaptıklarını, nerelere girdiklerini bildiklerini söylüyor. Ancak %52’si bunu her zaman değil bazen bildiklerini söylemektedir.
- Ailelerin %80’i, çocuklarının uygunsuz içerikle karşılaşabilecekleri konusunda endişe ediyorlar ve gereğinden fazla kişisel bilgilerini paylaşabileceklerinden korkuyorlar.

Yine, McAfee’nin 2010 yılında yaptırdığı bir araştırmaya göre, 10-17 arası yaş grubundaki gençlerin %69’u sosyal paylaşım sitelerinde anlık durumlarını paylaşırken lokasyon bilgisini de veriyorlar, %28’i gerçek hayatta tanımadığı kişilerle sohbet ediyor, %43’ü gerçek ismini paylaşıyor, %24’ü e-mail adresini paylaşıyor, %18’i gerçek fotoğrafını paylaşıyor, %12’si cep telefonu bilgisini paylaşıyor, %23’ü şifresiz kablolu ağları kullanarak İnternete bağlanıyor, %38’i ailesi odaya girdiğinde bulunduğu sayfayı kapatıyor, %32’si bilgisayarı kapatırken tarayıcının geçmiş sayfa bilgilerini temizliyor, %55’i İnternette ne yaptığını ailesinden saklıyor (McAfee,

2010). Yine İngiltere’de yapılan bir araştırmaya göre, 12-19 yaşları arasındaki ev İnternet kullanıcılarının %63’ü çevrimiçi ortamdaki faaliyetlerini ebeveynlerinden gizlemek için çeşitli yollara başvurmaktadır (Canbek ve Sağıroğlu, 2007b: 35).

1.1.3.2.3.2.2 Dijital Oyunlar Sorunu

Çocukların ve gençlerin İnternet kullanımında önemli yer tutan konulardan birisi de dijital oyunlardır. Eğitimciler oyunun, çocukların içgüdüsel ve eğitsel tecrübelerinin temelini oluşturduğunu ve bu tecrübelerin ileriki yaşlarda eylemlerine, alışkanlıklarına ve karakterlerinin oluşumuna tesir ettiğini belirtmektedir (Tezcan, 116-117). Dolayısıyla, çocuklar ve gençler arasında yaygın olarak kullanılan ve daha da yaygınlaşma eğilimi gösteren bu konunun üzerinde durulması gerekmektedir.

Dijital oyunların etkileşimli ve son derece eğlendirici bir formatta hazırlanmış olmaları günümüzde, dijital oyun oynama alışkanlığının her yaştan birey için gündelik hayatın bir parçası olmasında ve dünyada ekonomik açıdan hayli büyük yere sahip bir sektör haline gelmesinde etkili olmaktadır. Dijital oyunların eğlendirici olmasının dışında, onu geleneksel oyunlardan farklı kılan, bireyi cezbeden ve onu yaşamın vazgeçilmezi yapan birçok özelliği vardır. Bu nedenle, dijital oyunların insanlık tarihi boyunca en çok ilgilenilen eğlence ve boş zaman değerlendirme aracı olduğu ifade edilmektedir (Güneş, 2012: 15-18). Dijital oyunlar, yeni teknolojiler kullanılarak giderek daha da cazip hale getirilmektedir.²⁵

Dijital oyunların cazibesi, İnternet kullanımını da artırmaktadır. Araştırmalarda, İnternet kullanımının nedenleri arasında oyun oynamak daima ilk üç sebepten biri

²⁵ Bunların en önemlisi yapay zeka uygulamalarıdır. Yapay zekanın ana amacı insanların davranışlarının ve sezgisel yeteneklerinin bilgisayar üzerindeki benzetimidir. Nitekim, oyun firmalarının görsellik için harcadıkları çaba ve kaynağın önemli bir kısmı yapay zeka alanındaki çalışmalara kaymaktadır. Microsoft’un Natal projesi, yapay zekanın katılımı ile dijital oyunların gerçek hayata daha çok yaklaştığı yeni buluşları özetlemektedir. Bu projede kullanılan konsolda herhangi bir kontrol kumandası olmamasına karşın oyundaki karakterle gerçek bir insanla kurulabilecek her çeşit iletişim kurulabilmektedir (Xbox, 2010). Diğer bir yenilik olan “Multi User Virtual Environments” ise, ileriki dönemlerde İnternete yeni görünümünü kazandıracak olan çok kullanıcı sanal ortamın adıdır. Web’in bugün kullanılan iki boyutlu ara yüzünü üç boyutlu platforma aktararak Web 3D’yi yapılandırarak bu ortamlar, günümüzde çoğunlukla sosyalleşme ve çevrimiçi oyunlara sanal bir platform temin etmek amacıyla kullanılmaktadır. (Binark vd., 2009: 248).

olmakta ve çoğu kez %50'lik bir orana ulaşmaktadır (Özsoy, 2010: 20). NPD Group'un ABD bazlı araştırmasında düzenli olarak oyun oynayan genç sayısının genç nüfusun %82'sini oluşturduğu görülmüştür (NTVMSNBC, 04.12.2009). Avrupa'da her üç kişiden biri düzenli olarak, her iki çocuktan biri ise, her gün oyun oynamaktadır (ISFE, 2011). Keza, sosyal ağlar da İnternet ortamında oynanabilen oyunları desteklemekte ve pazarlamaktadır. Örneğin, Facebook kullanıcılarının 80%'i bu siteyi oyun oynamak için kullanılmaktadır (Dinç, 2012).

Bugün dijital oyun, "oyun" kelimesinin zihinde canlandığı basit ve eğlenceli olma durumundan farklı olarak, oldukça karmaşık ve ciddi bir kültürel-ekonomik ürün haline gelmiştir. Zira dijital oyun üretimi, tekno-kültürel ve kapitalist bir döngü içerisinde, teknoloji, kültür ve pazarlama unsurlarının kesiştiği bir noktadadır. Ürünün tüketici ile buluşturulmasında reklamların ve tanıtım kampanyalarının önemi büyüktür. Bu döngü dijital oyunlar sebebiyle hem teknolojik araçların gelişmesi hem de film endüstrisinin beslenmesi ile gerçekleşmektedir. Ayrıca, oyun karakterlerinin yer aldığı tişört, defter, kalem gibi bilumum sarf eşyalarının üretim, pazarlama ve satışı da bu döngünün içinde yer almaktadır (Binark ve Sütçü, 2008a: 49-71).

Günümüzde 1 milyarı geçen müşteri kapasitesi, krizlerden en az etkilenen ve katma değeri çok yüksek karakteri ile dijital oyun sektörü 2011'de 70 milyar dolarlık ciroyu aşarak, 30 yılda sinema sektörüne büyük fark atmıştır. Dijital oyun oynama yaşı 5-6'ya düşerken, piyasaya sürülen yeni ürünlerin satışında rekorlar kırılmaktadır.²⁶

Eğitimciler, kontrollü ve sınırlı düzeyde oynanan eğitici içerikli dijital oyunların çocuklar ve gençler üzerinde; eğlendirirken ödüllendirerek içgüdüsel olarak başarıma, ilerleme ve gelişme ihtiyaçlarını karşılaması, diğer oyuncularla kurulan iletişim sayesinde sosyalleşmesine yardımcı olması, el-göz koordinasyonunu, problem çözme ve çoklu görev becerilerini güçlendirmesi, kişisel gelişimleri, öğrenme durumları, eleştirel düşünceleri, yaratıcılıkları, kavramsal öğrenmeleri ve stratejik düşünme

²⁶ Örneğin, Xbox Kinect sadece 60 günde 8 milyon adet satarak Guinness Rekorlar kitabına en hızlı satılan elektronik ürün olarak girmiştir. Call of Duty adlı oyun 24 saatte 223 milyon Euro'luk satış yapmıştır. Angry Birds oyununu 450 milyondan fazla kişi indirmiştir. 250 Milyondan fazla kişi Zynga'nın FarmVille, CityVille gibi oyunları oynamaktadır. (Dinç, 2012)

kabiliyetini geliřtirmeleri gibi konularda birok olumlu etkiler meydana getirdiđini belirtmektedir(Tüzün, 2006; MEB-EĐİTEK, 2008). Bunun yanında aşırı, kontrolsüz, amacı dışında ve bilinsiz kullanılması durumunda dijital oyunların ocuklar ve gençlerde olumsuz etkiler meydana getirdiđi; bağımlılık oluřturması yanında, başka bir takım fiziksel ya da psiko-sosyal sağık sorunlarına neden olduđu görülmektedir.

Birok bilgisayar oyununda gösterilen kötü karakterler, ocukların ve gençlerin şahsiyetinin oluřmasında olumsuz rol oynamakta; verilen kuvvetli olmaya alıřma, başkalarının hayatını ve duygularını önemsememe, yařamak için yok etme, ahlaki deđerlerin horlanması, karřısındakine deđer vermeme, insanları kategorize etme gibi mesajlar ocukların ve gençlerin kiřiliđinin geliřmesine olumsuz tesir oluřturmaktadır. Keza, řiddet başta olmak üzere, savař, suç, soygun, gaddarlık gibi olguları normalleřtirerek, duyarsızlık, bencillik, açgözlölük, düşmanlık, hilekarlık gibi olumsuz davranıřlara yönlendirmektedir (Turan, 2008: 81-82).

Özellikle řiddet unsuru içeren oyunlar, bireyler ve özellikle ocukları olumsuz yönde etkilemektedir. ocukluk ve gençlik dönemlerinde řiddete karřı eđilimin ortaya ıkmasında ve saldırganlıđın artmasında oynanan oyun türü, sıklıđı ve süresinin etkili olduđu görülmektedir (Kelleci, 2008: 253-256). Uzmanlar, řiddet içerikli oyunların insan dođasında deđiřikliklere yol açtıđını; başka varlıkları öldürmeye karřı ıkan duyguları yok ettiđini, zamanla řiddete karřı duyarsızlařtırdıđını, řiddeti olađan bir hal gibi görmeye ve bir süre sonra ondan zevk almaya neden olduđunu ve řiddete eđilimli hale getirdiđini belirtmektedir (Boliřık ve Muslu, 2009: 448).

Nitekim, ABD’de, 1997 ve 2002 yılları arasında dijital oyunların içerdıđi řiddetin sebep olduđu düşünölen 16 olay tespit edilmiřtir. Bu olayların birođunda failler lise öđrencileri, kurbanlar ise öđrenci arkadaşları ya da tesadüfen yoldan geen vatandaşlar olmuřtur (Anderson, 2004: 113). Keza, Norve’te bir gençlik kampında katliam yapan aşırı sađ eđilimli Breivik’in mahkemede, rol yapma oyunu türündeki savař oyunları Call of Duty: Modern Warfare 2 ve World of Warcraft’tan etkilendiđini söylemesi, dijital oyunlar ve řiddet arasındaki iliřkiyi yeniden gündeme getirmiřtir (Telegraph, 2011).

ABD’li Ulusal Medya ve Aile Enstitüsü’nce, hazırlanan rapora göre; oyunların, çocukları bağımlı yapabilme ve daha saldırgan, saygısız ve hantal hale getirebilme ihtimali yüksektir (Çehreli, 18.07.2008).²⁷ Keza, araştırmalar, İnternet kullanımına bağlı olarak çocukların yetişkinlere göre daha fazla psikososyal sorunlarla karşı karşıya kaldıkları; İnternet ve dijital oyunlara ayırdıkları süre fazlaştıkça yalnızlık hissi, sosyal yalıtım, şiddete duyarsızlaşma ve saldırganlık gibi duygusal ve davranışsal problemlerin arttığı, fizyolojik sorunların yaşandığı ve depresif belirtiler görülme oranının yükseldiği tespit edilmiştir (ASAGEM, 2008: 36-45).

Yine, bir tür İnternet bağımlılığı olarak literatürde yer alan dijital oyun bağımlılığının sadece çocuklar ve gençler için geçerli olmadığı, fantezi içerikli konularla çekici hale getirilen dijital oyunların çocukları olduğu kadar yetişkinleri de cezbediği ve yetişkinler üzerinde de bağımlılık oluşturduğu bilinmektedir.²⁸

Kısaca, aşırı ve kontrolsüz oynanan dijital oyunlar sonucu özellikle okul çağındaki çocuklar, sağlık problemleri, aile ilişkilerinde aksama, derslerde verim azalması ve başarısızlık, bağımlılık, şiddet eğilimleri, psikolojik ve bedensel problemler (el bileği sendromu, boyun kaslarında tutulma, sırt fizyolojisinde bozulma, uyku saatlerinin azalması, gözlerde çeşitli rahatsızlıklar), asosyallik gibi yaşamlarını negatif yönde etkileyebilecek birçok sorunla karşı karşıya kalabilmekte ve bu durum onların hem akademik hem de kişisel gelişimlerinde olumsuz etkilemektedir. (Selçuk, 2011, 34).

Oyun sektöründeki hızlı büyüme ile birçok firmanın bu sektöre yönelme isteği oyunların içeriğinin denetlenmesi, endüstrinin kontrol mekanizmalarının oluşturulması ve tüketicilerin satın aldığı oyunlarla ilgili bilgilendirilmesi ihtiyacını

²⁷ Nitekim, 1998 yılında üç serilik bir oyunun ilki olarak piyasaya çıkan ve sayısız ödül kazanan rol yapma oyunu Baldur's Gate'in başlangıç sahnesinde beliren Nietzsche'nin şu vecizesi oldukça dikkat çekicidir: "Canavarlar ile savaşanlar, kendilerinin canavara dönüşmemesi konusunda dikkat etmelidir. Cehennem'e uzun bir süre bakarsanız, cehennem de size bakar" (Güneş, 2012: 38-39)

²⁸ Bu bağımlılığın kimi zaman trajik sonuçlar doğurduğuna dair haberler zaman zaman medyaya yansımaktadır. Güney Kore'de 28 yaşındaki bir gencin bir İnternet kafede 50 saat boyunca durmaksızın oyun oynaması ve sonrasında vefat etmesi, Almanya'da World Of Warcraft adlı bilgisayar oyununun müptelası olan 27 yaşındaki bir annenin üç bebeğini doğar doğmaz 'oyun yüzünden onlara zaman ayıramayacağı' gerekçesiyle öldürmesine dair haberler bunlardan bazılarıdır. (Edubilim, 2011; Stargazete, 2011)

doğurmuştur. Dolayısıyla dünyanın çeşitli ülkelerinde oyunları derecelendirme kuruluşları oluşturulmuştur. Derecelendirme çalışmalarında amaç, uygunsuz oyun içeriğine karşı daha iyi koruma sağlamak ve ailelerin risk ve tehlikeleri anlamalarına yardımcı olmaktır. Derecelendirmeler, oyunun hangi yaşa uygun olduğunu gösteren yaş sınıflandırması ve içeriğin unsurlarını gösteren içerik açıklaması şeklinde yapılmaktadır. Sınıflandırma sembolleri ve içerik açıklayıcılar satılan ürünün içinde yer aldığı kutunun üzerinde bulunmaktadır. Her ülke kendi ahlaki, kültürel ve sosyal yapısına göre oyunları değerlendirme ve derecelendirme çalışmaları yapmaktadır.

Dijital oyunların hem reel hem de sanal ekonomiyi beslemesi, bu sektörün, oyunun yazılım aşamasından pazarlamasına kadar birçok yan endüstri ile ilişki içerisinde bulunması, mali anlamda genişleyen bir pazar olma özeliği oyun dünyasının ticari cazibesini artırırken, bunun yanında, mali denetimden yoksun bırakılan bu kaynak, art niyetli kişilerin de tercih ettikleri bir seçenek haline gelmiştir. Dolayısıyla, Dünya’da dijital oyun düzenlemesi konusunda geniş coğrafyaya hitap eden düzenleyici kuruluşların bu devasa endüstrinin etkisi altında etkin bir koruma geliştiremediği eleştirisi yapılmaktadır (Güneş, 2012: 4).

1.1.3.2.3.2.3 Siber Zorbalık Sorunu

Son zamanlarda İnternet’in yaygınlaşması ve gençler tarafından daha sık kullanılmaya başlanması ile öğrenciler okullarda uyguladıkları zorbalık davranışlarını sanal ortama taşımaya başlamışlardır. Bu şekilde, okullarda öğrenciler arasında yaşanan zorbalık türleri arasına sanal zorbalık (cyber bullying) adı verilen yeni bir zorbalık türü de eklenmiştir (Ayas ve Horzum, 2010).

Sanal zorbalık, bir veya daha fazla kişinin İnterneti kullanarak kasıtlı ve sürekli olarak bir ya da birden fazla kişiye zarar verme eylemlerinde bulunmasıdır (Bilsey, 2007: 14). Sanal zorbalık, bilgi ve iletişim teknolojilerini kullanarak kişileri sürekli rahatsız etme, kişilerle alay etme, hakaret etme, isim takma, tehdit etme, korkutma, dedikodu yayma ya da kişinin rızası olmadan fotoğraflarını yayınlama gibi ilişkisel saldırı davranışlarını içermektedir (Ergene, 2012).

Çocuklar sanal zorbalığa genel olarak elektronik posta, sohbet ortamları, sosyal ağlar ya da cep telefonları aracılığı ile maruz kalmaktadır. Siber zorbalığa maruz kalan çocuklarda, derslerde başarısızlık, disiplini bozma, okula gitmekte isteksizlik, arkadaşlarıyla görüşmek istememek, bilgisayar/cep telefonunu kullanmada tereddüt etmek, depresif ruh hali, öfke/kızgınlık, çocuğun kendisine olan saygısını yitirmesi, başkalarının gözünde saygınlığını kaybetme, diğer insanlarla ve ailesiyle ilişkilerinde bozulma gibi fiziksel ve duygusal durumların görülebildiği belirlenmiştir (Erdur-Baker ve Kavşut, 2007: 31-42; Ergene, 2012).

Aile içinde yaşanan sorunlar, düşük öz-saygı ve güvensizlik, okulda başarısızlık, başarıyı bu şekilde yakalama arzusu, kendini arkadaşlarına ispat etmeye çalışma, popüler olma isteği, başkaları tarafından benzer davranışlara maruz kalma veya kişinin ruh sağlığında sorunlar olması gibi nedenlerle çocukların ve gençlerin siber zorbalık davranışlarında bulundukları dile getirilmektedir (Ergene, 2012).

Siber zorbalık, yakın zamanda birçok ülke gibi, ABD ve Kanada'da eğitim bilimciler ve psikologlar başta olmak üzere pek çok uzman tarafından araştırılan ve önem verilen bir konu haline gelmiştir (Arıca, 2009: 167). Dünya genelinde siber zorbalığa ilişkin yapılan araştırmalar, siber zorbalığın okullarda sıkça karşılaşılan ve çocukların en çok etkilendikleri ve üzüldükleri bir tehdit unsuru haline geldiğini göstermektedir (LSE, 2009). Nitekim, Kanada'da yapılan bir çalışmada, çocukların %27,3'ünün e-posta yoluyla, %36,4'ünün ise iletişim ortamlarında siber zorbalıkla karşılaştığı tespit edilmiştir (Ayas ve Horzum, 2010). The National Crime Prevention Council'in bir çalışmasında, gençlerin %43'ünün siber zorbalık kurbanı olduğu (Ayas ve Horzum, 2010); ABD'de yapılan bir çalışmada, sanal zorbalık olaylarının devlet okullarında %54, özel okullarda %34, sınavla alınan özel okullarda ise %12 oranında gerçekleştiği tespit edilmiştir (Ayas ve Horzum, 2012).

1.1.3.2.3.3 İnternet Bağımlılığı

İnternetin getirdiği diğer bir olumsuzluk ise, "İnternet bağımlılığı"dır. İnternet bağımlılığı genel olarak İnternetin aşırı kullanılması isteğinin önüne geçilememesi,

İnternete bağılı olmadan geçirilen zamanın önemini yitirmesi, yoksun kalındığında aşırı sinirlilik hali ve saldırganlık olması ve kişinin iş, sosyal ve ailevi hayatının giderek bozulması olarak tanımlanabilir (Young, 2004: 402-441).

Kumar, seks, alışveriş, televizyon izleme, yemek yeme gibi kimyasal olmayan davranışsal/eylemsel bağımlılıklar da tıpkı alkol-madde bağımlılıklarında olduğu gibi bağımlılığın ana bileşenleri olan fiziksel ve psikolojik bağımlılık belirtilerini (zihinsel meşguliyet, duygu durum değişkenliği, tolerans, yoksunluk, kişilerarası çatışma ve tekrarlama) gösterebilmektedir (Dinç, 2010: 7-8). Dolayısıyla, zevk, haz, risk, macera ve uzaklaşma duygularını kamçılayan birçok madde gibi İnternet de bağımlılık yapabilmektedir (Odabaşı ve vd., 2007: 82). Bağımlının hayatında sanal dünya ile gerçek dünya arasında sürekli olarak bir çatışma vardır ve genelde kazanan sanal dünya olmaktadır (AREM, 2008: 231).

1997’de psikiyatr Ivan Goldberg, bu bozukluğu dile getirdiğinde, rahatsızlığın bu derece ilerleyeceği tahmin edilememiştir (Egger and Rauterberg, 1996). Nitekim, İnternet bağımlılığı için yataklı ilk klinik 2006 yılında Pekin’de açılmıştır. ABD, Çin, Güney Kore, Tayvan İnternet bağımlılığını ulusal bir problem olarak tanımlamışlardır. Şu an sadece Güney Kore’de 140’ın üzerinde İnternet bağımlılığı tedavi kliniği hizmet vermektedir (Şenormancı, 2012).

İnternet bağımlılığı için bir takım kriterlerden söz edilmektedir. Bazı uzmanlar, çocuk ve gençlerin günde en az 4 saatini İnternette geçiriyor olması ya da sosyal çevre içinde (kendi akraba ve arkadaşlarının yanında) 4 saat iletişimsiz kalabiliyor olmalarını “bağımlı” kişiler olduklarının ölçüsü saymaktadır (Aksiyon, 2009).

ABD’de İnternet bağımlılığını tedavi amacıyla kurulan ilk kurumlardan olan ReSTART adlı merkezin yöneticisi olan Hilarie Cash’a göre, eğer bir birey 12 ay boyunca aşağıdaki belirtilerin 5 veya daha fazlasını gösteriyor ise bu kişide İnternet bağımlılığı olduğu düşünülmelidir (Haber7, 09.07.2009):

- İnternete bağılı değilken bile zihnin İnternetle meşgul olması
- Tatmine ulaşılması için giderek artan bir şekilde İnternet kullanımı

- İnternet kullanımını kontrol edememe
- İnternet kullanımını kesmeye veya harcadığı zamanı düşürmeye çalıştığında kişinin kendisini huzursuz hissetmesi ve daha çabuk sinirlenmesi
- İnternet kullanımını gerçek hayat problemlerinden bir kaçış gibi görmesi
- İnternette daha fazla zaman geçirmek için çevresine yalan söylemesi
- İnternet kullanımı yüzünden eğitim, iş veya kariyer fırsatlarını riske atması
- İnternet erişimine harcanan yüksek ücretlere rağmen kullanımı sürdürmesi
- İnternete bağlı olmadığı zamanlarda kişinin sosyal yaşamdan geri çekilmesi veya içine kapanması
- İnterneti ilk kullanmaya başladığı zaman ile karşılaştırıldığında şu anki kullanım süresinin uzaması

İnternet bağımlılığının ortaya çıkmasında etkili olduğu düşünülen alanlar ise cinsellik, flört, muhabbet, kumar, pornografi, sohbet, borsada oynamak, açık artırmalara katılmak, oyunlar ve saplantılı bir şekilde yeni bilgiler peşinde koşmak şeklinde sıralanmaktadır (Ekici, 2002: 161). Beş tür İnternet bağımlılığından bahsedilmektedir (Gönül. 2002: 105-110; Ocak, 2012: 29):

1) *Siberseks Bağımlılığı*: Pornografik sitelerin aşırı kullanımı olarak ifade edilmektedir. Kişilerin İnternet aracılığıyla pornografik film, hikaye, resim vb. materyallere bağımlı hale gelmesini anlatmaktadır. Yetişkin İnternet pornografisi, çocuk pornografisi, yetişkin içerikli sohbet odaları, gerçek hayattaki ilişkileri direk olarak etkileyen yetişkin fantezi rol oynama siteleri bu kategoriye girmektedir.

2) *Siber-ilişki Bağımlılığı*: Kişinin gerçek veya takma adlarla sürekli sosyal paylaşım sitelerini kullanması, çok sık çevrimiçi sohbetlere ve sohbet odalarına katılması olarak tanımlanmaktadır.

3) *Net Bağımlılığı*: Aşırı çevrimiçi kumar, bahis, şans oyunları, alışveriş, İnternet üzerinden yapılan hisse senedi alım ve satımı ve açık artırma düşkünlüğüdür.

4) *Bilgi Bağımlılığı*: Gerçek hayatta daha az sosyal etkileşime yol açan ve iş üretimini etkileyen İnternet gezinmeleri, İnternette durmaksızın veri tabanlarına girme, bilgi stoklama olarak ifade edilmektedir. Bu durum, kişinin ulaşmayı

hedeflediği bilgiden uzaklaşarak, dikkat dağınıklığına ve gereksiz bilgiye boğulmasına neden olabilmektedir.

5) *Bilgisayar ve İnternet Oyunu Bağımlılığı*: Bilgisayar ve İnternet oyunlarına aşırı düşkünlüğü ifade etmektedir. Eğlence aracı olarak bilgisayar ve İnternet oyunlarının İnternet bağımlılığının oluşmasında ya da bağımlılığın gelişmesinde önemli bir neden olduğu belirtilmektedir. Oyunda başarılı olmak, bir sonraki bölüme geçmek ya da yarışı kazanabilmek kişide üstünlük duygusu oluşturmaktadır. Kişi bu durumdan haz almaya başlar oyun oynayarak mutlu olur, haz eşiği yükselir. Zevk alma ya da haz duyma, oyunun son özelliğidir (Kelleci, 2008: 253-256; Binark vd., 2009: 43). Bu özellik ile oyun bağımlılığı arasında yakın bir illiyet bağı bulunmaktadır. Zira bağımlılık, her ne şekilde olursa olsun beyinde ödül ve zevk mekanizmalarının aşırı aktif hale gelmesinden kaynaklanmaktadır (Bozarth, 1994). Bu durumun bir sakıncası, haz veya zevk duygusunun bir merkezde toplanması neticesinde, insanın başka bir şeyden zevk alamaz hale gelmesidir. Bu durum, mükafat-zevk sisteminin maksadı dışında kullanılması sebebiyle iflası olarak açıklanmaktadır. Bu noktada haz alma dürtüsü o kadar yükselir ki, bu doyumunu daha çok yaşamak için kişide sürekli oyun oynama isteği oluşturur (Aydın, 2004: 14).

İnternet bağımlılığında en büyük risk grubu 12-18 yaş arası ergenlerdir. İnternet başında uzun zaman harcanmasından ötürü bireyde kas ve iskelet sistemlerinde bozukluklar, göz ve baş ağrıları, uykusuzluk çekme, hareketsizlik ve düzensiz yeme alışkanlığı nedeniyle kilo alma gibi bir takım fiziksel problemlerin dışında, aşırı İnternet kullanımının bağımlılığa dönüşmesiyle kaygı, üzüntü, depresyon, hoşgörü eksikliği gibi zihinsel problemler de bireyleri etkisi altına alabilmektedir (Kayri ve Günüş, 2009: 157-175; Kelleci, 2008: 253-256). İnternet bağımlılığı, çocuk ve gençlerin akademik başarılarını ciddi manada düşürmekte, sosyal kayıplara ve aile ile çatışmaların artmasına neden olmaktadır (Dinç, 2010: 10-11).

Yapılan bir araştırmada, katılımcıların %25'inin İnternet bağımlısı olduğu bulunmuştur (O'Toole, 2000). Başka bir çalışmada, 11-18 yaş grubunda patolojik İnternet kullanım oranı %18,3 olarak belirlenmiştir (Kelleci, 2008: 255). Güney Kore'de, lise öğrencilerinin haftada ortalama 23 saat bilgisayar oyunu oynadıkları ve

2.1 milyon lise öğrencisinin bağımlılık riski taşıdığı, Çin’de ergenlerin yaklaşık %13,7’sinin İnternet bağımlısı olduğu tespit edilmiştir (Dinç, 2010: 29-30).

1.1.3.2.3.4 Sosyal Ağlar ve Etkileri

Sanal ortamda sosyal iletişim kurmaya yarayan ağlara “sosyal ağlar” denilmektedir. Genellikle ortak özelliklerden (bölge, meslek, okul, hobi, vb.) hareketle yola çıkan, çok sayıda üyesi bulunan ve üyelerin birbirleri ile ilgili daha fazla bilgi edinebildikleri ortamlar olan sosyal ağlar günümüzde çok popüler olmuşlardır. Nitekim bu yeni durumu Rheingold, “ağdan (the Net) ortaya çıkan sosyal toplulukların sanal cemaati” olarak tanımlamaktadır (Rheingold, 1994: 5). Özellikle gençler bu sanal cemaatlere katılarak, gruplar kurarak sosyalleşme ve yeni toplumsal formasyonlar oluşturma yoluna gitmektedir. Bu sanal cemaatler ve gruplar üzerinden gençler, yeni bireyselleşmiş kamusal alanlar ve yeni toplumsallaşma biçimleri oluşturmakta; yeni bir kimlik inşası meydana getirmektedir (Şener, 2009: 1).

Bugün İnternet’te sosyalleşmek için oluşturulan en popüler alan; Facebook, Twitter, LinkedIn, Myspace, LiveJournal gibi sosyal ağlardır. Dünyayı bir çığ gibi etkisi altına alan sosyal ağlar kullanıcı sayılarıyla rekora koşmaktadır. Sosyal ağların en popülerlerinden biri olan ve dünyada en çok ziyaret edilen site durumunda bulunan Facebook’un dünya genelindeki kullanıcı sayısı 2012 Martında 835.525.280’e ulaşmıştır (internetworldstats, 2012a). 2012 Haziranında dünyadaki İnternet kullanıcı sayısı 2.405.518.376 olarak tespit edildiği(internetworldstats, 2012b) dikkate alınır, toplam İnternet kullanıcılarının %34,73’nün Facebook kullandığı görülmektedir.

Dünyada İnternet trafiği incelendiğinde sosyal ağ ve paylaşım sitelerinin, listelerde gün geçtikçe üst sıralara doğru tırmandığı görülmektedir. Örneğin; Alexa’nın 22 Haziran 2013 tarihli verilerine göre en çok ziyaret edilen ilk yirmi site arasında Facebook 1., Twitter 11., LinkedIn 15. sırada yer almaktadır (Alexa, 2013a).

Keza, EU Kids Online’ın 25 Avrupa ülkesinde yapmış olduğu araştırma sonuçlarına göre; 9-10 yaşındaki çocukların %24’ü, 11-12 yaşındakilerin %48’i, 13-14 yaşındakilerin %72’i ve 15-16 yaşındakilerin %81’i sosyal paylaşım sitelerinden

birinde profilleri bulunmaktadır. Kullanıcı çocukların %29'u herkese açık profile sahiptir (LSE, 2009). Bunun yanında, içerisinde yüzlerce kişinin belirlenen herhangi bir başlık altında tartışma yapabildiği, kişilerin görüşlerini ve bilgilerini kolaylıkla paylaşabildiği sanal ortamlar olarak forumlar da bir tür sosyal ağ olarak tanımlanabilir. Dolayısıyla, forumların da sosyal ağlar ile bu yönüyle ortak özelliklere sahip olduğu söylenebilir.

Sosyal ağlar daha önce yüz yüze hiç karşılaşmamış insanların birbirleriyle sanal ortamda bir tanışıklık yanılgısı (Turan, 2008: 52) içinde yakınlık kurmasına imkan vermektedir. Bir süre sonra uzun yıllardır tanışılıyormuş duygusu içinde hareket edilmekte; aslında yeterince tanınmayan, gerçek kimliği ve kişiliği bilinmeyen insanlarla ileri seviyelerde yakınlık geliştirilebilmektedir. Bu süreçte farkında olmadan, aslında kim olduğu yeterince bilinmeyen insanlara karşı güven duygusu oluşturulabilmektedir. Bazen sanal ortamda başlayan yakınlık yüz yüze iletişime de dönüşebilmekte ve bu ağları kişisel çıkarları uğruna istismar etmek isteyen ve sayıları giderek artan kişilerce kullanıldığı için bu durum riskler oluşturmaktadır.

Sosyal ağlar bireyleri, kişisel verilerini kullanmak suretiyle profil oluşturmaya davet ederek ve kendi içeriklerini paylaşmaları ve birbirleriyle etkileşimlerini mümkün kılacak araçlar sunarak, büyük oranını kullanıcıların doğrudan sunduğu önemli miktarda kişisel veriye sahip olmaktadır. Sosyal ağ hizmeti sunan İnternet siteleri reklam verenlere, kullanıcılarının sunmuş olduğu kişisel veriler ve içerikler yardımı ile oldukça etkin reklam imkanı sunmakta ve gelirlerinin büyük bir kısmını kullanıcılarına yönelik reklamlardan kazanmaktadır.

Dolayısıyla, sosyal ağların risklerinden birisi, daha önce de değinildiği gibi, kontrolsüz bir şekilde kişisel bilgilerin ve özel fotoğraf, video benzeri görüntülerin paylaşılmasıdır. Özellikle çocukların ve gençlerin daha çok düştüğü bu hata, bir yandan bilişim korsanlarına ihtiyacı olan bilgilere ulaşma imkanı sunarken, diğer yandan art niyetli insanlarca tanınmaya ve ulaşılabilir hale gelmeye ya da bu kişilerin özel bilgi ve görüntüleri kötü amaçlarla kullanabilmesine olanak tanımaktadır (Yavanoğlu ve Sağıroğlu, 2010: 113-114).

Nitekim, Pingdom'ın yaptığı araştırmaya göre, sadece Facebook'a her ay 2.5 milyar fotoğraf yüklenmektedir. Bu güne kadar 30 milyardan fazla fotoğrafın yüklendiği tahmin edilmektedir (Stargazete, 31.01.2010). Microsoft'un araştırması ise, ilk gençlik çağındaki Avrupalı çocukların %71'inin İnternetteki sanal ağlara fotoğraf ve videolarını gönderdiğini belirlemiştir (Medyatava, 09.02.2010). Ancak, daha büyük tehlike, yetişkin kişilerin, çocukların ve gençlerin kişisel bilgilerine ve fotoğraflarına erişmesi ve çocuk veya gençmiş gibi onlarla iletişim kurması ve mesajlaşmasıdır. Bu ortamlarda kandırılan çocuklar; uyuşturucu, alkol, pedofili, organ mafyası, istismar, taciz ve şantaj ile karşılaşabilmektedir (Yavanoğlu ve Sağiroğlu, 2010: 114).

Sosyal ağların farklı risklerinden de söz edilmektedir. Oxford Üniversitesi'nde çalışan Nörobilimci Susan Greenfield, sosyal paylaşım sitelerinin çocukların beyinlerini etkileyerek daha fazla bencil olmalarına yol açtığını, dikkatlerini azalttığını, sitelerdeki iletişimin içeriğinin ve niteliğinin beyin gelişimini engelleyebildiğini ifade etmektedir (Özsoy, 2010: 43). 'Toxic Childhood' kitabının yazarı olan Sue Palmer de, bu siteler nedeni ile çocukların beyin gelişimlerinin hasar gördüğünü, çünkü çocukların binlerce yıldır eğlendikleri sahici aktiviteleri terk ettiklerini, halbuki, çocukların bu sosyal sitelere alışmadan önce insanlarla gerçek iletişim kurmayı öğrenmek zorunda olduklarını belirtmektedir (Zaman, 25.02.2009).

Cornwell ise, teknolojinin tek tipleştirdiği bu neslin kendi adlarına düşünemediklerini ve empati kuramadıklarını söylerken (Cornwell, 2008), Dr. Sigman de, sosyal ağların insanın biyolojik yapısına tesirlerinden bahsederek, bilgisayar önünde oturarak sosyalleşmenin genlerin çalışma biçimini ve hormon seviyelerini değiştirebileceğini, bağışıklık sistemini etkileyebileceğini, damar sisteminin fonksiyonlarını ve kişinin ruh halini bozabileceğini hatırlatmaktadır (BBC,09.10.2012).

Keza, bilgisayar ve İnternet teknolojisinin sunmuş olduğu imkanlarla birlikte bir "gözetim kültürü"nün oluşmasından ve yaygınlaşmasından da söz edilmektedir (Staples, 1997: 3). Nitekim, "Hükümet" ve "devlet" gözetlemesi, bu kültürün sadece bir parçasıdır. İnternet teknolojisi sadece iktidar organları için değil artık bireyler için

de yerlerinden kalkmadan gözetleme yapabilmelerine olanak sağlamakta, bireye kendi “özel hafıyesi” olma olanağı tanımaktadır (Bennett, 2001: 197-210).

Kullanıcılar zaten daha baştan İnternet teknolojisinin gözetlenmeye imkan sağladığını kabul etmektedir. İlginç olan durum ise bazı İnternet kullanıcılarının gözetlendiklerini bile bile bazen farklı amaçlar için “gözetlenmek” ve hatta “incelenmek” istemeleridir. Hatta “gözetleme” nin devam etmesi için gözetleyenlerin istediği kriterlere uyan ancak kendi kişiliklerini yansıtmayan sanal kimlikler oluşturma yoluna bile gitmektedirler (Altheide, 2004: 229-241).

Böylece, İnternet kullanıcıları arasında “röntgenci” ve “sergici/teşhirci” bir “gözetim kültürü” yayılırken (Altheide, 2004: 241) diğer yandan, “görmek” ve “göstermek” üzerinden kurulan bu yeni ilişkilene pratikleri ile “mahrem/özel” olan “kamusal alana” dahil olmaktadır (Toprak, 2009: 12). “Mahremin dönüşümü” olarak da adlandırılabilir bu “teşhircilik ve görme/gösterme hazzı” boyutu ayrıca irdelenmelidir. Günümüzde görülmektedir ki, İnternet ortamında bireyler isteyerek girdikleri bu denli açık ilişkilene durumlarıyla bir yandan “denetlenmekten/gözetlenmekten” haz alma anlamında “teşhirciliğe”, diğer yandan gözetlerken dahi “gözetleme/dikizleme” eyleminde bulunarak “röntgenciliğe” yönelmişlerdir. Bu da sosyal ağların toplumsal etkileri bakımından gelen ilginç ve endişe verici başka bir noktayı işaret etmektedir (Toprak, 2009: 13).

Nitekim, sosyal paylaşım sitelerinde, şimdiye kadar bize sorulmasından rahatsızlık duyacağımız pek çok özel bilgimizi sırf trend olduğu için veriyor ve bundan keyif duyuyoruz. Keza, biz de başkalarının paylaştığı bilgileri okumaktan, fotoğraflarına bakmaktan, videolarını izlemekten, 'tweet'lerini okumaktan zevk alıyoruz. Teşhir ve dikizleme bu kadar gözde bir trend olunca da pek çok kişinin paylaştığı bilgiler aslında nasıl olduklarını değil, nasıl algılanmak istediklerini gösteriyor (Dede, 2010).

Tezde buraya kadar ele alınan konular; bilgi toplumu olgusuna yönelik kuramsal eleştiriler ve bilgi toplumunun beraberinde getirdiği sorunlarla birlikte, bilgi toplumunun sembolü olan İnternetin neden olduğu güvenlik, yasadışı ve zararlı

içeriklerle mahremiyet ihlallerine ilişkin risk ve sorunlar, bilgi toplumu ve İnternetin sunduğu imkan, fırsat ve yararlarından oluşan olumlu boyutunun yanında, risk, tehlike ve sorunlardan oluşan olumsuz bir boyutunun da olduğunu göstermektedir.

Bilgi toplumu ve İnternetin hakikatına vakıf olabilmek için konuyu bu iki boyutunu da ihata edecek şekilde ele almak gerekmektedir. Dolayısıyla, bilgi toplumu ve İnternete ilişkin politikalarda bu iki boyutun birlikte değerlendirildiği ve analiz edildiği yaklaşımlar geliştirilmelidir. Aksi halde, risklerin ve sorunların görmezden gelinmesi veya yeterince dikkate alınmaması, söz konusu risk ve sorunların ihmal edilmesi sonucunu doğuracak ve bilgi toplumu ve İnternet politikalarında karşı önlem geliştirilmesi ve mücadele edilmesine yönelik hususların yeterince yer bulmasına mani olacaktır. Yani, politikaların söz konusu olumsuzluklarla mücadeleyi kapsayan ayağının eksik veya yetersiz kalmasına neden olacaktır.

Nitekim, bilgi toplumu ve İnternet politikalarında, bahsi geçen tüm risk ve sorunlara rağmen bugüne kadar yasadışı ve zararlı İnternet içerikleri ile mücadeleyi öngören düzenleme ve uygulamaların yeterince yer bulmamasının arka planında bu bütüncül yaklaşımın eksikliği görülmektedir. Bu durum ise, tüm toplumu ve özellikle çocukları, gençleri ve aileleri olumsuz yönde etkileyen yasadışı ve zararlı içeriklerden oluşan sosyal maliyetleri gün geçtikçe artırmaktadır.

Keza, İngiltere’de Psikoloji Profesörü Tanya Byron yönetiminde yapılan ve 2008’de yayınlanan “Dijital Dünyada Güvenli Çocuk Raporu”nda, sanal ortam ve medyanın ticari kaygılar ve popülist yaklaşımları nedeniyle “Vahşi Batı”yı hatırlattığı, buna karşı mücadele veren yönetsel ve toplumsal grupların bulunduğu, fakat bu iki tarafın yaklaşım farkları ve korumaya çalıştıkları şeylerin farklı olması nedeniyle şiddetli bir çatışma ortamının olduğu ve bu çatışma ortamında kaybedenlerin ise çocuklar ve aileleri olduğu belirtilmektedir (Safer Children in a Digital World, 2008).

Tezin bu kısmına kadar, bilgi toplumu bağlamında, neden oldukları riskler ve sorunlar çerçevesinde, yasadışı ve zararlı içeriklerle mücadele edilmesi için içerik düzenlemelerinin neden gerekli olduğu konusu ve sosyal gerekçeleri ortaya

konulmuştur. Böylece, tezin temel hipotezinin bir bölümü ile alt hipotezlerimizin ilk dördüne ilişkin tartışmalar ve değerlendirmeler gerçekleştirilmiştir.

Bundan sonra ise, temel hipotezimizde yer alan, İnternetin daha faydalı, güvenli ve etkin kullanımını sağlamak amacıyla gerçekleştirilecek bu düzenlemelerin meşruiyeti ve başarısını etkileyecek şartlar değerlendirilecektir. Bu kapsamda tezin birinci bölümünün ikinci kısmında, İnternetin teknik özellikleri ve uluslararası yönetimi konuları ele alınacaktır. Böylece, içerik düzenlemelerin meşruiyet ve başarı şartlarından olan “İnternetin kendine özgü yapısı ve özelliklerinin gözetilmesi” hususuna açıklık getirilmiş olacaktır. Zira, bu şekilde, İnternetin kendine özgü yapısı ve özelliklerinin ne olduğu ile gelişimine ve büyümesine etki edecek unsurların neler olacağı görülecek ve dolayısıyla, içerik düzenlemelerinde bu çerçevede hesaba katılması gereken değişkenler ve sınırlar açığa çıkmış olacaktır. Ayrıca, içerik düzenlemelerinin İnternet kaynaklı teknik ve yönetsel sınırlılıkları da görülecektir. Eleştiriye açık pek çok yönüne karşın, İnternet teknolojilerinden vazgeçmek mümkün olmayacağına göre, bu teknolojiden insanlığın daha fazla yararlanabilmesinin şartlarını oluşturmak açısından, İnternetin kendine özgü yapısından kaynaklı teknik ve yönetsel sınırlılıklarını bilmek önem arz etmektedir.

1.2 İNTERNET

Tezin odak noktasını oluşturan İnternete ilişkin büyük fotoğrafın netleşmesi için İnternetin teknik özellikleri ve yönetimi boyutunun incelenmesi gerekmektedir. Bu amaçla, İnternetin ne olduğu, gelişim süreci, yapısal unsurları, alt yapısı, aktörleri, geleceği, uluslararası yönetim sorunu ve İnternet yönetişimi konuları ele alınacaktır.

1.2.1 İnternetin Gelişimi

İnternet kelimesi, İngilizce “kendi aralarında bağlantılı ağlar” anlamına gelen “Interconnected Networks” sözcüklerinin kısaltmasından meydana gelmiştir (Wikipedia, 2010a). İnternet, iletişim sistemine (Modem ya da LAN (Local Area Network) bağlantısı) sahip dünya üzerine yayılmış milyonlarla ifade edilen sayıdaki bilgisayarların birbirlerine bağlanmasıyla oluşan bilgisayar ağlarının aralarında tekrar

bağlantı kurmalarıyla büyüyerek gelişen global bir bilgisayar ağları sistemidir (Erkan ve Songür, 1999: 282; İnan, 1998: 5).²⁹

İnternetin teknolojik temellerinin atılmasında soğuk savaş döneminin iki süper gücü arasındaki mücadele ve karşılıklı duyulan endişeler önemli rol oynamıştır (Sınar, 2001: 22). 1957 yılında ABD’de, muhtemel bir nükleer savaş veya sosyal karışıklık durumunda yeni iletişim sisteminin bütünüyle yok olmaması için, tek bir ana bilgisayar ünitesinden bağımsız olarak çalışabilen ve dolayısıyla tek bir merkezden yönetilmeyen bir bilgisayar ağı kurulması fikri ortaya atıldı (Winston, 1996:140).

Bu sistemi gerçekleştirmek için, ABD Savunma Bakanlığı bünyesinde 1969 yılında “ARPANET Projesi” (Advanced Research Project Authrotiy Net) başlatılmıştır (İnan, 1998: 7). İnternetin mucidi denilebilecek Carl Lickleider, yaptığı çalışmalar ile bilgisayarların bir merkeze bağlı olmaksızın birbirlerini tanımaları ve iletişim kurmalarını sağlamıştır (Winston,1996:140). İlk olarak 1969’da California’daki üç ayrı merkez ile Utah’ta bulunan toplam dört farklı noktadaki bilgisayarlar arasında bilgi aktarımı gerçekleştirilmiştir (Köksal vd., 1996: 17; İçel, 2000: 407). Bu başarı, ARPANET’in resmen uygulamaya geçirilmesini sağlamış ve ağ sistemi geliştirilerek ARPANET isimli askeri bir bilgisayar ağı kurulmuştur (Sınar, 2001: 22). Bir süre sonra bilgisayarlar arasında uyumsuzluk ve iletişim kuramama sorunları ortaya çıkmıştır. Bu sorunun aşılması amacıyla, bugün de kullanılan TCP/IP adı verilen bir protokolün 1968 yılında temelleri atılmış ve 1983 yılında protokol tam olarak oluşturulmuş ve uygulamaya konulmuştur (Sınar, 2001: 22; Özdilek, 2002: 19).

ABD Ordusu, 1980 yılından itibaren ARPANET’i, üniversiteleri ve diğer kamu kurumlarını da kapsayacak şekilde kullanıma açmıştır. Zamanla özel işletmeler de bu geniş ağına dahil edilmiştir. 1983 yılında Amerikan ordusu bu ağdan ayrılarak kendine MİLNET isimli yeni bir ağ kurmuş (Wikipedia, 2010b) ve ARPANET’i tamamen sivilin kullanımına bırakmıştır (Köksal vd., 1996: 17). Ortaya çıkan bu “ağlar sistemi” ise “İnternet” olarak isimlendirilmiştir (Işıklı, 2001: 8).

²⁹ İnternet kelimesi özel isim olduğu için ilk harfi büyük olarak yazılmaktadır. Küçük harf ile yazılırsa birden fazla ağı birleştiren bağlantıları (internetwork) ifade etmektedir (Sarıhan, 998: 10).

1986'da ABD Ulusal Bilim Vakfı (National Science Foundation-NSF), bugün bile İnternet için önemli bir iletişim servis omurgası olan NSFNET'in oluşumuna başlamıştır (Akbulut, 1999:17). 1989 yılında, Cenevre'deki CERN (Centre Européen Recherces Nucléaires) merkezinde World Wide Web (www) standardı geliştirilerek hizmete sunulmuştur. 1992 yılında World Wide Web'in dayandığı en temel dosya transfer protokolü olan Hypertext Transfer Protocol (http) geliştirilmiştir (Wikipedia, 2010c). Bu teknoloji ile, İnternet üzerinden yazı, resim, ses, video gibi farklı nitelikteki verilerin veri bütünlüğü bozulmadan transfer edilmesi mümkün olmuştur. Böylece ARPANET tamamen ortadan kalkmıştır (Sınar, 2001: 23). 1994 sonrasında hızla artan bu yeni ağ ve ağ omurgaların İnternete katılımı ve İnternetin bireysel kullanıma açılmasıyla İnternet, gerçek anlamıyla ortaya çıkmış ve hızla yaygınlık kazanarak bugünkü durumuna ulaşmıştır (Özdilek, 2002: 19; Sınar, 2001: 23).

1.2.2 Dünyada İnternet Kullanımı

Günümüzde İnterneti kullanan kişi sayısı her geçen gün artmaktadır. 1995 yılında, dünya genelinde İnternet kullanıcı sayısı 16 milyon iken, 2012 Haziran ayı itibariyle 2 milyar 405 milyona ulaşmıştır. Aynı tarihler için Dünya nüfusu içinde İnternet kullanım oranı ise, %0,4'den %34,3'e yükselmiştir (internetworldstats 2012b).

Dünya genelinde 1995 ve 2012 yıllarında en çok İnternet kullanıcılarına sahip ilk beş ülkeye bakıldığında ise; geçen 15 yılda dengelerin değiştiğine şahit olunmaktadır.

Tablo 0.1. 1995 ve 2012 yıllarında en çok İnternet kullanıcılarına sahip ülkeler

X	1995 Yılındaki Kullanıcı Sayısı	X	2012 Yılındaki Kullanıcı Sayısı
1	A.B.D (25 milyon)	1	Çin (538 milyon)
2	Japonya (2 milyon)	2	A.B.D (245 milyon)
3	Almanya (1.5 milyon)	3	Hindistan (137 milyon)
4	Kanada (1.2 milyon)	4	Japonya (101 milyon)
5	İngiltere (1.1 milyon)	5	Brezilya (88 milyon)

Kaynak: **The rather petite Internet of 1995**, <http://royal.pingdom.com/2011/03/31/internet-1995/> (25.04.2011); <http://www.internetworldstats.com/top20.htm> (04.03.2013)

Tablo1.1.'de görüldüğü üzere 1995 yılında en çok İnternet kullanıcısına sahip ülke ABD iken 2010 yılında Çin ilk sırayı almıştır. Keza, geçen zaman içinde gelişmiş batılı ülkelerin yerlerini Hindistan ve Brezilya gibi gelişmekte olan ülkelere bıraktığı görülmektedir. Kuşkusuz bu tablonun oluşumunda söz konusu ülkelerin sahip olduğu yüksek nüfusun önemli bir faktör olduğunu belirtmek gerekmektedir.

Tablo 0.2. Dünya genelinde en çok İnternet kullanıcısına sahip ilk 20 ülke

Ülke Adı	Nüfus	İnternet Kullanıcısı (2000)	İnternet Kullanıcısı (2012)	Kullanım Oranı	Tüm Kul. İçindeki Oranı
Çin	1.343.239.923	22.500.000	538.000.000	40,10%	22,40%
ABD	313.847.465	95.354.000	245.203.319	78,10%	10,20%
Hindistan	1.205.073.612	5.000.000	137.000.000	11,40%	5,70%
Japonya	127.368.088	47.080.000	101.228.736	79,50%	4,20%
Brezilya	193.946.886	5.000.000	88.494.756	45,60%	3,70%
Rusya	142.517.670	3.100.000	67.982.547	47,70%	2,80%
Almanya	81.305.856	24.000.000	67.483.860	83,00%	2,80%
Endonezya	248.645.008	2.000.000	55.000.000	22,10%	2,30%
İngiltere	63.047.162	15.400.000	52.731.209	83,60%	2,20%
Fransa	65.630.692	8.500.000	52.228.905	79,60%	2,20%
Nijerya	170.123.740	200.000	48.366.179	28,40%	2,00%
Meksika	114.975.406	2.712.400	42.000.000	36,50%	1,70%
İran	78.868.711	250.000	42.000.000	53,30%	1,70%
Kore	48.860.500	19.040.000	40.329.660	82,50%	1,70%
Türkiye	79.749.461	2.000.000	36.455.000	45,70%	1,50%
İtalya	61.261.254	13.200.000	35.800.000	58,40%	1,50%
Filipinler	103.775.002	2.000.000	33.600.000	32,40%	1,40%
İspanya	47.042.984	5.387.800	31.606.233	67,20%	1,30%
Vietnam	91.519.289	200.000	31.034.900	33,90%	1,30%
Mısır	83.688.164	450.000	29.809.724	35,60%	1,20%
İlk 20 Ülke	4.664.486.873	273.374.200	1.776.355.028	38,10%	73,80%
Diğer Ülkeler	2.353.360.049	87.611.292	629.163.348	26,70%	26,20%
Dünya Toplam Kullanıcılar	7.017.846.922	360.985.492	2.405.518.376	34,30%	100,00%

Kaynak: <http://www.internetworldstats.com/top20.htm> (04.03.2013)

Dünya genelinde en çok İnternet kullanıcısına sahip ilk 20 ülke, 2000 yılından 2012 yılına kadar bu ülkelerdeki kullanıcı sayılarındaki değişim ve bu ülkelerin İnternet kullanıcılarının dünyadaki toplam kullanıcılar içindeki oranları Tablo 1.2. de görülmektedir. Keza, bu ilk 20 ülkenin kullanıcılarının toplam sayısı ve bu rakamın dünyadaki toplam kullanıcılar içindeki oranları da bu tabloda yer almaktadır.

Tablo 1.3.'den, dünyada bölgesel bazda İnternet kullanıcı sayısında 2005-2010 yılları arasındaki büyümeye bakıldığında, en fazla büyümenin % 2.357'lik bir oranla Afrika bölgesinde gerçekleştiği görülmektedir. Ancak, kullanım oranına bakıldığında aynı bölgenin %10,9 ile dünyanın en gerisinde kaldığı tespit edilmektedir. Yayılım oranı en yüksek olan bölge %77,4 ile Kuzey Amerika olduğu ve onu sırasıyla Avustralya, Avrupa, Latin Amerika, Ortadoğu, Asya ve Afrika'nın izlediği görülmektedir.

Tablo 0.3. Dünyada bölgesel olarak İnternet kullanıcı ve nüfus istatistiği

Dünya Bölgeleri	Nüfus(2012)	İnternet Kullanıcısı (2000)	İnternet Kullanıcısı (2012)	Kullanıcı Oranı	Büyüme (2010-2012)	Tüm Kullanıcılar İçindeki Oranı
Afrika	1.073.380.925	4.514.400	167.335.676	15,60%	3606,70%	7,00%
Asya	3.922.066.987	114.304.000	1.076.681.059	27,50%	841,90%	44,80%
Avrupa	820.918.446	105.096.093	518.512.109	63,20%	393,40%	21,50%
Orta Doğu	223.608.203	3.284.800	90.000.455	40,20%	2639,90%	3,70%
Kuzey Amerika	348.280.154	108.096.800	273.785.413	78,60%	153,30%	11,40%
Latin Amerika	593.688.638	18.068.919	254.915.745	42,90%	1310,80%	10,60%
Avustralya	35.903.569	7.620.480	24.287.919	67,60%	218,70%	1,00%
Dünya Toplamı	7.017.846.922	360.985.492	2.405.518.376	34,30%	566,40%	100,00%

Kaynak: <http://www.internetworldstats.com> (27.04.2011)

1.2.3 İnternetin Yapısal Unsurları

Bu bölümde, İnternetin yapısal unsurlarına ilişkin bazı temel bilgilere yer verilmiştir.

1.2.3.1 TCP/IP Protokolü

İnternet aracılığıyla bilgi iletimi ve paylaşımını gerçekleştirmek bazı kurallara uyulmasına bağlıdır. Bu kurallara "İnternet protokolleri" veya "TCP/IP Protokolü" denir (İçel, 2000: 407; Akbulut, 1999: 17). Bu protokolleri, dünya üzerindeki milyonlarca bilgisayarın ve yerel ağların birbirleri ile iletişim kurmalarını sağlayan ortak anlaşma dili olarak tanımlayabiliriz (Sınar, 2001: 24). İnternet hizmetlerini kullanabilmek için gerekli olan tüm programlar ve bağlantı programları, TCP/IP protokolüne uygun olarak çalışır ve işlevlerini yerine getirirler (Köksal vd., 1996:19).

TCP/IP protokolü, iki ayrı protokolün bir araya gelmesi sonucunda oluşmuştur. Bunlardan TCP (Transport Control Protocol) mesajların doğru yere ulaşmasından, IP (Internet Protocol) ise adresleme sisteminden sorumludur (Kaya, 2009: 7). İnternet'e doğrudan bağlı her bilgisayarı tanımlayan bir IP numarası vardır. Bu numara aynı zamanda IP adresi olarak da tanımlanır. IP numarası, birbirlerinden noktalarla ayrılmış dört rakam kümesinden meydana gelir. Bu rakamlar 0-225 arasında değişen bir tam sayıdır. Örneğin, 212.165.121.158 gibi. Bu rakam kümesi İnternetin hiyerarşik yapısını tanımlar. Gerçekte İnternet iletişimde bu sayısal adresler kullanılır. Hangi bilgisayarla İnternete girildiğinin tespiti açısından bu IP numaraları önemlidir. Bir İnternet sitesinin IP adresi biliniyorsa, adres çubuğuna (web tarayıcısı) bu adres yazılarak siteye ulaşılabilir. Ancak bu rakamları akılda tutmak zor olduğu için her bir IP adresine karşılık gelen alan adları kullanılmaktadır (Sarıbaş, 2007: 64).

1.2.3.2 World Wide Web (www)

Kısaca "web" denilen ve kelime anlamı olarak, dünyayı saran ağ anlamına gelen World Wide Web, dünyanın her yerindeki binlerce bilgisayarda kayıtlı bulunan milyonlarca dosyadan oluşan bir bütündür (Yıldız, 2007: 22). "www", film, video, animasyon, ses, yazı, resim gibi birbirlerinden farklı verilere etkileşimli olarak ulaşmamızı sağlayan çoklu bir hiper ortam sistemidir (İnan, 1998: 72).

Web'i oluşturan donanım, yazılım ve protokolleri şöyle sıralayabiliriz:

1. *Web Tarayıcısı:* Web adreslerine ve hizmet birimlerine ulaşmayı sağlayan kullanıcı ara birim programlarına “web tarayıcısı” (web browser) denilmektedir. Günümüzde, Microsoft Internet Explorer, Fireworks, Google Chrome ve Yandex en büyük web tarayıcılarıdır (Odabaşı vd., 2007:17; Sırabaşı, 2007:62; Yıldız, 2007:23).

2. *Web Sayfaları:* Kullanıcının bir web hizmet merkezine bağlandıktan sonra tek seferde bilgisayar ekranına aktarabildiği verilerden oluşan dosya “web sayfası”dır. Bu sayfadaki veriler metin, resim, grafik veya ses bilgileri içerebileceği gibi, başka merkezlerle de bağlantılı olabilir ve sayfanın içinden değişik sayfalara bağlantılar (linkler) konulabilir. Web sitesi, belli bir kuruluş veya kişiye ait web sayfalarından oluşmaktadır. Web sayfası bir sunucuya yüklenmiş HTML dokümanıdır ve web aracılığıyla ulaşılabilmesi için URL’ye sahiptir(Sırabaşı, 2007: 62; Yıldız, 2007: 23).

3. *HTTP Protokolü:* HTTP (Hyper Text Transfer Protocol) ise, İnternet üzerinde HTML işaret dili kullanılarak oluşturulan web sayfalarının aktarılabilmesi için kullanılan standart protokolün adıdır. HTTP protokolü, bu özelliği ile web üzerinde en çok kullanılan protokoldür. Örneğin, araç çubuğuna “www.sistem.com.tr” adresi yazıldığında, HTTP protokolü, alt seviyedeki protokollere bu adresin nereden, nasıl isteneceğini ve nasıl aktarılacağını söylemektedir (Yıldız, 2007: 24; İnan, 1998: 547).

4. *URL Adresi:* İnternet üzerinde web sayfaları da dahil, erişilebilecek olan servisleri belirtmek ve tanımlamak için kullanılan adreslere URL (Uniform Resource Locator) denir. Terim, “Standart Kaynak Bulucu” olarak Türkçeye çevrilebilir. Her İnternet sayfasının sadece kendine ait bir URL’si vardır. Bu dosyaya ulaşabilmek için kullanılan yöntem olan transfer protokolünü URL’nin birinci kısmında görürüz. Birçok web sayfasının başında “http” harflerinin görülmesi, erişimin HTTP Protokolü üzerinden yapılmasındandır. (Yıldız, 2007: 25; İnan, 1998: 547).

1.2.3.3 Alan Adı ve Adreslerin Gruplandırılması:

Alan adı (domain name), İnternet’te bir siteye ulaşmak için kullanılan ve kolayca hatırlanabilen kısaltmalardan oluşan adrestir. Bu, alan adı ve buna karşılık gelen IP numarasından oluşan iki bileşenin yardımıyla olmaktadır. Geniş veri tabanlarında

(registry), alan adları ile bunların karşılığı olan IP sayısal adreslerinin bir listesi yer almaktadır. Bu veri tabanları, alan adları ile bu isimlere karşı gelen IP sayısal adreslerinin eşleştirilme fonksiyonunu yerine getirirler (Alkan ve Canbay, 2003: 2; Işıklı, 2011: 10-11). İnternet üzerinde aynı adres ancak bir kere tescil ettirilebilir. Bu nedenle, başkası tarafından tescil ettirilmiş bir adres satın alınamaz (Canbay, 2005).

Alan adı sisteminde, “www.selcuk.edu.tr” örneğinde olduğu gibi, bir alan adı noktalarla ayrılan dört ana bölümden (labels) oluşur (ICANN, 2011a). Soldan sağa doğru ilk kısım kullanılan TCP/IP alt protokolünü gösterir (örneğin; www, ftp, icr vs). İkinci kısımda adresin ait olduğu kuruluşu tanıttıcı ifade yer alır (Sırabaşı, 2007: 64; Yıldız, 2007: 25). Üçüncü kısım, bu adresin bağlı olduğu kurumun hangi türden bir kurum olduğunu gösterir. Başlıca alan ekleri şunlardır: “.com” ticari kuruluşlar, “.org” sivil toplum kuruluşları, “.edu” eğitim kuruluşları, “.ac” akademik kuruluşlar, “.gov” hükümet kuruluşları, “.int” uluslararası kuruluşlar, “.mil” askeri kuruluşlar. (İçel vd., 2000: 409; Köksal vd., 1996: 39).

En son kısımdaki iki harfli kısaltma ise, ülke tanıtım kodudur. İnternet yayınının bulunduğu ülkeyi, yani yayının hangi ülke çıkışlı olduğunu gösterir. Örneğin Türkiye için “.tr”, Almanya için “.de”, Fransa için “.fr”, İngiltere için “.uk” gibi kısaltmalar kullanılmaktadır. İlginçtir ki, İnternetin anavatanı olan ABD, bu konuda diğer ülkelerden ayrılır. Bu ülkeden çıkış yapan adreslerde kural olarak ülke kısaltması bulunmaz. (Sırabaşı, 2007: 64; Yıldız, 2007: 25; İçel vd., 2000: 409). Uluslararası düzeyde alan adları ile ilgili politikalar ICANN isimli kuruluş tarafından belirlenmektedir. ICANN, ülke kodu içermeyen alan adlarının hukuki yapısı ve tescil şartlarını doğrudan kendisi belirlerken, ülke kodlu alan adlarının yönetimini ise belirli kurallar çerçevesinde her ülkede bir kuruluşa devretmiştir (Dal, 2010: 486).

1.2.4 İnternetin Alt Yapısı

İnternet ortamındaki veri iletişimi, omurga (backbone) adı verilen ana iletişim hatları üzerinden sağlanmaktadır. Bu altyapıların omurga olarak nitelendirilebilmeleri için geniş coğrafi alana yayılmış olmaları ve küçük İSS'lara trafik taşıma hizmeti

sunmaları gerekmektedir (Güngör ve Evren,2002:7). Bu omurgalar başka omurgalara bağlı bulunabilmektedir. Diğer veri iletişim hatları ise, bir ağacın dalları misali, bu ana hattan ayrılarak verileri çeşitli merkezlere iletirler (Erkan ve Songür, 1999: 45).

Nitekim, ABD’de kurulan omurgalar, 11 Ağ Erişim Noktası (Network Access Point-NAP) aracılığıyla birbirlerine bağlanmıştır. Bu şekilde bir omurgadaki veri iletişimi bir diğer omurgaya aktarılabilir (Sınar, 2001: 29). NAP’lar İnternet omurgasının ana unsurlarından birisidir. Çünkü, NAP’lar içerisindeki bağlantılar trafiğin nasıl yönlendirileceğini belirlemektedir (Güngör ve Evren, 2002: 8).

İnternet omurgası işletme yetkisi, bu konuda belirlenmiş olan kurallara uymak şartıyla, yatırım yapan herhangi bir özel sektör kuruluşu tarafından kullanılabilir (İçel vd., 2000: 410). Bu büyük çaplı ağ işletmecileri omurga sağlayıcılar olarak adlandırılmaktadır. Omurga sağlayıcının İSS’lara sağladığı bu ana hizmet İnternet sektörünün toptan (wholesale) pazarını oluşturmakla birlikte teknolojinin getirdiği olanaklar sayesinde bu işletmeler sıkça perakende İnternet hizmetleri (İSS) sektöründe de boy göstererek dikey bütünleşmeye yol açmaktadır. Omurga sağlayıcı sektöründe rekabetin üst düzeyde olduğu iki önemli ülke ABD ve Kanada’dır (Güngör ve Evren, 2002: 7-8).

1.2.5 İnternetin Aktörleri

İnternetin son kullanıcıya ulaştırılmasında ulusal ölçekte aracı unsurlar olarak görev ifa eden İnternet aktörleri, İSS ile erişim, yer ve içerik sağlayıcılarıdır. Erişim, yer ve içerik sağlama faaliyetleri zaman zaman iç içe geçmesine rağmen, fonksiyonları ve hukuki sorumlulukları birbirinden farklıdır.

1.2.5.1 İnternet Servis Sağlayıcılar

İnternet’in kullanıcılara ulaştırılmasına ve kullanımına sunulmasına aracılık eden gerçek veya tüzel kişiler İnternet Servis Sağlayıcı (İSS) olarak adlandırılır Bunlar özel kişilerin ve özel hukuk veya kamu hukuku tüzel kişilerinin İnternete

bağlanmalarını, İnternet üzerinden iletişim kurmalarını ve İnternetin sağladığı olanakları kullanmalarını temin eden aracı unsurlardır (Pekşirin vd., 2012).

Geniş anlamı ile İnternet hizmeti sunan herhangi bir kuruluşa İSS denebilir. Bu tanım çerçevesinde çevirmeli İnternet erişimi sunan bir işletmeciden Uluslararası Telekomünikasyon Birliği (International Telecommunication Union-ITU)'ne kadar İnternet hizmeti veren her kuruluş İSS olarak değerlendirilebilir. Bir İSS'nın yaptığı işi, sahip olduğu bilgisayar donanımı ve yerel şebekeden kiraladığı hatlar aracılığı ile kullanıcıları yerel ve uluslararası İnternet omurgalarına taşımak olarak özetleyebiliriz. İSS'ların kullanıcıya sattığı bu hizmet, İnternet sektörünün perakende (retail) pazarını oluşturmaktadır (Güngör ve Evren, 2002: 7).

İSS'lar farklı ülkelerde, farklı yapılarda olmalarına rağmen, genel olarak salt İnternet erişimi (mere conduit - AB Direktif'i tanımı) sağlamaktadırlar. Fakat İSS'ların erişim hizmeti dışında, sunucu kiralama, alan adı sağlama (domain name hosting), sunucu barındırma (hosting), uygulama servis sağlayıcılığı (application service provider), içerik (bilgi) sunma gibi hizmetleri de bulunmaktadır (Pekşirin vd., 2012).

İnternet'e bağlanabilmek için gerekli olan İSS dışındaki tüm unsurlar, aslında dünyanın her yerinde ölçülebilen özellik ve kalitede temin edilebilen belli standartlara sahip maddi unsurlardır. Bu unsurlardan sadece İSS'nın, sağladığı hizmet kalitesi ve standartları ile İnternet'i kullanma konusunda farklılık oluşturması mümkündür. İnternet sistemi içinde asıl birinci derece önem taşıyan aktör ve dinamik hüviyetteki hukuk sujesi İSS işletmeleridir (Pekşirin vd., 2012).

1.2.5.2 İnternet Erişim Sağlayıcılar

Kullanıcılarına İnternet ortamına erişim imkanı tanıyan gerçek ve tüzel kişiler İnternet Erişim Sağlayıcılar (İES) olarak değerlendirilmektedir (Sarı, 2011: 47). İES, İnternete bağlanmak isteyen kişiler ile İnternet arasında köprü görevi görerek, kullanıcıların, genellikle belirli bir ücret ve sözleşme karşılığında İnternet'e ulaşmasını sağlamaktadır (Sınar, 2001: 41). Verdikleri hizmet teknik yönden farklılık

göstermesine rağmen, çoğu zaman İES, İSS'ları kavramının içerisinde mütalaa edilmektedir (Kiremitçi, 2012: 11).

Erişim sağlama hizmetinin ana omurgasını, haberleşme ve veri akış kanallarını kontrol altında tutmaları nedeniyle sabit telekomünikasyon işletmeleri oluşturmaktadır. İletişimin gelişmesiyle birlikte günümüzde cep telefonu şirketleri de çok sayıda aboneye İnternete erişim imkanı sağlamaktadır. Telekomünikasyon işletmeleri mevcut telefon hatları içerisinde ayırdıkları hatları, şirketler veya kamu kurum ve kuruluşlarına İnternet bağlantı hizmeti sunmak üzere kiralamakta veya devretmektedirler. Birçok ülkede telekomünikasyon alt yapısını kurma ve bunu işletme hakkı ya kamu kurumu niteliğindeki kuruluşlara ya da imtiyaz tanınan özel sektör kuruluşlarına verilmiştir (Kiremitçi, 2012: 11-12).

İnternet erişim hizmeti sağlayan işletmeciler, uluslararası erişim hizmeti veren operatörler ile kiralık bağlantılar sağlayarak kullanıcılarının yurtdışı içeriğe erişimini sağlamaktadır. Ülkemizde erişim sağlama hizmeti sunan şirketlerin bazılarını Türk Telekom A.Ş., Süperonline, Koçnet, Doğan Telekom, Borusan Telekom örnek olarak verilebilir. Ülkemiz yurtdışı irtibat noktaları ise, Almanya, Hollanda, İngiltere'dir. Bunların dışında, İran, Suriye, Gürcistan, Azerbaycan, Mısır, Irak gibi ülkelere Türkiye'de hizmet veren İnternet altyapısına sahip bazı operatör alt yapıları üzerinden İnternet erişim hizmeti verilmektedir (Sarı, 2011: 49).

1.2.5.3 İnternet Yer Sağlayıcılar

Bir İnternet sitesinin İnternet üzerinden erişilebilir kılınması isteniyorsa hazırlanmış olan İnternet sayfalarının ve resim, video gibi ilgili tüm materyallerin İnternet kullanıcılarına ulaştırılabilmesi için yirmi dört saat açık bir bilgisayarda tutulması gerekmektedir. Bu İnternet sitesini ve ona ait tüm dokümanları saklayan ve İnternette yayınlanmasını sağlayan donanımsal ve yazılımsal olarak özel üretilmiş bilgisayarlara “sunucu” denilmektedir (Bilişim Akademi, 2006).

İnternet sayfalarının ve resim, video gibi ilgili tüm materyallerin sunucu üzerinde barındırılması işleminin genel ismi “yer sağlama” olarak adlandırılmaktadır (Sarı,

2011: 33). Diğer bir ifadeyle yer sağlama, “İnternet sitelerine ait dosyaları saklayan ve kullanıcıların erişimine sunan bilgisayarlar (web sunucusu-web server) aracılığıyla bu verileri saklama ve yayınlama işlemidir” (Hostbul, 2012). Yer sağlayıcı ise, bu işlemi yapan yani, İnternet ortamında bulunan içeriği sunucularında barındıran ve yayınlayan kişi/kuruluştur. Dünyada bu işleme ve işlemi yapanlara “hosting” denilmektedir (Bilişim Akademi, 2006). Hostingler, ücret karşılığında, İnternet sayfalarına yüksek hızda ve çok sayıda kullanıcının aynı anda bağlanmasına imkan sağlayacak donanımda yer sağlama hizmeti verirler (Hostbul, 2012).

Günümüzde farklı türde yer sağlama hizmetleri sunulmaktadır. Yer sağlama hizmetlerini, paylaşılan barındırma (Shared web hosting), kiralık sunucu (Dedicated web hosting), yönetimli kiralık sunucu (Managed web hosting), sunucu barındırma (Co-location web hosting), bayi web barındırma (Reseller web hosting), sanal sunucu (Virtual private server), içerik dağıtım ağı (CDN-Content delivery network) ve bulut bilişim (Cloud computing) şeklinde sıralamak mümkündür (Özbey, 2011: 22-23).

İnternet ortamında bir web sitesi yayınlatabilmek için, isminin kolayca hatırlanabilmesi ve İnternet’te bulunabilmesi amacıyla öncelikle bir alan adı satın alınması, daha sonra web sitesindeki materyallerin yer sağlama hizmeti sunan bir şahıs, şirket veya kurumun sunucusuna yüklenmesi gerekmektedir. Tüm bunlar sağlandıktan sonra bu İnternet sayfasına ulaşmak isteyen kişiler ancak erişim sağlayıcılar aracılığıyla web sitesine ulaşabilecektir (Kiremitçi, 2012: 12).

1.2.5.4 İnternet İçerik Sağlayıcılar

İnternet içeriği, İnternet ortamında kullanıcılara erişim imkanı sağlanmış her türlü bilgi, belge, resim, video, veri tabanı ve materyali ifade etmektedir. İnternet içerik sağlayıcı ise, içeriği bizzat üreten ve düzenleyen kişi ya da kuruluştur (Kiremitçi, 2012: 12). Esasında içerik sağlayıcı kişi veya kuruluşlar, belli bir bilgiyi İnternet ortamına aktarmaktadır. Örneğin bir web sayfasının sahibi içerik sağlayıcıdır. Keza, “downloading” yolu ile elde edilecek nitelikteki bilgileri hazırlayıp sunanlar da içerik

sağlayıcı durumundadır. İnternet ortamında erişilebilen serverler da, doğal olarak birer içerik sağlayıcı durumundadır (Superonline Workshop, 2000).

1.2.6 İnternetin Geleceği: Web 1.0 dan Web 3.0'a

Web 1.0, kişiler tarafından oluşturulan, ziyaretçiler tarafından müdahale edilemeyen, sadece okunan, dinlenen veya izlenen içeriklerdi. Kullanıcılara içeriği okuma, izleme, program ve dosya indirme imkanı sağlıyordu ve tüm kontroller web sitesinin elindeydi. İnsan etkileşimi yoktu. (Wikipedia, 2010d; Türk İnternet, 2010).

Web 1.0'ın yetersizliğinden dolayı Web 2.0 doğmuştur. Web 2.0, 2004 yılından itibaren kullanılmaya başlayan yüksek etkileşimli yeni nesil İnternet teknolojilerinin genel adıdır. Bu teknolojiler kullanıldığında web siteleri kullanıcılarına yorum yazarak, resim göndererek veya bizzat içerik oluşturarak içeriğin bir parçası olma imkanı sağlamaktadır. Web 2.0 verinin akış yönünü değiştirmekte ve veri web sitesinden kullanıcıya değil kullanıcıdan web sitesine akmakta, kullanıcı edilgen olmaktan çıkmaktadır (Wikipedia, 2010d; Türk İnternet, 2010).

Web 2.0 teknolojilerinin yıldızı ise blog servisleridir. Bu servisleri kullanarak web sitesi oluşturmak çok kolay hale gelmiş ve kişisel web siteleri olan bloglar hızla çoğalmıştır. Bloglar özellikle genç kullanıcılar tarafından tercih edilmekte ve böylece kullanıcılar bilgiyi hem oluşturmakta hem de tüketmektedir. Blog servislerinin kullandığı teknoloji, kişinin yalnızca bir sayfaya link vermesini değil, sayfaya abone olarak sayfa her değiştiğinde bir bildirim almasını da mümkün kılmaktadır. Böylece, hem içerik hem de linkler canlılıklarını korumaktadır (Türk İnternet, 2010).

Web 2.0 teknolojilerinin yaygınlaşmasıyla milyonlarca üyesi olan blog, sosyal ağ siteleri, web tabanlı özgür ansiklopediler, yer imleme servisleri gibi çevrimiçi topluluklar ortaya çıkmış ve etkileşim ve paylaşım olanaklı hale gelmiştir. Bu teknolojiler İnternet üzerinden işbirliğini, paylaşımı ve seçim haklarını harekete geçirmekte ve bireylerin bilgiyi öğrenme, tüketme ve hatta siyasal alışkanlıklarını derinden etkilemektedir. Bunun yanında, Web 2.0 teknolojilerinin hızlı ve çoğu

zamanda ücretsiz kullanılması bilgi kirliliğine yol açtığı gibi, fikri mülkiyet ihlalleri benzeri bazı hukuki sorunlara da neden olmaktadır (Kaya, 2009: 23).

Bilişim teknolojileri o kadar hızla gelişmektedir ki, henüz Web 2.0 teknolojileri bir standart haline gelmemişken Web 3.0 teknolojileri gündeme gelmiştir. Geleceğin İnterneti olarak gündeme gelen Web 3.0 da İnternet sayesinde sağlanacak makine etkileşiminden söz edilmektedir. Semantik veya Ontolojik Web (Anlamsal Web) de denen Web 3.0 da, verinin makineler tarafından anlamlandırıldığı ve kontrolün makineler tarafından yapılacağı bir veri paylaşımı söz konusudur. Web 3.0 cihazlar arası etkileşimle İnternetin kendi kendini üreteceği bir Web dünyası olacaktır (Web3event, 2011; Howstuffworks, 2011).

Web 3.0 ile, İnternet üzerindeki tüm bilgileri ve bunların birbirleriyle ilişkilerini makineler de anlayabilecektir. Makineler insan beyni gibi bilgileri hafızaya alacak ve birçok alanda size en uygun olanlarını sunacaktır. Yani kontrol yapay zekalı teknolojilere bırakılacak; üretilen girdileri işleyip anlamlı çıkarımlar yaparak, aynı zamanda bağımsız uygulama ve veritabanları birbiriyle konuşturan uygulamalar bütünü ortaya çıkacaktır (Web3event, 2011; Howstuffworks, 2011).

Web 3.0 tüm arama mantığını değiştirecektir. Semantik Web' kavramı ile yepyeni bir kullanıcı deneyimi yaşanacaktır. Semantik, “araştırmak” ve “gerçek anlamı bulmak” demektir. Semantik Web verilerin doküman içeriğinden ayrıştırılmasını sağlayacak; bu sayede bilgisayar, verilerin semantiğini anlayarak web tarayıcısında arama yapıldığında gerekli bilgileri sunacaktır (Web3event, 2011; Howstuffworks, 2011).

Web 3.0 uygulamalarının ulaşacağı ideal nokta kişiye özel öğrenen akıllı robotlardır. Bu robotlar okuyacak, okuduğunu anlayacak, yorumlayacak; kullanıcıların kişi veya üye olunan grup bazında Web'deki davranışlarına göre mantıksal çıkarımlar yaparak önüne koyacaklar ve tüm bunları saliseler içinde gerçekleştirecektir. Üstelik robotların öğrenme eğrisi, sizden ve İnternet gezintilerinizden bilgi aldıkça çok dik şekilde ivmelenerek artacaktır (Web3event, 2011; Howstuffworks, 2011).

1.2.7 İnternetin Yönetimi

Üzerinde yasal bir otorite veya merkezi bir kural koyucu bulunmadığı için İnternet merkezi bir otorite ve kontrolden uzaktır (Işıklı, 2001: 6-7). Yani, İnternet ağının tamamını kontrol eden tek bir ulusal veya uluslararası otorite bulunmamaktadır (Deibert vd., 2008: 65; Goldsmith and Wu, 2006: 21). İnternetin çok kısa bir sürede yaygınlaşmasını sağlayan ve cazibe merkezi haline gelmesine neden olan temel faktörün bu özelliği olduğu dile getirilmektedir (Kaya, 2009: 9).

İnternet ağının tamamını yöneten tek bir otoritenin olmaması, bu ortamın bütünüyle başıboş ve hukuksuz olduğu anlamı taşımamaktadır. İnternetin yönetimi ve işbirliğinin sağlanması konusunda çeşitli ulusal ve uluslararası kuruluşların işbirliğinden oluşan karmaşık ilişkiler bütününden ve çok aktörlü bir yapıdan söz edilebilir. Zira, özel bir mevzuatı bulunmamakla birlikte İnternet ağının kontrolüne ilişkin ulusal ve uluslararası bazı düzenlemeler vardır (Kaya, 2009: 9; Işıklı, 2001:7).

1.2.7.1 İnternet Yönetimiyle İlgili Kurumlar

İnternet mekanizmalarının yönetimi ve politikaların belirlenmesiyle ilgili çeşitli uluslararası kurumlar görev yapmaktadır. Bu kurumların başlıcaları ele alınacaktır.

1.2.7.1.1 ICANN

1980'lere kadar kullanıcı isim ve adresleri ile tahsis edilen İnternet sayılarının ve isimlerinin listeleri, İnterneti yöneten ABD Savunma Bakanlığı bünyesinde oluşturulmuştur. Bundan sonra isim listesi oluşturma işi giderek yoğunluk kazanınca, sürecin daha kolay ilerlemesi için Alan Adları Sistemi (DNS) geliştirilmiştir. 1990'larla birlikte İnternet üzerinde söz sahibi olmaya başlayan ABD Ulusal Bilim Vakfı (NSF), İnternet alan adı sisteminin kayıt, koordinasyon ve bakım gibi ana fonksiyonlarının yerine getirilmesi işini yaptığı anlaşma ile 1993 tarihinde beş yıl süreliğine Network Solutions Inc.(NSI) adlı şirkete vermiştir. NSI tarafından işletilen kayıt kurumu InterNIC adını taşımaktadır (Canbay, 2005: 18-20; ICANN, 2011b).

İnternetin hızla ticarileşmesi ve küresel olarak yaygınlaşması, özellikle “.com” alanı içindeki kayıt işlemlerinin kısa sürede beklenmedik ölçüde artması, InterNIC tarafından başlatılan ve piyasadaki tekeli kullanarak yeni isim kaydı yapanlardan ücret alma gibi bazı uygulamalarla astronomik karlar elde etmesi, isim hakkı uyuşmazlıklarında daha çok şirketleri kayırıyor olması, İnternet camiasında huzursuzluklara ve çeşitli kesimlerin tepkilerine yol açmıştır (Drissel, 2006: 110).

NSI’nın konumuna karşı artan eleştirilerin bir sonucu olarak 1996 yılında, Alan Adı Sisteminde değişiklik önerileri geliştirmek üzere, IANA (Internet Assigned Numbers Authority-İnternet Tanımlanmış Sayılar Otoritesi), İnternet Topluluğu (Internet Society-ISOC), ITU gibi çeşitli hükümet dışı ve hükümetler arası örgütlerin temsilcilerinden oluşan bir Özel Seçilmiş Uluslararası Komite (Internaitonal Ad-Hoc Committee-IAHC) kurulmuştur. Bu kuruluş, 1997 tarihli raporu ile Alan Adı Sisteminin yönetiminin uluslararası örgütler, iş kesimleri ve ISOC’un temsilcilerinden oluşacak, ITU bünyesinde faaliyet gösterecek ve uluslararası bir antlaşmayla kurulacak olan ulus-üstü, kar amacı gütmeyen bir yapıya devretmeyi önermiştir (Drezner, 2004: 495). İsim hakkı uzlaşmazlıklarını çözmek amacıyla da Dünya Fikri Mülkiyet Örgütü (World Intellectual Property Organization-WIPO) denetiminde yeni bir standart sisteminin kabulü teklif edilmiştir (Drissel, 2006: 110).

IAHC’nin önerisi başta ABD olmak üzere bazı hükümet ve İnternet uzmanlarınca tepkiyle karşılanmıştır. İnternetin yönetimini ITU gibi bir BM kuruluşuna vermeye niyeti olmayan ABD hükümetinin, raporu onaylamayı reddetmesiyle, IAHC’nin çalışmaları sonuçsuz kalmıştır. Ancak, mevcut sisteme yönelik artan eleştiriler nedeniyle sistemde bazı kökten değişikliklere gidilmesi de zorunlu hale gelmişti. Bu ortamda, ABD Ticaret Bakanlığınca yapılmış olan yeni öneriler, Alan Adı Sisteminin bugünkü yönetim şeklinin ilk şablonunu oluşturmuştur (Yeşilyurt, 2007: 3).

ABD Ticaret Bakanlığı ve IANA’nın teklifi ile, alan adı sisteminin sahip olduğu tekeli yapısının değiştirilmesi ve rekabetçi bir yapıya kavuşturulması amacıyla, sistemin özelleştirilmesi, rekabetin artırılması ve uluslar arası katılımın teşvik edilmesi için, 1998 de ICANN (Internet Corporation for Assigned Names and

Numbers-İnternet Tahsisli Sayılar ve İsimler Kurumu) yetkilendirilmiştir (Canbay, 2005: 18-20: ICANN, 2011b). ICANN, ABD'nin California eyaleti hukukuna tabi, ABD Ticaret Bakanlığı tarafından belirlenen esaslara göre faaliyet gösteren, kar amacı gütmeyen ve kamu yararına faaliyet gösteren özerk bir kuruluş olarak 25.11. 1998'de kurulmuş ve Alan Adı Sisteminin yönetimini devralmıştır (Fuller, 2001: 1).

ABD bu süreçte minimum uluslararası düzenleme, maksimum özel sektör öncülüğü ve rekabet ilkeleriyle hareket etmiş, fakat bireysel kullanıcıların İnternetin yönetimine katkısı ilk defa dile getirmiştir. Diğer yandan, yeni kuruluşun özel, kar amacı gütmeyen, kendi kendini düzenleyen, demokratik, şeffaf ve coğrafi olarak farklı yörelerin çıkarlarını yansıtacak yapıya sahip olacağına dair güvenceler verilerek, uluslararası düzenleme fikri tekrar reddedilmiştir (Yeşilyurt, 2007: 3-4).

ICANN'ın görevi, "İnterneti çalıştırmak", İnternet polisliği, sitelerdeki ihlaller, güvenlik, içerik değil, aksine, İnternetin istikrarını sağlamak, merkezi bir koordinasyon gerektiren belirli teknik, idari ve politika geliştirme görevlerini koordine etmektir (Canbay, 2005: 26). İnternet alan adları sisteminin teknik yönetimini, IP adres alanlarının tahsisini, protokol parametrelerinin belirlenmesini ve kök sunucu sistemi yönetimi işlevlerini koordine etmekle ve Alan Adı Sisteminin yönetimiyle görevlendirilmiştir. Kuruluşunu müteakip ICANN, rekabetçi bir alan adları kayıt sistemine geçişi temin etmek için kayıt kurumlarını akredite etmeye başlamıştır. NSI, veri tabanı idarecisi olmaya devam etmektedir (ICANN, 2012b).

ICANN'ın ilk kurulduğu zaman hükümetlere fazla söz hakkı vermeyen ve iş çevreleri ile İnternet kullanıcılarının temsili dengelemeye çalışan bir yapıdaydı. Ancak kuruluşundan sonra örgütün demokratik olamadığı, temsili sağlayamadığı, meşruiyet kaynağının sorunlu olduğu, rekabeti temin edemediği, ABD hükümetine çalıştığı ve diğer hükümetlere söz hakkı tanımadığı ve daha çok şirket çıkarlarını kayırdığı eleştirilerine maruz kalan ICANN, bu yapıda bazı değişiklikler yapmak zorunda kalmıştır. ABD'nin de ICANN'ın mutabakat zaptında belirtilmiş hedeflerin çoğunu yerine getirmediğini belirtmesi üzerine, 2002 Romanya toplantısında ICANN Yönetim Kurulu örgütün yapısını büyük oranda değiştirmiştir (Yeşilyurt, 2007: 5).

Yeni düzenleme ile ICANN’da devletlerin rolü artarken, bireysel kullanıcıların rolü azalmıştır. Burada en çok göze çarpan değişikliklerden birisi, Hükümet Danışma Komitesi (Governmental Advisory Committee-GAC) aracılığıyla ICANN’ın yönetiminde devletlere söz hakkı verilmesi olmuştur. GAC, ülkelerin hükümetleri, çok uluslu kuruluşlar ve uluslararası örgütler tarafından atanmış temsilcilerden oluşmaktadır. Komitenin görevi, hükümetlerin görüşlerini ICANN Yönetim Kuruluna sunmaktır. GAC, hükümetlerin ilgi ve uğraş alanları ile tüketicilerin ilgi alanlarını da kapsayacak şekilde tartışma zemini oluşturacak bir forum gibi çalışmaktadır. Danışma Komitesi olduğu için GAC, ICANN için çalışmak ya da ICANN’ın faaliyetlerini kontrol etmek gibi yasal bir güce sahip olmamakla birlikte, bulgularını ve tavsiyelerini ICANN Yönetim Kuruluna bir raporla bildirmektedir. Yönetim Kurulu, Hükümet Danışma Komitesi tarafından verilen önerileri politika oluştururken göz önünde bulundurmak ve aksi takdirde de hükümetlerin yetkililerini gerekçe konusunda bilgilendirmekle yükümlü kılınmıştır (ICANN, 2012c; 2012d).

Sahip olduğu yetkileri sebebiyle İnternetin tamamını ICANN’ın yönettiği şeklinde bir yanlış vardır (USA Today, 14.11.2005). Bu sebeple, ICANN ilk oluşturulduğu günden beri her zaman eleştirilere ve menfaat çekişmelerine maruz kalmıştır (Fuller, 2001: 1). Halbuki, mali işlemler, İnternet içeriğinin kontrolü, istenmeyen ticari e-postalar ve veri korumasıyla ilgili kurallar gibi İnternet kullanıcılarını ilgilendiren diğer sorunlar, ICANN’ın görevinin dışında kalmaktadır. Buna rağmen, İnternetin hızla gelişmesi, bireylerin, özel sektör/kamu/uluslararası kuruluşların İnternette yer almaya başlamasıyla ve alan adlarının ekonomik değerlerinin artmasıyla, İnternet ve alan adları ile ilgili pek çok sorun ortaya çıkmaya başlamış ve ICANN’a yönelik eleştiriler artarak sürmüştür (Alkan ve Canbay, 2003: 3).

ICANN’ın hukuki meşruiyetinin bulunmadığı, işlemlerinin gizli olduğu, çok yavaş çalıştığı, sorunları çözmekte yetersiz kaldığı, çalışma süreçlerinin ve prosedurlerinin düzgün, kolay ve anlaşılabilir olmadığı, hükümet, endüstri ve İnternet toplumunun tüm paydaşlarını biraraya getiremediği, yeterli mali kaynaklara sahip olamadığı, İnternet toplumundan kopuk olduğu şeklinde yoğun eleştiriler dile getirilmektedir (Alkan ve Canbay, 2003: 3).

1.2.7.1.2 IANA

Dünyadaki İnternet protokol parametrelerinin düzenlenmesi ve koordine edilmesi IANA (Internet Assigned Numbers Authority-İnternet Tanımlanmış Sayılar Otoritesi) tarafından gerçekleştirilmektedir. IANA, ICANN ile koordinasyon içerisinde IP adreslerinin yönetimini gerçekleştirmek için bağımsız olarak faaliyet göstermek üzere ABD Ticaret Bakanlığınca yetkilendirilmiş kurumdur (IANA, 2012a). IANA'nın yetkisi, IP yönetimi için politikalar belirlemekten ziyade önceden belirlenmiş politikaları tarafsız bir şekilde uygulamaya yöneliktir (Kaya, 2010: 11).

IANA, 1972 yılında “Birleşik Devletler Savunma Bilgi Sistemleri Ajansı-US Defence Information Systems Agency“ tarafından kurulmuştur. ABD Hükümeti ile yaptığı sözleşme 1998 yılında dolmasına rağmen günümüzde de IANA, Bölgesel IP Numarası Kayıt Kurumları (Regional İnternet Registrars-RIRs)'na bu sayısal adresleri blok olarak tahsis etmeye devam etmektedir. IANA, IP numaralarının koordinatörlük görevini, ABD Hükümeti ile General Atomic, Amerikan Telefon ve Telgraf Şirketi (AT&T) ve Network Solution firmaları arasında yapılan bir anlaşma ile gerçekleştirmektedir (IANA, 2012b). ICANN'a yönelik dile getirilen uluslararası katılım sorunu IANA için de geçerlidir (Kaya, 2010: 11).

IANA, belirlenmiş politika ve hedefler doğrultusunda, talep etmeleri durumunda RIRs'lara IP havuzundaki IP adreslerinden tahsis etmektedir. RIRs'lar, IP adreslerini adil bir biçimde tahsis etmek, yönetmek ve kontrolsüz gelişimi engellemekten sorumludur (Canbay, 2005: 37). Dünya'da beş tane RIRs vardır:

- 1- ARIN (American Registry for Internet Numbers): Kuzey ve Güney Amerika'da faaliyette bulunur. Merkezi Virginia'dadır (ARIN, 2012).
- 2- RIPE (Reseaux IP Europeens Network Coordination Centre): Avrupa, Ortadoğu ve Orta Asya'da faaliyette bulunur. Merkezi Amsterdam'dadır (RIPE, 2012a).
- 3- APNIC (Asia Pacific Network Information Centre): Asya ve Pasifik bölgesinde faaliyette bulunur. Merkezi Brisbane-Avustralya'dadır (APNIC, 2012).

4- LACNIC (Latin American and Caribbean Internet Addresses Registry):Latin Amerika ve Karaip'te faaliyette bulunur. Merkezi Uruguay'dadır (LACNIC, 2012).

5- AFRINIC (African Network Information Centre): Afrika'da faaliyette bulunur (AFRINIC, 2012).

Bölgesel Kayıt Kurumları IP numaralarını, IANA'dan blok olarak alırlar. NIR (National Internet Registry-Ulusal İnternet Kayıt Merkezi) ve LIR (Local Internet Registry-Yerel İnternet Kayıt Merkezi) olarak isimlendirilen büyük İSS'ları bu bölgesel kurumlara başvurarak IP sayılarını blok olarak alır ve daha sonra aldıkları IP sayısal adreslerini daha küçük servis sağlayıcılara ve nihai kullanıcılara tahsis ederler. Bölgesel Kayıt Kurumları IP numaralarının dağıtımını organize ederken, DNS ile ilgilenmezler. DNS ve IP numarası dağıtım görevleri ayrıdır ve aynı organizasyon tarafından yerine getirilmesi zorunlu değildir (RIPA, 2012b).

1.2.7.1.3 Kök Sunucu Operatörleri

Tüm sorumluluğu ICANN'a ait olmak üzere İnternet trafiğini düzenleyen toplam 13 kök sunucu bulunmaktadır. Bu sunucuları ICANN tarafından akredite edilmiş farklı kurumlar yönetmektedir (Canbay, 2005: 13). Kök sunucular veri güvenliğinin sağlanması için düzenli olarak birbiriyle senkronize olmakta ve bu süreçte A Kök Sunucu kayıtları esas alınmaktadır. A kodlu sunucu ana kök sunucudur ve tüm veriler burada toplanmaktadır. Diğer kök sunucular bu sunucudaki verilerle veritabanlarını hergün güncellemektedir. Kök sunucular, kaliteli, verimli ve güvenilir hizmet sunmakla yükümlüdür (Canbay, 2005: 13). ABD'nin tüm kök sunucuların yönetimi üzerindeki etkisi nedeniyle, ICANN ve IANA için yöneltilecek uluslararası katılım eleştirileri kök sunucu yönetimi için de dile getirilmektedir (Kaya, 2010: 11).

1.2.7.1.4 Diğer Kurumlar

Tüm bu kurumlar dışında, 1986 yılında oluşturulan ve İnternetin geliştirilmesi ve protokol mühendisliği alanlarında hizmet vermekte olan IETF (Internet Engineering Task Force-İnternet Mühendisliği Çalışma Gücü) ve bu grubun alt çalışma grupları

olan IAB (Internet Architecture Board-İnternet Mimarisi Kurulu) ile IESG (Internet Engineering Steering Group-İnternet Mühendisliği Yönetim Grubu), IRTF (Internet Research Task Force-İnternet Araştırmaları Çalışma Gücü), 1991 yılında İnternete resmi bir yapı sağlamak ve İnterneti geliştirmek üzere kurulmuş olan ISOC (Internet Society-İnternet Topluluğu) ve World Wide Web Consortium gibi kurumlar İnternet ile ilgili temel politikaların belirlenmesine yardımcı olmakta ve bu alanda çeşitli araştırma-geliştirme çalışmaları yapmaktadırlar (Kaya, 2010: 11).

1.2.7.2 İnternetin Uluslararası Yönetim Sorunu ve İnternet Yönetişi

Bugün İnternetin ciddi bir uluslararası yönetim sorunu vardır. Keza, bu sorun ve bununla ilişkili olarak İnternet yönetişi konusu, İnternetin düzenlenmesi konusunun en önemli parametrelerinden birisini oluşturmaktadır.

1.2.7.2.1 İnternetin Uluslararası Yönetim Sorunu

İnternetin kullanım alanlarının artması, hızla gelişmesi ve yaygınlaşması, bireylerin, özel/kamu/uluslararası kuruluşların İnternette yer almaya başlamasıyla İnternetle ilgili pek çok sorun belirmiştir. Bu sorunların başında İnternetin güvenliğinin, güvenilirliğinin ve istikrarının sağlanması, telif hakları, zararlı içeriğin denetimi, veri gizliliği ve güvenliği, kültürel ve dilsel çeşitliliğin sağlanması ve tüm bunlarla ilişkili olarak İnternetin uluslararası yönetimi gelmektedir (Alkan ve Canbay, 2003: 3).

Bu çerçevede, İnternet üzerinden gerçekleştirilen elektronik ticaretin milyarlarca dolarlık bir hacme ulaşması, alan adlarının değerlendirilmesi ve çeşitli telif hakkı ihlallerine yol açması ve İnternet üzerinden veri iletişiminin ulusal güvenliğin bir parçası olarak görülmesi gibi nedenlerle alan adları ve IP adreslerinin yönetimi büyük bir menfaat çatışması ve mücadeleye konu olmaktadır (Canbay, 2005: 20). Öyle ki, İnternet üzerinde söz sahibi olma, alan adları ve IP numaralandırma politikalarını belirleme ve kontrol etme sorunu sadece devletler ve özel sektör arasındaki bir ihtilaf olarak değil, devletlerarası bir menfaat ve ideoloji sorunu olarak değerlendirilmektedir (Kaya, 2010: 12).

Dolayısıyla, hangi ülkeye ne kadar IP adresi tahsis edileceği, hangi IP adresi aralıklarının kullanılabileceği, hangi alan adlarının hangi şartlarda kayıt edilebileceği, hangi üst-düzey alan adlarının oluşturulacağı ve onları kimin kontrol edeceği gibi konular, telefon numaralarının veya trafik plakalarının tahsis edilmesi gibi basit bir teknik sorun olarak görülmemektedir (Goldsmith and Wu, 2006: 31).

Diğer yandan, devletler, İnternetin yaygınlaşmasıyla, İnternetin sosyal, siyasal ve ekonomik hayatı yönlendiren etkili bir araç olduğunun farkına varmışlar ve her biri farklı bir iç dinamikten dolayı İnternet üzerindeki etkilerini ve etkinliklerini hem ulusal hem de uluslararası ölçekte artırmaya çalışmaktadır (Kaya, 2010: 12). Fakat, uluslararası hukukta, devletlerin İnternet üzerindeki hakimiyetleri okyanuslar, hava ve uzay gibi evrensel kaynaklar ile ilgili egemenlik tartışmalarına benzetilerek (Goldsmith and Wu, 2006: 171), bu gibi evrensel kaynakların hukuki statüsü konusunda egemenlik ilkesinden hareket edilmediği; devletlerin iktisadi ve bilimsel gelişme derecesi ne olursa olsun, bu kaynaklardan yararlanma konusunda tüm devletlerin kullanım hakkının bulunduğu kabul edilmekte ve egemenlik hakkından ziyade yararlanma hakkı üzerinde durulmaktadır (Toluner, 1996: 49).

Bunun yanında, siber uzayın mimarisinin bu teknolojileri geliştiren ve üreten devletlerin politikaları doğrultusunda şekillendiği de bir gerçektir. Zira, büyük oranda, teknoloji üreten ülkelerin özel ve kamusal güçleri bu alanın sınırlarını ve kurallarını belirlemektedir. Bu kurallar, çoğu zaman diğer devletler ve kullanıcılar tarafından istemsiz bir biçimde de olsa kabul edilmektedir. Keza, kurgulanan mimari üzerine inşa edilen uygulamalar, mimari tarafından izin verildiği ölçüde başarılı olmakta veya uygulanma imkanı bulmaktadır. Bu nedenle siber uzayın temel mimarisini şekillendirenlerin bu alanın regüle edilmesinde baskın güç olduğu söylenebilir. Dolayısıyla, devletler çoğu zaman, kendi başlarına yaptıkları düzenlemelerde egemen güç olarak değil, ikincil uygulamaların yapılmasını gözeten etkin olmayan bir denetleme organı olarak hareket etmektedir (Lessig, 1998: 8-11).

Bununla birlikte, İnternet trafiğinin farklı ülkeleri saniyeler içerisinde geçerek akması, bu karmaşık yapı içerisinde bir noktadaki bir sorunun dünyanın çok uzak bir

noktasındaki İnternet trafiğini olumsuz yönde etkileyebilme özelliği, web sitelerini barındıran sunucuların dünyanın her tarafına yayılmış bulunması, genel veya bölgesel İnternet noktalarının kontrolü, bakımı, hatların sayısının artırılması gibi nedenler İnternetin işlerliğinin devamı için tüm devletlerin aktif katılımını, uluslararası işbirliği ve koordinasyonu zorunlu kılmaktadır (Kaya, 2010: 12).

Bununla birlikte, İnternetin kötüye kullanılmasını önlemek amacıyla ulusal politikaların oluşturulması ve sürdürülmesi, bu politikaların uluslararası düzeydeki gelişmeler ışığında birleştirilmesi ve koordinasyonunun sağlanması bakımından devletlerin rolü önemlidir. Bu çerçevede, her bir devletin İnternet üzerinden işlenen suçlarla mücadele etmesi ve kötüye kullanılmasının önüne geçmeye çalışması için kendi egemenlik alanında üzerine düşeni yapması gerekmektedir (Akdeniz, 2003: 51-54). Bu mücadele hem devletlerin hem de uluslararası toplumun menfaatinedir. Aksi durumda, bazı devletler İnternet suçları için odak haline gelmekte ve dolayısıyla İnternet güvenliği için tehdit oluşturarak İnternete olan güveni zedelemektedir (Kaya, 2010: 13).³⁰

Buna mukabil, İnternet ortamı fiziki bir coğrafya ile sınırlı olmadığı için, ulusal yasalarla bu sorunu çözmek, bu olumsuzluklara engel olmak, gerçek sorumluları veya suçluları bulmak ve cezalandırmak çoğu zaman mümkün olmamaktadır. Bu nedenle, bu sanal ortamın zararlı tesirlerinden korunmak ve “serbest suç işleme bölgelerinin” oluşmasını engellemek için uluslararası işbirliği ve her ülke için geçerli olacak yeknasak kurallar gerekmektedir (Günaydın, 2010: 103). Zira, İnternetin kötüye kullanılmasını önlemeye çalışan ve yaptırım uygulamaya yetkili merkezi bir otoritenin bulunmaması, İnternetin küresel ve merkezi olmayan yapısının getirdiği en önemli sorunlardan birisidir (Sınar, 2001: 30). Bu konuda devlet düzenlemeleri sorunları çözmede yeterli olamamakta; ulusal düzeydeki politikaların geliştirilmesinde uluslararası yetki konularının dikkate alınması ve uluslararası işbirliği gerekmektedir (Akdeniz, 2003: 49).

³⁰ Örneğin siber suçlar için kullanılan çeşitli yazılımların en çok barındırıldığı ülke olan Çin, bu yönüyle ön plana çıkmaktadır. Bkz. MSNBC, **The top countries for cybercrime**, <http://www.msnbc.msn.com/id/19789995/> (09.12.2012)

Dolayısıyla, İnternetle ilgili uluslararası düzenlemeler yapılmasının gereği ortadadır. Ulus devletlerin bu düzenlemelere bağlı olmaları ve kendilerine ait olan yetkileri bu alandaki uluslararası yapılarla paylaşmak zorunda bırakılmaları ulusal egemenliğin kısıtlandığı tartışmalarına neden olsa da, bu sorunu çözmenin yolu, İnternet yönetimiyle ilgili uluslararası düzenleme ve kararların dengeli, adil, makul ve kabul edilebilir niteliklere sahip olmasından geçmektedir. Bunun temin edilebilmesi ise, düzenleme ve karar alma süreçlerinde hükümetleri etkin konuma getirmekle mümkün olacaktır (Alkan ve Canbay, 2003: 6).

Lakin, mevcut durum bunu temin etmekten uzak gözükmektedir. Günümüzde İnternetin yönetiminde önemli iki kurum olarak ortaya çıkan ICANN ve IANA'nın yapılanma şekillerinin ve karar alma süreçlerinin İnternet politikalarının tarafı oluşmasına neden olduğu görülmektedir (Preston, 2008: 2). ICANN ve IANA devlet müdahalesi olmaksızın İnterneti düzenleyecek ve tüm aktörleri arasında etkileşimi sağlayacak bağımsız kurumlar olma iddiasıyla oluşturulmuştur. Fakat bağımsız olamamış ve ABD Ticaret Bakanlığı'nın bir parçası olmaktan kurtulamamıştır (Goldsmith and Wu, 2006: 169; Preston, 2008: 2). Nitekim, bunun bariz bir örneğini, tüm kök sunucular üzerinde ve özellikle verileri tüm kök sunucular tarafından temel değer olarak alınan A Kök sunucusu üzerindeki ABD'nin mutlak hakimiyetinde görmekteyiz. Öyle ki bu durum devletlerin kendi üst düzey ülke alan adları üzerinde bile söz ve hak sahibi olmalarına engel olmaktadır (Kaya, 2010: 13).

ICANN ve IANA'nın uluslararası bir kuruluş olmaması ve hükümetlerin bu kuruluşların çalışmalarında yeteri kadar yer almaması, bu kuruluşlar açısından meşruiyet tartışmalarına neden olmaktadır. Özellikle ICANN üzerindeki mevcut ABD etkisi sebebiyle, bu kuruluş tarafı, gayrimeşru ve rekabet bozucu olmakla ve İnternet kullanıcılarının gerçek temsilcisi olmamakla suçlanmaktadır (Arx, 2003: 1).

Ayrıca, kök sunucuların sorumluluğunun ICANN'da bulunmasına karşın hayati önem taşıyan bu sunucuların farklı şirketler tarafından kontrol edilmesi, Avrupa ve Uzak Doğu ülkeleri başta olmak üzere değişik ülkelerin ICANN'dan kök sunucuların düzenli çalışması ve güvenliği konularında garanti istemesine neden olmaktadır.

Devletlerin katılım taleplerine olumsuz bakan ICANN, kök sunucuların düzenli çalışması ve güvenliği konusunda devletlere güvence vermeyi de reddetmektedir. ICANN'ın taşıdığı sorumluluğa karşılık bunu anlaşmalarla kağıda dökmekteki isteksizliği, devletlerin şiddetli eleştirilerini haklı kılmaktadır (Canbay, 2005: 31).

Bu nedenler, söz konusu kuruluşların çalışmalarının dünya çapında uygulanabilir ve etkin olmasını engellediği gibi, bütün çağrılara rağmen hükümetlerin bu kuruluşların çalışmalarına rağbet etmemesine de sebep olmaktadır. İnternetin gelişimiyle ortaya çıkan ve yukarıda ifade edilen sorunlarla mücadele etmesi istenen hükümetlerin İnternetin uluslararası yönetiminde etkili olamamaları bu isteksizliği körüklemektedir. Bu itibarla, ICANN'ın tek bir hükümetin kontrolünde gayriresmi yapısından kurtarılarak tüm yetkilerinin bağımsız bir uluslararası örgüt tarafından gerçekleştirilmesi talep edilmekte ve tüm hükümetlere açık uluslararası meşruiyeti olan bir kuruluşa dönüştürülmesinin gerektiği dile getirilmektedir (ITU, 2003a).

Tüm bu eleştirilere rağmen ABD, ICANN'ın yönetiminin teknik bir sorun olduğunu ve özerk yapısının devam etmesi gerektiğini savunarak, başka devletlerin müdahalesinin gereksiz olduğunu iddia etmektedir. Buna karşılık, İnternetle ilgili politikaların görünürde bağımsız ama gerçekte ABD'nin etkisindeki ICANN tarafından belirlenmesinin ABD'nin siyasal sorumluluktan kaçmasını sağladığı görüşü de dikkat çekmektedir (Fuller, 2001: 2).

Nitekim, sorunun ABD'nin iddia ettiği gibi basit bir teknik düzenleme olmadığına en çarpıcı örnek olay, 2007 yılında, pornografik içerikli web sitelerinin diğer İnternet içeriğinden ayrılması için ICM Registry Inc. şirketince ICANN'a “.xxx” üst düzey alan adının oluşturulması önerildiğinde yaşanmıştır (ICANN, 2007). Bu teklif ile “.xxx” üst düzey alan adının oluşturulmasının, pornografik içeriğin diğer İnternet içeriğinden ayrılmasına ve daha kolay filtrelenmesine, çocuk pornografisinin kolay takibine ve aynı zamanda pornografik içeriğe erişmek isteyen yetişkinlerin oluşturulacak gizlilik politikaları sayesinde korunmasına hizmet etmesi düşünülmekteydi (Preston, 2008: 2). Ancak, söz konusu üst düzey alan adının oluşturulması, ABD'nin yaptığı müdahaleler sonucu, gerekli kamuoyu desteği

sağlanamadığı gerekçesiyle uzun bir süre askıya alınmıştır. Dünyanın en büyük pornografi sektörüne sahip ülkenin ABD olduğu göz önüne alındığında, söz konusu müdahalenin nedeni kolayca anlaşılmaktadır. Bu olayda ABD, kendi ekonomik menfaatleri olumsuz etkilenmemesi için uluslararası toplumun istek ve çıkarlarını gözardı etmiştir (Kaya, 2010: 15).

ABD, İnternet üzerindeki hakimiyetini ve yönetimi ile ilgili sahip olduğu yetkilerini elinde tutmak istemekte, hatta İnternet üzerindeki yetkilerini daha da artırmak için çeşitli girişimlerde bulunmaktadır. Askeri iletişim stratejisinin bir parçası olarak ortaya çıkardığı İnterneti, güvenlik stratejisinin bir parçası olarak kullanmaya devam etmekte ve bu nedenle İnternet üzerindeki egemen konumunu korumayı ekonomik ve ulusal güvenlik menfaatleri için gerekli görmektedir (Kaya, 2010: 13).

ABD tarafından keşfedilerek kullanılmaya başlanması nedeniyle İnternet üzerindeki ABD etkinliği belirli bir süre ve ölçüde makul karşılanabilirse de, artık küresel hale gelen ve kullanıcılarının büyük çoğunluğu ABD dışında bulunan İnternetin, yönetim boyutuyla da küresel ölçekte düşünülerek, uluslararası hale getirilmesi ve hükümetlerin yönetim süreçlerinde yer almalarının sağlanması gerekmektedir (Alkan ve Canbay, 2003: 6).

İnternetin önemli bir ticari potansiyel taşıması ve kritik iletişim alanlarında kullanılması, devletlerin gizlilik politikalarına ve ulusal güvenliklerine karşı tehditler barındırması ve üçüncü dünya ülkelerinin mevcut İnternet yönetim politikaları sebebiyle İnterneti az veya sınırlı bir şekilde kullanmaları ve İnternet konusunda neredeyse hiç söz sahibi olmamaları sebebiyle ABD'ye yönelik eleştiriler giderek artmıştır. Başta AB olmak üzere uluslararası toplum, İnternet üzerindeki ABD etkisinin kırılması ve İnternet politikalarının belirlenmesine daha etkin bir şekilde katılmak için çeşitli girişimlerde bulunmuştur (Arx, 2003: 7). Bu süreçte İnternet yönetimi kavramı gündeme gelmiştir.

1.2.7.2.2 İnternet Yönetimi

İnternet yönetiřimi konusu 1990’larda Alan Adı Sistemi’nin yönetimi tartiřmaları ile bařlamıř, fakat zamanla teknoloji, ekonomi, soyso-kültürel boyut, politika gibi farklı alanları da içerecek řekilde, dünyadaki tüm ölkelerin konuya daha fazla dahil olması ile řekillenmeye devam etmiřtir (Yeřil ve Alkan, 2007).

İnternet üzerindeki ABD etkisinin kırılması konusundaki giriřimlerin ilk mecrası ITU koordinasyonunda düzenlenen Dünya Bilgi Toplumu Zirveleri(WSIS)dir. Bu zirveler, Alan Adı Sistemi’nin idaresi ve ICANN’ın en geniř anlamda ve uluslararası olarak tartiřıldıđı ilk platform olması hasebiyle, genel olarak devletlerin, mevcut sisteme ve ABD’ye bir tepkisi olarak deđerlendirilebilir. WSIS, aynı zamanda BM’in de İnternet yönetiřimi tartiřmalarına müdahil olmaya bařladıđının bir göstergesi olarak, ilki 2003’de Cenevre’de, ikincisi de 2005’de Tunus’ta gerçekleřtirilmiřtir. Dünyanın dört bir yanından hükümet temsilcilerinin katıldıđı WSIS’in İnternet yönetiřimi tartiřmalarını uluslararasılařtırdıđını söyleyebiliriz (Yeřilyurt, 2007: 6).

2003’te Cenevre’de gerçekleřtirilen ilk WSIS’de, İnternet yönetiřimine deđinilmiř ve en önemli tartiřmalar, geliřmekte olan ölkeler ve geliřmiř ölkeler arasında İnternet yönetiřimi kavramının tanımı, ne derece kamu politikası öđesi içerdıđı ve geliřmekte olan ölkelerin küresel İnternet politikalarının oluřum sürecine katılımı konularında yařanmıřtır (Peake, 2004: 3-9). Zirvede, İnternet yönetiřimiyle ilgili çalıřmalar yapmak ve sonraki zirveye öneriler sunmak üzere, geliřmekte olan ve geliřmiř ölkelerden hükümetlerin, özel sektörün ve sivil toplumun katılımıyla bir İnternet Yönetiřimi Çalıřma Grubu (WGIG) oluřturma kararı alınmıřtır (ITU, 2003b).

Zirve’nin sonunda yayınlanan Deklarasyonda İnternet ile ilgili politikaları belirleme konusunun ölkelerin egemenlik haklarından olduđu belirtilerek, İnternet yönetiřiminde hükümetlerin rollerine, diđer aktörlere kıyasla birinci derecede vurgu yapılmıřtır. İnternetin idaresinin hükümetlerin tümünün, özel sektörün, STK’larının ve uluslararası örgütlerin katılımıyla çok taraflı, řeffaf ve demokratik bir biçimde gerçekleřtirilmesi gerektiđi üzerinde durulmuř ve adil bir kaynak dađılımının sađlanması, herkesin kendi dilinde eriřiminin kolaylařtırılması ve İnternetin istikrarlı ve güvenli řekilde çalıřmasının gerektiđi belirtilmiřtir (ITU, 2003b).

WGIG'in, 2005 nihai raporunda İnternet yönetişimini, "devletler, özel sektör ve sivil toplum tarafından, ilgili roller doğrultusunda, İnternetin kullanımını ve evrimini şekillendiren paylaşılmış ilkelerin, normların, kuralların, karar verme süreçlerinin ve programların geliştirilmesi ve uygulanması" olarak tanımlanmıştır (WGIG, 2005: 4).

WGIG Raporu, İnternet yönetişimine ilişkin olarak ele alınması gereken konuları dört ana başlık altında toplamıştır: *İnternet Altyapısı ve Kritik Kaynakların Yönetimi* (Telekomünikasyon altyapısı, genişbant erişim, teknik standartlar, alan adlarının, IP adreslerinin, kök sunucuların yönetimi gibi konular), *İnternet Kullanımına İlişkin Hususlar* (Spam, siber güvenlik, siber suçlar, şebeke güvenliği, bilgi sistemlerinin güvenliği, kritik altyapının korunması, sınırlar arası koordinasyon gibi konular), *İnternetten Daha Geniş Etki Alanlarına Sahip Hususlar* (Rekabet politikaları, özelleştirmeler, fikri mülkiyet hakları, e-devlet, e-ticaret, elektronik kimlik doğrulama, kanunsuz içerik, tüketicilerin korunması, bilginin özgürce akması, kişisel verilerin korunması gibi konular), *Gelişim Boyutu* (Evrensel hizmet, ulusal altyapıların geliştirilmesi, kiralık hatların maliyetleri, eğitim, insan kaynağı niteliğinin geliştirilmesi, kültürel çeşitlilik gibi konular) (WGIG, 2005: 5).

Hükümet, özel sektör ve sivil toplumun İnternet yönetişimindeki rol ve sorumluluklarını ayrı ayrı sayan rapor, İnternet yönetişiminin geleceğine ilişkin olarak dört farklı model geliştirmiştir (WGIG, 2005: 8-16):

1. Hükümetlerin belirleyici olacağı, özel sektör ile sivil toplumun ise sadece tavsiye verici konumda bulunacağı, ICANN'ın yaptığı görevlerle birlikte, spam, güvenlik, siber suçlar, sözleşmeler, çok dillilik, maliyet temelli bağlantı ücretleri ve uyuşmazlık çözümü gibi tüm konuları uhdesinde bulunduracak ve ICANN'ın üzerindeki ABD gözetiminin yerine geçecek Küresel İnternet Konseyi (Global Internet Council-GIC) adında bir BM kuruluşunun oluşturulması.
2. İnternet yönetişimi konularının resmi bir şekilde tartışıldığı bir İnternet Forum'u olarak ICANN'da mevcut bulunan Hükümet Danışma Komitesi'nin güçlendirilmesi ve bunun katılımcı saydam mekanizmalarla desteklenmesi.

3. Bir Uluslararası İnternet Konseyi (International Internet Council-IIC) kurularak, ICANN ve IANA üzerinden ABD Ticaret Bakanlığı'nın yetkilerini devralması ve İnternet yönetişiminin kamu politikalarına ilişkin yönleriyle ilgilenmesi. Konsey'de hükümetlerin belirleyici olması, özel sektör ile sivil toplumun ise tavsiye verici konumda bulunması ve ICANN'ın rolünün daha dar bir teknik düzeye indirilmesi.

4. Üç yeni örgütten oluşan bir yapı kurulması. İlk örgüt, hükümet temsilcilerinden oluşacak, özel sektör ile sivil toplumun sadece gözlemci olarak bulunacağı ve İnternet'e ilişkin kamu politikalarının tartışılacağı Küresel İnternet Politikalar Konseyi idi. İkinci örgüt ise, teknik ve ekonomik konulara bakacak ve ICANN'ın yerini alacak olan BM bünyesinde yapılandırılacak Dünya İnternet Tanımlanmış Adlar ve Sayılar Kuruluşu idi. Bu örgütte özel sektör belirleyici, hükümetler ve sivil toplum gözlemci/danışman statüsünde olacaktı. İnternete ilişkin kamu politikaları konusunda koordinasyon ve tartışma platformu olacak Küresel İnternet Yönetişimi Forumu (The Global Internet Governance Forum-GIGF) ise üçüncü örgüttü. Burada hükümetler, özel sektör ve sivil toplum eşit konumda bulunacaktı.

Genelde devletler ağırlıklı ve sivil toplumun rolünü simgesel düzeyde bırakan bu modellerde, sadece daha eşitlikçi bir devletlerarası sistem tasarlanmaya çalışılırken, bireysel kullanıcılara hiç bir özel atıfta bulunulmaması dikkat çekmektedir(Yeşilyurt, 2007: 8). Ayrıca WGIG Raporu, İnternete ilişkin alan adından, IP dağıtımı, siber suçlardan, spama, ifade özgürlüğünden, veri güvenliğine, çok dillilikten, politika geliştirmeye kadar pek çok konuda uzlaşmayla ulaşılmış ve büyük çoğunluğu makul sayılabilecek kısa ve öz birçok önerilerde bulunmaktadır (Akgül, 2011).

WSIS'in ikincisi 2005 Kasımında Tunus'ta gerçekleşmiştir (ITU, 2012). Zirve, İnternet yönetişimi tartışmalarının gölgesinde kalmıştır (USA Today, 16.11.2005). Bu tartışmaların bir tarafında, mevcut sistemin istikrarı sağladığını ve sürdürülmesi gerektiğini savunan ve hükümetler ya da BM kontrolüne karşı çıkan ABD hükümeti ve ICANN yer alırken, diğer tarafında, WGIG raporu kapmasında temsil kabiliyeti olan uluslararası yeni bir yönetim yapılanması gerektiğini savunan gelişmekte olan ülkeler ve AB yer almaktaydı(Yeşilyurt, 2007: 8). Zirve'ye AB, alan adı yönetiminin

ICANN ve ABD Ticaret Bakanlığı'ndan BM nezdindeki bir ihtisas kurumuna aktarılmasını içeren radikal bir öneriyle gelmiştir (Goldsmith and Wu, 2006: 171).

Tartışmaların sonunda, iki tarafı da az çok tatmin edecek bir ara formül bulundu ve İnternet'in günlük idaresinin olduğu gibi devam etmesi kararlaştırılırken, Brezilya hükümetinin önerisiyle, İnternet yönetişimine ilişkin birçok konunun kapsamlı bir şekilde tartışılacağı çok taraflı, çok çıkar sahipli (multi-stakeholder), demokratik ve şeffaf bir uluslararası forumun oluşturulmasına karar verildi (ITU, 2005). Böylece bir yandan, ABD radikal bir değişikliğin önüne geçmiş olurken, diğer yandan, gelişmekte olan ülkeler ile AB, seslerini daha iyi duyurabilecekleri ve İnternetin kontrolünü elinde tutan ABD üstünlüğünün zayıflatılmasında önemli bir aşama olarak algıladıkları bir platformun oluşturulmasını sağlamıştır (Yeşilyurt, 2007: 8).

Zirve kararları, bunların yanında, İnternet yönetişimi kavramına siyasi, sosyal, ekonomik ve teknik boyutlarıyla kapsamlı bir şekilde yaklaşarak, konuyla ilgili gördüğü, siber güvenlik kültürü, istenmeyen e-postalar (spam), gizlilik, ifade hürriyeti, İnternetin kötüye kullanımının ve terörizmin önlenmesi, elektronik ticaretin teşvik edilmesi, tüketici haklarının korunması, uluslararası bağlantı ücretlerinin düşürülmesi, erişimin önündeki engellerin kaldırılması, İnternet üzerinden eğitimin desteklenmesi, çok dilliliğin teşvik edilmesi gibi birçok konuda hükümetleri harekete geçmeye davet etmiştir (ITU, 2005: md. 39-58).

WSIS Tunus Zirvesi'nde kararlaştırılan ilk İnternet Yönetişimi Forumu (IGF) 30.10-02.11.2006 tarihlerinde Atina'da gerçekleştirilmiştir. Herhangi bir kural koyma yetkisi olmamasına rağmen IGF, ulusal heyetleri, uluslararası örgüt temsilcilerini, ticari şirketleri, hükümet dışı kuruluşları ve bireysel kullanıcıları tek bir tartışma platformunda buluşturması yönüyle önemli bir işlevi yerine getirmiştir. Forumdaki tartışmalar ICANN ile sınırlı kalmamış, bir bütün olarak İnternet olgusu birçok boyutlarıyla daha geniş bir çerçevede ele alınmıştır (Yeşilyurt, 2007:10).

Bugün de İnternet yönetişimi tartışmaları kapsamında ICANN tarafından yürütülmekte olan çalışmaların BM'ye bağlı uluslararası özel uzmanlık kuruluşu olan

ITU'ye devredilmesi fikri ciddi destek görmektedir. Teknik ve idari birikime sahip, hükümet-endüstri-sivil toplum ortaklığını kurmayı başaran, oturmuş ve kolay anlaşılabilen çalışma sistemi ve prosedurleri olan, ekonomik kaynaklara sahip, ICANN'ın ilgilendiği sorunlarla ilgili ileri düzeyde çalışmalar yapmış olan ve en önemlisi meşruiyet sorunu olmayan ITU'nun İnternetin geleceği ve gelişimi açısından bir fırsat olacağı değerlendirilmektedir (Canbay, 2005: 199-200).

Böylelikle İnternetin güvenilir ve nitelikli bir kuruluşa emanet edileceği, kullanıcılarına ek maliyetler çıkarılmamış olacağı ve İnternet alan adlarının tahsisi ve diğer çalışmalardan elde edilecek gelirlerin az gelişmiş ve gelişmekte olan ülkelerde İnternetin geliştirilmesi ve yaygınlaştırılmasına kullanılabileceği ifade edilmektedir. Ayrıca, İnternet yönetiminin ITU'ya devrinden sonra ICANN'ın, ABD Ticaret Bakanlığı ile yapmış olduğu anlaşma çerçevesinde ABD de aynı fonksiyonları yürütmeye devam edebileceği belirtilmektedir (Alkan ve Canbay, 2003: 8).

Diğer taraftan, İnternet yönetiminin BM'e bırakılması teklifine de çeşitli eleştiriler getirilmektedir (Arx, 2003: 7). İnternet yönetiminin BM'e bırakılmasının bürokrasiyi artıracığı ve bunun da İnternet gibi dinamik bir yönetim gerektiren bir alanın işlerliğini tehlikeye sokacağı endişesi bunlardan birisidir (Csmonitor, 2005). Keza, İnternet yönetiminin BM'e ek mali külfet getireceği ve BM'in bunu tüm devletlere adil bir şekilde yansıtmakta zorlanacağı belirtilmektedir. Tüm bunların yanı sıra, BM'in mevcut yapılanmasında kararları veto yetkisine sahip Güvenlik Konseyi'nin beş daimi üyesinin (Amerika, Çin, Fransa, İngiltere ve Rusya) bulunmasının, diğer ülkelerin aleyhine bir durum oluşturduğu belirtilerek, aynı dengesizliğin İnternet politikalarına da yansıtacağı kaygısı dile getirilmektedir (Kaya, 2010: 15).

Bu noktada İnternet yönetişimi ile ilgili olarak ortaya çıkan ve sorun olarak dile getirilen bir başka olgu da, en geniş anlamıyla sivil toplumun ve özellikle bireysel İnternet kullanıcıların İnternet yönetişimindeki rollerinin giderek azalmasıdır. Bu grupların, ICANN Yönetim Kurulundaki belirleyici rollerinin 2002'den itibaren sona erdirilmesi yanında, 2003'ten itibaren sürmekte olan WSIS sürecinde devletlerin İnternet yönetişimindeki en önemli aktörler olarak hak ve çıkarlarının birinci sırada

vurgulanıp, daha sonra, adeta görüntüyü kurtarmak amacıyla araya bir “sivil toplumun katılımının sağlanması” maddesinin eklenmesi bu olgunun en bariz göstergesidir. Eğer tek bir hükümetin (ABD) gözetimi altında özel sektör öncülüğünü simgeleyen mevcut sistem sivil toplumun İnternet yönetişimine katılımı için yeterli olanakları sağlayamıyorsa, dünyadaki bütün devletlerin eşitlikçi bir temelde temsilini sağlasa dahi, kurulacak devletlerarası bir yapılanmanın, sivil toplum katılımı için mevcut yapılanmadan daha iyi imkanlar sunacağı şüphelidir (Yeşilyurt, 2007: 11).

Diğer bir görüşe göre ise, İnternetin kimin tarafından yönetildiğinden ziyade nasıl yönetildiğine odaklanılması gerekmektedir (Kaya, 2010: 15). Yönetimden beklenen tarafsızlığın sağlanması (Akdeniz, 2003: 35), İnternet ile ilgili karar verme sürecinin ilgililerin katılımına açık olması, ticari hayatın gerekliliklerinin göz önünde bulundurulması, düzenlemelerin şeffaf ve öngörülebilir olması ve karar vericilerden hesap sorulabilirliğin temin edilmesidir (Fuller, 2001: 6). Tüm bunlar yapılırken, İnternetin teknik işlerliğine öncelik verilmesi ve yönetimin teknik, politik ve yapısal olarak pratik ve İnternetin doğasına uygun olması, düzenlemelerin engelleyici değil, İnternetin yaygınlaşmasını teşvik edici olması gerekmektedir (Kaya, 2010: 17).

Sonuç olarak, ortaya çıkışından bu yana yaşanan süreçte, İnternetin ekonomik, sosyal ve siyasi boyutlarının ve ne derece önemli bir kaynak olduğunun farkına varan devletler, onun tek bir ülkenin yahut içinde söz haklarının sınırlı olduğu tek bir kuruluşun gözetimi altında kalmasına direnmektedirler. Nitekim İnternet yönetişimi tartışmalarının temelinde de bu konu ön plana çıkmaktadır. Ancak, bu gün için henüz devletlerin İnternet yönetişimi konusunda gittikçe artan taleplerini tatmin edecek düzeyde bir yapılanmaya gidilebilmiş değildir. ICANN, ABD’nin uluslararası sistemdeki egemen konumu sayesinde varlığını hala sürdürmektedir. Mevcut yapının veya ICANN’ın radikal bir dönüşüme uğramasının ancak ABD’nin uluslararası sistemdeki bu konumunun değişimine bağlı olduğu bilinmekle birlikte, uluslararası baskıların zaman içinde köklü değişikliklere yol açabileceği ya da en azından yakın gelecekte söz konusu kurumda çeşitli yeniden yapılanma girişimlerinin gerçekleştirilebileceği beklenebilir (Yeşilyurt, 2007: 10).

Görüldüğü gibi, tezin temel hipotezinde “İnternetin kendine özgü yapısı ve özellikleri” vurgusu ile yasadışı ve zararlı içeriklerle mücadeleyi “zorlaştırıcı ve sınırlandırıcı engeller” ifadesinde karşılığını bulan İnternetin uluslararası yönetimi ve işbirliği konusu, içerik düzenlemesine ilişkin sorunun en kritik faktörlerden birisini oluşturmaktadır. Nitekim, bu kritik faktöre ilişkin olarak yukarda yürütülen tartışmalar ve değerlendirmeler, temel hipotezi destekleyen ve güçlendiren beşinci alt hipotezimizin haklılığını ortaya koymaktadır.

Zira, tartışmalar, İnternetin, mevcut egemen güçler tarafından oluşturulan temel mimarisi ve buna uyumlu karmaşık, merkezi kontrolden uzak uluslararası yönetsel yapısının; kötüye kullanılmasını önlemeye yönelik yönetim temelli kararların alınmasını ve uluslararası ölçekte içerik düzenlemelerine gidilmesini ve bu konularda işbirliği yapılmasını önemli ölçüde zorlaştırmakta olduğunu ve hatta imkansız hale getirdiğini göstermektedir. Bu ise, ulusal sınırları tanımayan küresel bir ağ olan İnternette yer alan yasadışı ve zararlı içeriklerle mücadeleyi ve bu konudaki ulusal düzenlemeleri büyük oranda etkisiz kılmaktadır. Dolayısıyla, bu durum içerik düzenlemelerinin ve uygulamalarının etkinliğini sınırlandıran en önemli etkidir. Temel hipotezimizde ve bunu destekleyen beşinci alt hipotezimizde tam da bu noktanın altı çizilmekte ve içerik düzenlemesine ilişkin politika, karar ve uygulamalarda bu hususun mutlaka göz önünde bulundurulması ve söz konusu sorunu aşmaya yarar girişimlerde bulunulması gerektiğine dikkat çekilmektedir.

Tezin bu birinci bölümünde, alt hipotezlerimiz ile tartışmaya, doğruluğunu ve geçerliliğini ölçmeye ve test etmeye çalıştığımız temel hipotezimiz çerçevesinde ele aldığımız İnternet içerik düzenlemesi sorununun iki temel unsuru olan “bilgi toplumu” ve “İnternet” olgusu kavramsal, kuramsal ve tarihsel arkaplanı ile konumuz açısından değerlendirilmiştir. Mercek altına alınan İnternet içerik düzenlemesi sorununun boyutlarının anlaşılması, sınırlarının ve sınırlılıklarının görülmesi açısından oldukça önemli olan bu iki olgunun değerlendirilmesi, ilk beş alt hipotez tartışılarak ve doğruluğu test edilmek suretiyle gerçekleştirilmeye çalışılmıştır.

Bu kapsamda ilk olarak, “İnternet”in, “bilgi toplumu” ikliminde yetişen ve ona rengini veren bir ürün olduğu; dolayısıyla, İnternet içerik düzenlemesi sorununun özünde bir bilgi toplumu sorunu olarak görülmesine ve bu bağlamı içinde “bilgi toplumu”nun düşünsel, sosyal, siyasal, ekonomik ve yönetsel arkaplanı ve koşulları içinde değerlendirilmesine imkan tanıyacak doneler ortaya konulmuştur. Bu bağlamda oluşturulan birinci alt hipotez değerlendirilerek doğruluğuna hükmedilmiştir. Yani, içerik düzenlemesi sorununun DNA’sında “bilgi toplumu” yapı taşlarının yer aldığına dikkat çekilerek, sorunun bu derinliği ve karakteristik özelliği belirginleştirilmeye çalışılmıştır.

İkinci olarak, birinci alt hipotezdeki yaklaşımın devamı olarak, ikinci alt hipotezde içerik düzenlemesi sorununun bir başka bağlamı olan “bilgi toplumu ve devlet/kamu yönetimi” ilişki ve etkileşimine işaret edilmiştir. Buna göre, İnternetin belirleyeci olduğu “bilgi toplumu” olgusunun “devlet/kamu yönetimi”ni düşünce ve uygulama olarak köklü bir değişime ve dönüşüme uğrattığı ortaya konulmuş ve “devletin/kamu yönetiminin”, “bilgi toplumu” ile gündeme gelen içerik düzenlemesi gibi yeni sorun alanlarına ilişkin belirsizlik ve dönüşümlere yanıt ve çözümler üretmeye, gelişen kavram, yapı ve yaklaşımları doğasına uyarlamaya çalıştığı açığa çıkartılmıştır. Keza, bu etkileşim sürecinin İnternetle ilgili en önemli yönetsel sonucunun “yönetişim” modeli ve “düzenleyici kurullar” olduğu tespit edilmiştir. Yani, bu hipotez ile içerik düzenlemesi sorununun, diğer bir belirleyicisi olan “bilgi toplumu” ve ona uygun olarak ortaya çıkan yönetim yapısı ve özelliklerinin altı çizilmiştir.

Üçüncü olarak ise, bilgi toplumu ve İnterneti, sunduğu fırsatlar ve riskler, güçlü ve zayıf yönleri, faydaları ve zararları, imkanları ve sorunları bakımından olumlu ve olumsuz yönleri ile birlikte, nesnel ve bütüncül bir bakış açısıyla ele almak gerektiği, aksi takdirde, söz konusu olguların gerçekliklerine vakıf olunamayacağı ve dolayısıyla oluşturulan politikalarda yasadışı ve zararlı içeriklerden kaynaklanan risk ve sorunlara ilişkin etkili önlemlerin alınamayacağı üçüncü alt hipotezde savunulmuştur. Bu hipotez etrafında yürütülen tartışmalar ve değerlendirmeler ile günümüzde fazlaca örneğine rastlanılan yanlış bir yaklaşıma dikkat çekilmek istenmiştir; o da, bilgi toplumu ve İnternet konusunda oluşturulan aşırı iyimser algı

nedeniyle, içerik düzenlemelerinin sebebi olan risk ve tehlikelerden oluşan olumsuzlukların örtbas edilmeye çalışılmasıdır. Nitekim, tezin ilgili bölümlerinde bahsi geçen bilgi toplumu kuramına yapılan eleştiriler, bilgi toplumu ile ortaya çıkan sorunlar ve İnternetle beraber beliren riskler ve tehlikeler bu hipotezimizin doğruluğunu ortaya koymuştur.

Dördüncü olarak, İnternet ortamında yer alan pornografi, çocukların cinsel istismarı, şiddet, ırkçılık, ayrımcılık ve nefret içerikleri, kumar ve bahis, intihara ve uyuşturucuya yönlendirme, siber zorbalık gibi yasadışı ve zararlı içeriklerin birçok toplumsal sorunlara neden olduğundan hareketle, bu tür içeriklerle ulusal ve uluslararası ölçekte etkin bir mücadelenin yürütülmesi gerektiği dördüncü alt hipotezde savunulmuştur. Bu kapsamda özellikle pornografi ve çocukların cinsel istismarı konusuna dikkat çekilmiştir. Nitekim, söz konusu yasadışı ve zararlı içeriklerin her bir türü için ortaya konulan istatistiki veriler, yapılan çalışmaların sonuçları, raporlar ve uzmanların görüşleri risklerin ve sorunların büyüklüğünü ve etkin bir mücadelenin gerekliliğini açık bir şekilde ortaya koymuştur.

Üçüncü ve dördüncü alt hipotez çerçevesinde tartışılan ve değerlendirilen konular ile İnternet içerik düzenlemesi sorununun sosyal boyutunun farkına varılması ve daha iyi anlaşılması hedeflenmiştir. Böylece, sorunun, söz konusu içerikle ulusal ve uluslararası düzeyde etkin bir mücadele yürütülmesi zarureti ortaya koyan sosyal gerçekliğine ait genel bir fotoğraf dikkatlere sunulmuştur. Beşinci alt hipotezin ise, içerik düzenlemesi sorununun tam da bu “etkin bir mücadele yürütülmesi zarureti” gerçeğinin uluslararası boyutuna denk geldiğine yukarıda değinilmişti.

Diğer yandan, birinci bölümde yer alan ilk beş alt hipotez etrafında genel olarak teorik düzeyde yürütülen bu tartışma ve değerlendirmelerin temel hipotezde savunulan temel alanlara ilişkin önemli argümanlar sunduğu ve temel tezi güçlendirdiği de görülmektedir. İkinci bölümde ise, birinci bölümdeki alt hipotezlerle oluşturulan teorik zemin üzerine, diğer alt hipotezlerle dünyadaki içerik düzenlemesi uygulamaları tartışılacak ve değerlendirilecektir. Böylece, sorunun uygulama boyutu alt hipotezler ve temel hipotez bağlamında ele alınmış olacaktır.

İKİNCİ BÖLÜM

DÜNYADA İNTERNET İÇERİĞİNİN DÜZENLENMESİ: YAKLAŞIMLAR, YÖNTEMLER VE UYGULAMALAR

Bu bölümde, yeni alt hipotezler ile temel hipotez, İnternet içeriğinin düzenlenmesi sorunuyla ilgili olarak dünyadaki tartışmalar, temel yaklaşımlar, yöntemler ve uygulamalar açısından tartışılacak, incelenecek ve değerlendirilecektir. Bu çerçevede, dünyada İnternet içerik düzenlemesinin nedenleri ve konuları, uygulanan modeller, ölçütler, ülkelerin konuya yaklaşımları, hukuksal ve örgütsel yapılar ve bunların işleyişleri gibi konular ele alınacaktır.

2.1 İÇERİK DÜZENLEMESİ TARTIŞMALARI, NEDENLERİ VE KONULARI

İnternet içeriğinin devlet eli ile düzenlenmesi sorunu, İnternet içeriğine müdahelenin doğru olup olmamasından, bunun devlet eli ile yapılmasının uygunluğuna; hangi içeriğe kim tarafından ne kadar müdahale edilebileceğinden, bunun hangi yöntemle ve nasıl gerçekleştirilmesi gerektiğine kadar birçok sorunu ve dolayısıyla tartışmaları içinde barındırmaktadır.

2.1.1 İçerik Düzenlemesine İlişkin Başlıca Tartışma Alanları

Düzenleme (regülasyon) kelime anlamı olarak her alandaki genel ve özel düzenleyici faaliyetleri tanımlamak için kullanılmaktadır. Buna göre, düzenleyici faaliyetler, her türlü “önlem” ve “müdahaleyi” kapsamaktadır. Düzenleme, devlet özelinde değerlendirildiğinde ise, “Bireylerin veya grupların davranışlarını değiştirmeye çalışan devletin önlem veya müdahaleleri” olarak tarif edilmektedir(Beceni, 2004: 5).

Günümüzde, dünyanın dört bir tarafında İnternetin zararlı etkileriyle mücadele etmek için çalışmalar yapılmakta ve bu bağlamda, İnternetin güvenli kullanımını sağlamak amacıyla ülkeler, giderek artan bir oranda, bir yandan siber suçlarla mücadele

ederken, diğer yandan da İnternet içeriğinin güvenliği ile ilgili bir takım düzenlemeler yapmaktadır (Bambauer, 2008).

Bununla beraber, yasadışı veya zararlı olarak nitelenen İnternet içeriğine ilişkin düzenleme yapılması, bu çerçevede İnternetin denetlenmesi ve erişimin engellenmesi hususları tüm dünyada birçok açıdan tartışılmaktadır. Fakat bütün tartışmalarda, düzenlemelerin “yöntemi” ve “kapsamı” olarak ifade edebileceğimiz iki temel ekseninde yürütüldüğü görülmektedir. Yani, tartışmaların genel olarak, düzenlemelerin “kapsam” ve “yöntem”ine ilişkin görüş ayrılıklarından ortaya çıktığı söylenebilir.

Bu çerçevede tartışmalar iki temel soruya/soruna odaklanmaktadır. Bunlardan birincisi, içerik düzenlemelerinin “insan hakları ve demokrasi ilkelerine uygunluğu” sorunudur. Diğer bir deyişle, düzenlemelerin hangi yöntem ve kapsam ile yapılması durumunda ifade ve bilgiye erişim özgürlüğünü de içine alan “insan hakları ve demokrasi”yle bağdaşabileceği konusudur. İkincisi ise, içerik düzenlemelerinin İnternetin kendine özgü yapısıyla ne kadar bağdaştığı sorunudur. Yani, düzenlemelerin hangi yöntem ve kapsam ile yapılması durumunda İnternetin dağıtık ve dinamik özgün yapısına daha çok uyum sağlayacağı konusudur (Kaya, 2010: 2).

Dolayısıyla, bu bağlamda içerik düzenlemelerinin “yöntemi” ve “kapsamı” en kritik konular haline gelmektedir. “Yöntem” konusundaki tartışmalar; içerik düzenlemesinin hangi yönetsel yaklaşımla ele alınması gerektiği, öngörülen önlem ve müdahalelerin kim/kimler tarafından, nasıl bir mekanizma ile yapılmasının uygun olacağı, “kapsam” konusundaki tartışmalar ise; İnternet içeriği düzenlemesinin sınırlarının ne olacağı ve hangi konuları içereceği noktasında düğümlenmektedir.

“Yöntem”e ilişkin temel görüş ayrılığı, içerik düzenlemelerinin doğrudan devlet eliyle mi, yoksa sivil inisiyatif tarafından mı, ya da her ikisinin birlikte mi yapılmasının ve uygulamasının uygun olacağı noktasında ortaya çıkmaktadır. Dolayısıyla, tartışmaların merkezinde, İnternet içeriğinin düzenlenmesinde ve uygulamasında devletin rolü konusu yer almaktadır. Bu bağlamda, “Devlet İnternet içeriğine ilişkin

önlem alma ve müdahalede bulunma konusunda aktif rol almalı mı? Düzenleme ve uygulamaların neresinde olmalı?” soruları etrafında tartışmalar yoğunlaşmaktadır.

Bir kısım İnternet kullanıcıları, bilişim uzmanları ve hukukçular, İnternet içeriğine ilişkin olarak devlet eli ile yapılan her tür doğrudan veya dolaylı düzenlemeye kökten karşı çıkmaktadır (Bakırcı, 2009: 7). Bu fikir daha çok 1990’lı yıllarda ABD’de savunulmuştur (Yasin Söyler ile kişisel iletişim, 01.08.2013). Bu fikri savunanlar devlet müdahalesinin İnternetin “özgürlükçü doğası”na aykırı olduğunu ileri sürerken aslında iki temel argümana atıfta bulunmaktadır. Bunlardan ilki, İnternetin kendine özgü yapısından ve teknik özelliklerinden dolayı devletlerin İnterneti düzenlemekte etkisiz ve yetersiz kalacağı savıdır. Bu kapsamda İnternetin sınırsız özelliği nedeniyle hükümetlerin siber uzayla ilgili egemenliğe ve düzenleme yapma yetkisine sahip olmadığını beyan ederek, “ifade” ve “kimlik” gibi geleneksel hukuki kavramların İnternette uygulama alanının bulunmadığını ileri sürmektedir (Barlow, 1996; Geist, 2003).

İkinci argüman ise, İnternet içeriğine ilişkin hükümetlerin yapacağı her tür düzenlemenin ifade, bilgi ve düşüncenin serbest dolaşımı, bilgiye erişim gibi özgürlüklere sınırlama getirme, yani “sansür”e sebep olma ihtimalinin yüksek bulunmasıdır. Çünkü, siyasal iktidarların bu yetkiyi genellikle ölçsüzce kullanacakları varsayılmaktadır. Bu sansür uygulamaları çoğu zaman hükümet politikası olarak ortaya çıkarken, bazen de uygulanan yöntemlerin teknik yetersizliğinden de meydana gelebilmektedir. Bu kapsamda, müdahalelerin İnternetin kalitesini düşüreceğini, İnternetin hızlı ve ucuz yoldan bilgiye erişim özelliğine darbe vuracağı iddia edilmektedir (Bakırcı, 2009: 7-8; Kaya, 2010: 2).

Ayrıca, her devletin İnterneti kendi yaklaşım ve önceliklerine göre düzenlemesi ve kontrol etmesi sonucunda, artık tek bir İnternette söz edilemeyeceği, düzenleme yapan ülke adedince farklı “İnternet”in ortaya çıkacağı, kısıtlamalar nedeniyle İnternetin görünümünün ülkeden ülkeye farklılaşacağı dile getirilmektedir. Bu durumda, İnternetin küresel ağ olma niteliğini kaybedeceği belirtilmektedir (Deibert vd., 2008: 2-4; Goldsmith ve Wu, 2006: 9). Böylece İnternet, bölgesel kontrolden

bağımsız bir siber alan olmanın ötesinde, giderek “görünümü ona nereden erişildiğine bağlı olan” bir araç haline gelecektir (Bambauer, 2008). Nitekim, Çin’den İnternete girdiğinizde, Çin Komünist Partisi’ni veya ülkenin insan hakları sicilini eleştiren sitelere erişimin olmadığı bir İnternetle karşılaşırken (OpenNet, 09.08.2012a), Fransa veya Almanya’da İnternete bağlandığınızda, Nazi içeriklerinin engellendiği bir İnternet görülecektir (OpenNet, 2010a). Aynı şekilde, Suudi Arabistan ve İran’da İslam karşıtı sitelerin bulunmadığı (OpenNet, 06.08.2009, 16.06.2009) bir İnternetle muhatap olunurken, Hindistanda, aşırı dinci Hindu sitelere erişimin engellendiği (OpenNet, 09.08.2012b) bir İnternetle karşılaşılacaktır.

Devletlerin hiçbir şekilde doğrudan İnternetin özgür ortamına müdahale etmesini uygun bulmayan bu görüşe göre, konu kendi araçları ve kendi kuralları ile çözmek üzere tamamen kullanıcılara, sivil topluma ve sektörün öz düzenleme girişimlerine bırakılmalıdır (Bakırcı, 2009: 7). Bu yöntemin İnternetin kendine özgü doğasına uygun uygulamalar geliştireceği, teknik ve operasyonel eksiklikleri en aza indireceği savunulmaktadır (Akdeniz, 2003: 55-56).

Mehmet Sarı ise, İnternetin icadından sonra ortaya çıkan ve günümüzde de kısmi yansımaları bulunan bu görüşün arka planında yeni olan herşeyin aşırı ilgi görmesi ve yüceltilmesi alışkanlığının etkisi olduğunu belirtmektedir. Sarı’ya göre, insanlık tarihinde yeni icad olunan veya yeni ortaya çıkan herşeyin genellikle önce kutsandığına, sınırsız bir kullanıma açıldığına şahit olmaktayız. İnternetin şu anda kutsanma dönemini yaşıyoruz. Bir müddet sonra bu heyecan azalacak, durun bakalım bu bize zarar vermeye başladı denilecek. Bu çerçevede bir süre sonra önlem alma düşüncesi gelişecektir. Dolayısıyla normalleşmesi, olması gereken yere oturması biraz zaman alacaktır. Bunu biraz da kapitalizme benzetebiliriz. Kapitalizmin ilk dönemlerini İnternette yaşıyoruz; şu anda sınırsız bir “bırakınız yapsınlar, bırakınız geçsinler” mantığı hakimdir. Bu böyle gitmeyecektir. Zaman içinde bu anlayışın mahzurları görüldükçe İnternetin denetimi ve düzenlenmesi düşüncesi gelişecektir (Mehmet Sarı ile kişisel iletişim, 24.07.2013).

Nitekim, yakın zamanda İnternetin gelişim sürecinde yeni bir trende girildiği görülmektedir. Artık İnterneti ve sanal ortamı keşfetme heyecanı sona ermiştir. Bu sanal ortamdaki en fazla faydayı sağlamak için konulması gereken kullanım kuralları konuşulmaya başlanmıştır. Yani, yeni trend önlem alma, diğer bir deyişle; sanal ortamın sağlıklı yaşam koşullarını belirleme trendidir (Bambauer, 2008).

Devletleri içerik düzenlemelerinin dışında tutmayı gerçekçi bulmayanlar ise, düzenleme olmayan bir İnternet fikrinin gerçekçi olmayacağına, özgürlük fikrinin “kuralsızlık” anlamına gelmeyeceğine, bilakis özgürlüğün teminat altına alınmasının da kuralları gerekli kıldığına işaret etmektedir (Bakırcı, 2009: 8). Keza, Şen’in de belirttiği gibi, İnternet hayatın içinde bir olgudur. Hayatın içinde olan her şey de hukukun ilgi alanına girer ve dolayısıyla düzenleme konusu olur. Sınırsız bir özgürlük yoktur. Mesela, kimsenin başkasını rahatsız etme özgürlüğü olamaz. Kimse trafikte kırmızı ışık benim özgürlük alanımı kısıtlıyor diyemez. Dolayısıyla, İnternette de kırmızı ışıklar olacaktır (O. Nihat Şen ile kişisel iletişim, 06.08.2013).

Keza, hükümetlerin ulusal çıkarları ve değerleri korumak için bu alanla ilgili düzenleme yapması kaçınılmaz görülmektedir (Bakırcı, 2009: 8). Bu kapsamda, devletin öncelikli görevinin vatandaşların maddi ve manevi varlığını koruyabileceği ve geliştirebileceği ortamı hazırlamak olduğunu; dolayısıyla, devletin İnterneti her türlü hukuka aykırı, zararlı ve sakıncalı içerikten arındırması gerektiği dile getirmektedir. Keza, devletin genel ahlakı ve aileyi koruma görevine de dikkat çekilerek bu bağlamda aktif rol oynaması gerektiği ifade edilmektedir (Kaya,2010:2).

Kimileri de bu alanın, içerisinde kamu kurumları bulunan fakat ilgili tarafların da yer aldığı bir mekanizma ile ortaklaşa düzenlenmesi ve yönetilmesini savunmaktadır. Bu yaklaşımda, içerik düzenlemelerinde devletin otoriter gücünün gerekliliği kabul edilmekle beraber, İnternet ile ilgili problemlerin çözümünde devletin yetersiz kalacağı görüşü dile getirilmektedir. Buna göre, İnternetin küresel ve merkezi olmayan, dağınık ve dinamik yapısı, ulusal düzeydeki devlet düzenlemelerinin, sorunları çözme konusundaki etkinliğini azaltmaktadır. Bu nedenle, bir yandan ulusal ölçekte İnternet’in çok taraflı yönetimi anlayışıyla hareket ederken, diğer yanda

ulusal düzeydeki politikaların geliştirilmesinde uluslararası yetki konularının dikkate alınması ve bu politikaların uluslararası düzeydeki gelişmeler ışığında birleştirilmesi ve koordinasyonunun sağlanması gerekmektedir (Akdeniz, 2003: 49, 54).

İçerik düzenlemesinin “kapsam”ı konusu da diğer temel bir tartışma eksenidir. Buna göre, düzenlemelerin öngördüğü önlem ve müdahalelerin sınırlarının belirlenmesi görüş ayrılıklarına neden olmakta ve özellikle erişim engellemeye veya filtrelemeye konu olan hususların sınırları tartışılmakta ve hangi içerik türlerinde ve alanlarında düzenleme yapılmasının uygun olacağı değerlendirilmektedir.

Bu kapsamda, içerik düzenlemesi konusunda çerçeveyi geniş tutma eğiliminde olan ve çok sayıda içerik türünü “yasadışı veya zararlı” kabul ederek düzenleme konusu yapmayı savunan görüşler ve uygulamalar içinde bulunan devletler daha fazla “sansürcü” nitelenmesine muhatap olmaktadır. Demokratik değerlere önem veren ülkelerin ise, genel çerçeveyi mümkün olduğunca sınırlı tutarak, sadece önemli gördükleri “çocukların cinsel istismarı”, “ırkçılık ve ayrımcılık” ve “terör” gibi belirli birkaç hususu düzenleme konusu edindikleri belirtilmektedir.

Nitekim, devlet düzenlemesini gerekli görenlerin bir çoğu sınırlı müdahaleyi özgürlükler ve demokratik değerler açısından en önemli gereklilik olarak öne sürmektedir. Bu bağlamda, düzenlemelerde adil, hesap verebilir ve kamu yararına göre ölçülülük ve gerekli olan en az müdahaleyi öngörmektedirler (Bakırcı, 2009: 8). Benzer şekilde, İnternetin doğasına en uygun yaklaşımın da bu yönde hareket etmeyi gerektirdiği; İnternetin bazı teknik özellikleri göz önünde bulundurulduğunda hükümet düzenlemelerinin teknik ve operasyonel eksiklikler taşıyacağı, bu nedenle kapsam ne kadar sınırlı tutulursa eleştirilere o kadar daha az hedef olunacağı dile getirilmektedir (Akdeniz, 2003: 24). Keza, devlet eliyle yapılacak düzenlemelerin İnternetin gelişimini engellemeyecek şekilde olması gerektiğine özellikle vurgu yapılmaktadır (Goldsmith ve Wu, 2006: 167).

Keza, özgürlükle eşdeğer olarak düşülülen “İnternet” olgusu karşısında kamu gücünü kullanan devletlerin nasıl bir konum ve tutum belirlemeleri gerektiği konusu bir

takım güçl klere iřaret etmektedir. Zira İnternet, ulus devletler i in bazı zorluklar meydana getirmiřtir. Bu zorlukların en  nemlisi de İnternetin, klasik ulusal egemenlik anlayıřlarına meydan okuyan karmařık,  ok deęiřkenli, dinamik ve sınır tanımayan k resel yapısıdır. Devletlerin  lke sınırları i erisinde vatandařlarına hukuk kuralı koyma ve bunu uygulama meřruiyetlerini esas alan klasik ulusal egemenlik yaklařımları, vatandaşlık, ulusal sınır gibi kavramları hi e sayan bu teknolojiyi kontrol altına alma kanallarını olduk a zorlamaktadır. Dolayısıyla, İnternet teknolojisi bug n “egemenlik” kavramını yeniden d ř nmeye mecbur kılmakta (Yeřilyurt, 2007: 1-2) ve İnternetin d zenlenmesi konusu “d zenleme” ve “devletin egemenlik yetkisi” kuramlarının temelden sorgulandıęı bir mecraya doęru ilerlemektedir (Beceni, 2004: 5).

Nitekim, řen de bu konuya dikkat  ekmekte ve “d zenleme”nin hakim olunan alan i inde, yani egemenlik alanı i inde yapılabileceęini, İnternetin yapısında ise devletler i in mutlak anlamda b yle bir alanın bulunmadıęını belirtmektedir. Zira, d zenleme yapmak istendięinde m cadele edilmek istenen i eriklerin yurtdıřında barınmasının s z konusu d zenlemeleri  oęu zaman iřlevsiz kıldıęını dile getirmektedir.  lkelerin, bařka bir  lkede barınan i erikler  zerinde tasarruf hakkı bulunmadıęı i in  abalar sonu suz kalmaktadır. Bundan dolayı İnternet i erik d zenlemesinin zor bir alan olduęunu vurgulamakta ve etkili c z m  i erik d zenlemesinin en  st d zeyde ITU veya BM’ce yapılmasında g rmektedir(O. Nihat řen ile kiřisel iletiřim, 06.08.2013).

Fakat uygulamada, İnternetin kendine  zg  bir sistemi olduęu kabul edilmekle birlikte, sanıldıęı gibi devlet m dahalesinden uzak ve tamamen  zg r bir ortam olarak g r lmedięine řahit olunmaktadır (Deibert vd., 2008: vii). Nitekim, İnternetin tamamını kontrol eden tek bir otorite bulunmadıęını ve dolayısıyla k t ye kullanmaya a ık bir sistem (Goldsmith ve Wu, 2006: 21) olduęunu farkedene devletler, bařlangı ta bu k t ye kullanımları  nlemek i in İnternete iliřkin sınırlı kurallar koymuřlarsa da, zamanla İnternet d zenlemelerinin nitelik ve nicelikleri deęiřmiř ve devletler  eřitli sosyal, k lt rel, siyasal, y netsel veya ekonomik sebeplerle İnternet i erięine doęrudan ya da dolaylı olarak m dahale etmeye ve

vatandaşlarının İnternet üzerindeki faaliyetlerini yoğun bir şekilde takip etmeye başlamışlardır (Goldsmith ve Wu, 2006: 166; Kaya, 2010; 3).

Devletlerin kendi egemenlik alanında kendi koyduğu kuralları uygulaması uluslararası hukukun en temel ilkelerinden birisi olduğuna göre, devletlerin İnternete müdahale etmeleri egemenliklerinin klasik bir kullanım şekli olarak kabul edilebilir. Bu bağlamda, yöntemi ve kapsamı tartışılmakla birlikte, devletlerin İnternet gibi bilgi ve iletişim ortamlarını kontrol etmeleri ve müdahalede bulunmaları yeni ortaya çıkan bir olgu değildir. Bugün liberal demokratik devletlerde bile ifade hürriyeti, iletişim ve bilgiye erişim hakkı, özel hayatın gizliliği gibi konular her türlü müdahaleden uzak mutlak haklar olarak görülmemektedir (Deibert vd., 2008: 31).

Dolayısıyla, ilk zamanlarda tamamen bir özgürlük alanı olarak görülen İnternet, bu gün değişik mülahazalar neticesi değişik içerik düzenlemelerine muhatap olmaktadır. Bugün artık, devlet İnternete hiç dokunmasın diye bir tartışma konusu yoktur (Yasin Söyler ile kişisel iletişim, 01.08.2013). Teori ve uygulamada yöntem ve kapsam farklılıkları olmakla birlikte, ülkeler günümüzde az ya da çok İnternet içeriğinin düzenlenmesi gerektiği noktasında fikir birliğine ve uluslararası bir uzlaşmaya varmış gözükmemektedir. Nitekim, bugün, İnternet yelpazesinin aşırı uçlarının kontrolü her devlet için büyük önem arz etmektedir (Deibert vd., 2008: 61).

Görüldüğü gibi, mevcut durum tezin altıncı alt hipotezinde savunulduğu noktada gözükmemektedir. Yani, devletler İnterneti denetim altına almakta önemli zorluklar yaşasalar da, değişik gerekçelerle İnterneti kontrol altına alabilmek için giderek daha fazla düzenleme yapma gereği hissetmektedirler. Tüm dünyada özellikle, İnternetteki yasadışı ve zararlı içeriklerle mücadelenin kapsam olarak giderek genişleyen bir trende sahip olduğu gözlemlenmektedir.

Diğer yandan, içerik düzenlemelerinin “kapsam” ve “yöntem” olarak “insan hakları ve demokrasi”yle bağdaşması ve İnternetin çok yönlü/aktörlü ve dinamik özgün yapısıyla uyum içinde olması gerektiği çerçevesinde yukarıda yürütülen tartışmalar, tezin sekizinci alt hipotezinin doğruluğunun ve geçerliliğinin sınanması açısından

faydalı olmuştur. Zira, her iki kriterin içerik düzenlemeleri açısından yaşamsal değere sahip olduğu ve her ikisiyle uyumu temin edecek yaklaşım tarzının “sınırlı müdahale” olduğu, tıpkı hipotezde savunulduğu gibi, yapılan tartışmalar ve değerlendirmeler sonucunda da ortaya çıkmıştır.

2.1.2 İçerik Düzenlemesinin Nedenleri ve Konuları

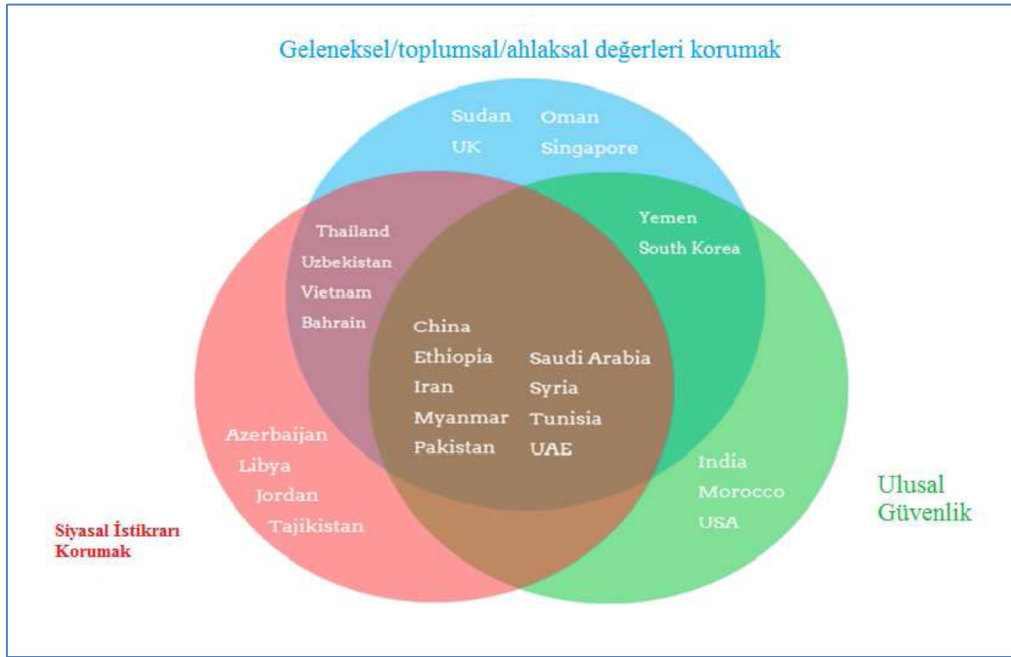
“Gerçek hayatta suç olanın çevrimiçi ortamda da suç sayılması” prensibinden hareketle farklı konulardaki bir takım içeriklerle ilgili, başvurular üzerine mahkemelerce erişim engelleme kararları alınarak söz konusu içeriklerle mücadele edilebilmektedir. Fakat bunlar dışında, birinci bölümde ana hatlarıyla önemli bir kısma değinilen ve ilerleyen sayfalarda dünya uygulamaları ile farklı örnekleri görülecek olan, birçok farklı nedenden ötürü devletler İnternet içerik düzenlemesi yapmaya yönelmektedir. Devletleri bu alanda düzenleme yapmaya iten başlıca nedenler ve gereksinimler genel olarak şu üç maddede toplanabilir:

- İnternetin terörizm amaçlı kullanılması, ırkçılık ve ayrılıkçılık türü içeriklere erişim sağlaması nedeniyle devletlerin ulusal güvenlik konularında endişe duymaları.
- İnternette yer alan kimi içerikler karşısında toplumların ve devletlerin, kendi geleneksel, tarihsel, kültürel, sosyal, siyasal, dinsel ve ahlaki değerlerine ilişkin kaygılar taşımaları. Özellikle çocuklar, gençler ve aileler başta olmak üzere İnternet üzerinden gelebilecek olumsuz etkilerden toplumu koruma amacı.
- İnternetteki devletle ilgili değer yargılarına yönelik hakaret içeren ifadeler, rejim, resmi ideoloji aleyhtarlığı yapılması gibi kurulu siyasal sisteme ve siyasi istikrara zarar verecek içeriklerden duyulan rahatsızlıklar.

Devletlerin içerik düzenlemesi uygulamalarına dayanak yaptıkları gerekçeler bazen tek bir hususla sınırlı kalırken, bazen de birden fazla hususu içerebilmektedir. Şekil 2.1.’de, bazı ülkelerin içerik düzenleme nedenleri görülmektedir. Buna göre, ülke güvenliği gerekçesiyle ABD, Hindistan ve Fas; geleneksel/toplumsal/ahlaki değerleri korumak için İngiltere, Sudan, Umman ve Singapur; siyasal istikrarı sağlamak amacıyla da Azerbaycan, Ürdün, Tacikistan ve Libya İnternete kısıtlamalar

getirmektedir. Son gruptaki ülkelerin ortak noktasının genelde Batılı ülkelerin çeşitli sebeplerle üzerlerinde nüfuzlarını artırmak istediği ülkeler olması dikkat çekicidir (Çağlar, 2011: 113).

Şekil 0.1. Ülkelerin İnternete müdahale nedenleri



Kaynak: Yuxiyou.net, 2011, <http://yuxiyou.net/open/> (25.09.2011)

Diğer yandan, Tayland, Özbekistan, Vietnam ve Bahreyn'in geleneksel değerleri korumak yanında siyasi istikrarı sağlamak amacıyla; Yemen ve Güney Kore'nin de yine geleneksel değerleri korumak amacıyla birlikte ulusal güvenliği sağlamak için İnternete müdahale ettiği görülmektedir. Ayrıca, üç farklı nedeni birden kullanarak İnterneti kısıtlayan Birleşik Arap Emirlikleri (UAE), Çin, Etiyopya, İran, Pakistan, Myanmar, Suudi Arabistan, Suriye ve Tunus gibi ülkeler de bulunmaktadır.

Yaklaşık 1995 yılından bu yana dünyadaki birçok ülke, bahsi geçen nedenlere paralel olarak farklı konularda içerik düzenlemesi gerçekleştirmektedir. Ülkeler genelde ortak görüş olarak çocuk pornografisi, ırkçılık ve ayrımcılık, terör gibi konularda, vatandaşlarını özellikle de çocukları ve gençleri korumak amacıyla söz konusu içeriklerle mücadele yoluna başvurmuştur. Örneğin, azınlıkları hedef alan ırkçı

söylemlerin hız kazanması nedeniyle Almanya ve Fransa aşırı sağcı içerikle, ABD çocuk pornografisiyle, mücadele etmektedir.

Bunun yanında, bazı devletlerin bir takım siyasal kaygılarla yaygın filtreleme yaptıkları ve katı kurallarla İnternet içeriklerini kontrol altına almaya çalıştıkları da görülmektedir. Bu devletlerin hedef aldıkları web hizmetlerinin, bloglar, haber ve STK'larına ait siteler olduğu gözlemlenmektedir. Söz konusu sitelerin ortak özelliği ise, statükonun istemediği veya tehdit olarak algıladığı içerikleri barındırmaları olarak ortaya çıkmaktadır (Çağlar, 2011: 28). Örneğin, Çin, komünizme karşı tehdit olarak gördüğü içerikle, Suudi Arabistan, İran ve Suriye rejim aleyhtarı içerikle, Güney Kore, Kuzey Kore propagandasına ait içerikle mücadele etmektedir.

Ülkelerin düzenleme ve denetleme yapma ihtiyacı duydukları İnternet içerikleri bazen farklı konu ve alanlara yönelik olsa da, çoğu zaman benzer ve ortak konu ve alanları kapsamaktadır. Uygulamada düzenleme ve denetlemeye en sık konu olan İnternet içeriği türleri genel olarak şöyle sıralanabilir (Çağlar, 2011: 28-29):

- *Telif hakkı ihlalleri:* Ülkelerin ortak önlem aldıkları en temel başlıklardan biridir. Hatta ABD diğer konulardaki içeriklere karşı doğrudan önlem almayı hala tartışırken, telif hakkı ihlalleri konusunda tartışmasız olarak önlem alınmasını benimsemiştir. Bu konuya ilişkin içerik düzenlemelerinin temel gerekçesi diğerleri gibi kullanıcının güvenliği ve korunması değil, üreticilerin ve rekabetçi piyasanın korunmasıdır. Nitekim, bu konudaki katı tutum nedeniyle, Youtube telif hakları ile ilgili büyük tazminatlardan korktuğundan bu alanda faaliyet gösteren meslek örgütlerinden gelen içerik çıkartma taleplerini hemen yerine getirmek için, bazı ülkelerde, tespit ettiği içeriği çıkarma yetkisine sahip yerel ajanslarla anlaşmıştır (Lütfi Güvener ile kişisel iletişim, 24.07.2013).
- *Çocuk Pornografisi ve cinsel istismarı:* Çocuk pornografisi, ABD ve Avrupa ülkeleri de dahil çok sayıdaki ülkenin önem verdikleri, hapis de dahil olmak üzere ağır yaptırımlarla cezalandırdıkları bir suçtur. Dünya'da çocuk pornografisi ve cinsel istismarı içerikli İnternet yayınlarına karşı önlem alınması, mücadele edilmesi ve bu tür içeriklere erişim engelleme uygulanması konusunda, birkaç istisna dışında

neredeyse tüm ülkeler arasında görüş birliği vardır. Bu önemli konu, hem çocukların bu içeriklerden etkilenmesi ve hem de bu içeriklerin üretilmesinde nesne olarak kullanılması açısından BM, AB ve Avrupa Konseyi (AK) tarafından hazırlanan uluslararası belgelere konu olmuştur (Dülger, 2011).

- *Irkçılık ve ayrımcılık:* Bu konudaki içerikler, birçok ülke tarafından ve özellikle bazı Avrupa ülkelerinde önlem alınması gereken içerikler sınıfında yer almaktadır. Keza, cinsiyet ayrımcılığı da bu başlık altında tartışılmaktadır.
- *Nefret ve şiddet uyandıran içerikler:* Önlem alınması konusunda, daha önce bahsi geçen içerik türleri kadar üzerinde ortak görüş oluşmasa da, bu içeriklerin bir kısmı, bir trend olarak önlem alınmaya başlanan içerikler arasında yer almaktadır. Özellikle intihara yönlendirici şiddet bu başlık çerçevesinde gündeme gelmektedir.
- *Pornografi:* Literatürde yetişkin (adult) pornografisi olarak geçen içeriklere ilişkin ülkelerin tavırları farklılık göstermekle birlikte, giderek bu tür içeriklerin denetim altına alınması ve mücadeleye konu edilmeleri yönünde yaygınlaşan bir eğilim gözlemlenmektedir. Bazı ülkelerde bir takım sosyal, ahlaki veya dini gerekçelerle bu tür içeriklerin tümüne yönelik olarak filtreleme ve erişim engelleme uygulanmaktadır. Bazı ülkelerde ise, çocukların bu tür içeriklerden korunması ön planda tutularak, +18 yaş doğrulaması benzeri uygulamalarla yetinilmektedir. Bir takım ülkeler ise, genel olarak bu tür içeriklerden sadece ekstrem pornografi (ensest, ölü sevicilik, hayvan vs.) kısmı ile ilgilenmekte ve bunlara yönelik tedbirler almayı benimsemektedir. Az da olsa bazı ülkeler ise, çocuk pornografisi dışındaki hiçbir pornografik içeriği dikkate almamaktadır. Fakat, pornografinin sosyal maliyetinin giderek artması ve özellikle kadınlara yönelik cinsel şiddeti tetiklemesi ve çocuklar üzerindeki olumsuz etkileri nedeniyle AB ülkeleri de dahil olmak üzere bazı batılı ülkelerin de yetişkin pornografisine yönelik tedbirleri gündemlerine almaya başladıkları görülmektedir. Fakat, bu içeriklerle kurumsal olarak mücadele etme ve önlem alma konusunda henüz dünyada genel bir uzlaşma ve irade bulunmamaktadır.

Görüldüğü gibi, İnternet içerik politikaları, ülkelerin ekonomik, teknolojik, kültürel gelişmişlik düzeylerine ve sosyolojik ve siyasal kodlarına, kültür ve inanç haritalarına göre şekillendiğini göstermektedir. Nitekim, bu kapsamda, devletleri

düzenleme yapmaya iten nedenler ve gereksinimler ile yasadışı ve zararlı içerik olarak kabul ederek düzenleme kapsamına aldıkları içeriklerde konular ve sınırları bakımından farklılıklar bulunmaktadır. Bu durum yedinci alt hipotezimizde savunduğumuz görüş ile örtüşmektedir.

2.2 İÇERİK DÜZENLEMESİNDE TEMEL YÖNETİMSSEL YAKLAŞIMLAR

İnternet içeriğinin düzenlenmesi, kurallar konulması ve önlem alınması konularında dünyada farklı yönetimsel yaklaşımlar uygulanmakta ve bu yaklaşımlar değişik boyutları ile tartışmalara konu olmaktadır. İçerik düzenlemesine ilişkin temel yönetimsel yaklaşımlar, devlet düzenlemesi (government regulation), kendi kendine/öz düzenleme (self-regulation) ve birlikte/ortak düzenleme (co-regulation) olarak üç başlık altında ele alınabilir.

2.2.1 Devlet Düzenlemesi

Daha önce görüldüğü gibi, tekniği, alt yapısı, işleyiş biçimi, uluslararası niteliği, suç yeri ve zamanı, sorumlu olabilecek kişiler vb. yönünden diğer suç işlenen araçlardan farklı özelliklere sahip İnternet ortamında gerçekleştirilen dolandırıcılık, kişilik haklarına saldırı, bilgisayar güvenliğini tehdit, siber terörizm gibi konularla ilgili bilişim suçlarıyla devletler özel kanunlar çıkararak mücadele vermektedir. Hatta, yer yer bu nevi suçlarla mücadele konusunda uluslararası işbirliğinin olanakları kullanılmakta ve özellikle İnternetin uluslararası niteliği gereği bu alanlardaki suç ve suçlularla daha etkin mücadele edilebilmesi konusunda devletlerarası işbirliği olanakları artırılmaya çalışılmaktadır.

Benzer şekilde, İnternet içeriğini düzenleme konusunda devletlerin doğrudan müdahale etmesini benimseyen yaklaşımlar ve uygulamalar mevcuttur. Buna göre devlet, konuyla ilgili düzenleme yapma yetkisini tekeline alarak, yetki verdiği bazı kamu kurumları eliyle söz konusu içeriklerle kamu gücünü kullanarak doğrudan mücadele etme yöntemini tercih etmektedir. Bir takım eleştirilere neden olsa da,

içeriğin bu nevi doğrudan ve aktif devlet müdahalesiyle kontrol altına alınmaya çalışılması ve farklı amaçlarla İnternetin kısıtlanması sıkça görülen bir uygulamadır.

Devletlerin aktif rol alarak sakıncalı veya zararlı içerik olarak kabul edilen İnternet içeriğiyle mücadele etmesi konusunda, bazı ortak noktalar bulunmakla birlikte, farklı nedenler, yöntemler ve uygulamalar göze çarpmaktadır. Bazı devletler temel prensip olarak İnternet içeriğine doğrudan müdahale etmeksizin vatandaşlarının hukuki veya cezai sorumluluğunu esas alırken, bazıları ise içeriğe müdahale etmeyi ön plana çıkarmaktadır. Bu çerçevede, her devlet farklı sorumluluk esaslarına göre İnternet kullanıcıları, İSS, yer sağlayıcıları ve diğer aktörlerin hukuki ve cezai sorumluluklarını düzenlemektedir (Kaya, 2010: 3).

Hangi yöntem kullanılırsa kullanılsın, işe başlarken devlet düzenlemelerinin incelenmesi, güçlü ve zayıf yönlerinin ortaya konulması önem taşımaktadır. Örneğin, devlet düzenlemelerinin en önemli enstrumanı olan ve ortaya çıkan herhangi bir sorunun çözümü ve genel olarak riskleri azaltmak için tasarlanan yasalaştırma yönteminin, her zaman en iyi yol olmayabileceği dile getirilmektedir. Buna göre, bazı durumlarda içerisinde devletin “hiçbir şey yapmama” seçeneğinin de yer aldığı diğer yöntemler yasalaştırmadan daha az maliyetli ve daha etkin olabilmektedir. Keza bazen, devletin düzenleme yapması soruna çözüm getirmeyip sorunu farklı yerlere taşıyabilmekte veya düzenlemenin maliyeti, sorunun oluşturduğu maliyetten daha pahalı olabilmektedir (Akdeniz, 2003: 51-55).

Bu çerçevede, devlet düzenlemelerinin “uygulanabilir”, “inanılır”, “açık ve saydam” olması ve mevzuat uygulamalarında, düzenleyici kurum ve kuruluşlara geniş takdir yetkisi vererek keyfiliğin meydana gelmesine sebebiyet vermemesi gerekmektedir (Akdeniz, 2003: 51-55).

Diğer yandan, üçüncü dünya ülkeleri ve özellikle Asya kıtasında görülen, doğrudan devlet ototritesinin egemen olduğu kurumların yönetiminde gerçekleştirilen içerik düzenlemesi uygulamalarında, genellikle katı bir müdahale yönteminin tercih edildiği ve kapsayıcı önleyici tedbirlerin alındığı görülmektedir (Çağlar, 2011: 115).

2.2.2 Kendi Kendine/Öz Düzenleme

Öz düzenleme (self-regulation), genel olarak her iş dalı veya sektörün kendi kural ve davranış ilkelerini kendisinin belirlemesi, kendi kendini düzenlemesidir. Bu yaklaşımın temelinde, piyasaları hukuken yöneten kuralların, yönetilen kişiler veya onların doğrudan temsilcileri tarafından belirlenmesi, geliştirilmesi, yönetilmesi ve yürürlüğe konulması düşüncesi vardır (Akdeniz, 2003: 55).

Burada hem öz denetim hem de davranış kuralları sektör içindeki firmalarca belirlenmektedir. Öz denetim kuralları, sektör içerisindeki firmaların tüketici güvenini ve memnuniyetini sağlama, dürüst ticaret yapma, kendi sektörleri içerisinde ilişkileri düzenleme amaçlarıyla oluşturduğu normlardır. Davranış kuralları ise, daha çok ticaret yapış biçiminde ahlaki ve hukuki değer taşıyan standart uygulamaları tanımlamakta kullanılmaktadır (Beceni, 2004: 16-18). Öz düzenleme, zorunlu olmamakla birlikte, bu ortak kurallara uymaya karar veren sektör mensuplarının getirilerini katılanların paylaştığı bir “gönüllülük” hareketidir (Akdeniz, 2003: 55). Dolayısıyla öz düzenleme resmi olmayan gönüllük esaslı düzenlemedir (Bakırcı, 2009: 11).

İnternet ortamının kurallarını belirleme ve önlem alma eğilimi sadece devletlerce değil, İnternet sitelerini ve sosyal ağları yöneten birçok büyük firmalar, ISS’lar ve erişim sağlayıcılarca da benimsenmektedir. Çünkü bu sürecin ticari tarafında olan firmalar, sanal ortamın, çocukların ve ailelerin zararlı olarak algıladığı bir hale gelmesinin bu alanla ilgili ciddi ve haklı önlemlerin alınmasına ve sanal ortamdaki uzak kalma eğiliminin artmasına neden olacağının farkındadırlar. Bu durumun sanal ortamın gelişmesinin ve yaygınlaşmasının, dolayısıyla ticari kazançlarının artmasının önünde bir engel oluşturabileceğini bilmektedirler.

Diğer yandan, söz konusu firmalar, sanal ortamın güvenli hale getirilmesi için gerekli olan tüm önlemlerin kendileri açısından yeni ticari fırsatlar doğurduğunu görmektedirler. İnternetle ilgili yapılacak her bir düzenlemenin ve alınacak önlemin yazılım ve donanım açısından yeni ticari ürünlere gereksinim meydana getireceğini

ve bunun yeni pazarların ortaya çıkmasına ve dolayısıyla kendilerine yeni ticaret alanlarının açılmasına neden olacağını farketmektedirler.

Ayrıca, sanal ortamın güvenli hale getirilmesiyle ilgili önlem alınması ve düzenleme yapılmasının kaçılmaz olduğunu gören ticari firmalar, bu sürece aktif katılım sağlamayı ticari çıkarları açısından daha doğru bir strateji olarak görmektedirler. Böylece, bu süreçte yeni fırsatlar oluşturmak ve olası zararlarını minimumda tutmak için ön almayı ve insiyatif kullanarak belirleyici olmayı daha doğru bir hareket tarzı olarak benimsemektedirler. Yani, bu alanda kurallar konulacaksa, bu kuralları da kendileri belirlemek istemektedirler.

Tüm bu sebepler, İnternet sektöründe yer alan firmaların öz düzenleme olarak adlandırılan bu yönetsel yaklaşımı ortaya çıkarmıştır. Bu yaklaşımda, İnternet dünyasının ticari tarafında olan ISS'ler, yer ve erişim sağlayıcılar gönüllülük esasına göre örgütlenmekte ve güvenli İnternet oluşturulmasına yönelik önlemleri, içerik filtreleme ve erişim engellemelerini bu örgütler eliyle yapmaktadırlar. Örneğin, Kanada, Danimarka, Norveç, İsveç ve İngiltere gibi bazı ülkelerde ISS seviyesindeki filtreleme sistemleri öz düzenleme şeklinde uygulanmaktadır (Bayzan, 2011: 68-70).

Benzer şekilde, AB uygulamalarında da genel olarak bu yöntemin tercih edildiği görülmektedir.³¹ AB Komisyonu'nun Güvenli İnternet Programları kapsamındaki kararları öz düzenlemeye yönelik tedbirleri desteklemek amacıyla oluşturulmuştur. Öz düzenleme uygulamalarında, hükümetler, ISS'ları üzerinden "gönüllülük" esasına göre kararların uygulanmasını hedeflemektedir. Bu çerçevede, AB ülkelerinde faaliyette bulunan gerek mobil gerekse de sabit İnternet hizmeti sunan işletmeciler, çocukların ve gençlerin güvenli İnternet kullanımına yönelik çalışmalar yapmakta ve alternatif hizmetler sunmaktadır.

³¹ Bkz. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31996F0443:EN:HTML>; http://aei.pitt.edu/5895/01/001527_1.pdf; <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:41997X0306:EN:HTML>; http://ec.europa.eu/information_society/activities/sip/archived/docs/pdf/programmes/decision/IAP_Decision_en.pdf (25.03.2012).

Bu kapsamda Avrupa ülkelerinde genelde erişim engellemesi, konuya ilişkin açık bir mevzuat olmaksızın sivil toplum, polis ve ISS işbirliği ile “gönüllülük” kapsamında yapılmaktadır. Fakat, hükümetler, sektör temsilcilerini, içerik düzenlemeleriyle ilgili “zorunlu gönüllü” işbirliği yapma konusunda oluşturdukları baskılar ile zorlamaktadır. Hükümet temsilcilerinin, “gönüllülük” esası tesis edilemediği takdirde başka yaptırımların uygulanacağına yönelik beyanları doğrultusunda, İSS’leri gerekli tedbirleri “zorunlu gönüllü” olarak uygulamaktadırlar (Bayzan, 2011: 70-72).

Keza, ABD’de de İnternet ortamında işlenen çocukların cinsel istismarı gibi belirli suçlara yönelik önleyici tedbirler alınması amacıyla, farklı adlarla da olsa sektörün içinden aktörlerin öz düzenleme yaklaşımıyla oluşturdukları yapıları teşvik etmektedir. Bu yapılar, genelde bağımsız ve özerk, fakat dolaylı olarak hükümetlere bağlı olarak içerik düzenlemesi faaliyetleri yapmaktadır (Çağlar, 2011: 115).

Öz düzenleme yaklaşımında kullanılan araçlar genellikle içerik filtreleme, derecelendirme ve ihbar merkezi uygulamaları olarak ortaya çıkmaktadır (Bakırcı, 2009: 12-17; Çağlar, 2011: 25-26):

a) *İçerik filtreleme*: Filtreleme, bir takım programlar kullanarak istenmeyen içeriğin engellenmesidir. Kara liste yöntemiyle belirli sitelerin engellenmesi, beyaz liste yöntemiyle belirli sitelere erişimin sağlanması, anahtar kelime blokesi, içerik izleme ya da bunların birleşiminden oluşan çeşitli prensiplere göre çalışmaktadır. Örneğin AB, hukuka aykırı veya zararlı içeriğin filtrelenmesi konusunu, öz düzenleme uygulamalarının önemli unsurlarından birisi yapmıştır. AB’nin içerik filtrelemeye ilişkin düzenleme esasları, tüm iletişim araçlarında insan haysiyetinin ve çocukların korunması amacıyla hazırlanan Yeşil Belge’de yer almıştır.³²

b) *Derecelendirme veya kategorizasyon*: Özellikle çocukları İnternetin zararlı içeriğinden korumak için İnternet sitelerine etiket vermek suretiyle derecelendirmesini sağlayan bir sistemdir. World Wide Web Consortium tarafından oluşturulan İnternet İçerik Seçimi Platformu (PICS-The Platform for Internet Content

³² Bkz. <http://www.ispo.cec.be/legal/en/Internet/gpen-toc.html> (22.10.2011)

Selection), bu sistemi saęlayanlardan en çok bilinenidir. PICS, küresel standardı oluşturmak için bu sektördeki firmalara ait bir girişim olarak ortaya çıkmıştır. PICS, filtreleme standartları yanında etiketleme sistemiyle siteleri kategorilere ayrılmakta ve ebeveynlerin site erişimlerine ilişkin kararlarına kaynaklık etmektedir. Sınıflandırmaları, değerlendirme (örneğin; çıplaklık, cinsel içerik, şiddet) ya da işaretler (farklı abonelerin ilgi ve uğraşlarına göre içeriğin belirlenmesi) gibi farklı bilgi tiplerine dayanmaktadır (w3.org, 2011). Bu yönüyle PICS'in, İnternet sitelerini düzenlemek ve İSS'ların müdahalesi olmaksızın içeriğin kontrol edilmesini saęlamak şeklinde önemli bir görev üstlendięi söylenebilir.

Bunun yanında, dünyada web sitelerinin derecelendirilmesi ile ilgili çalışmalarıyla bilinen en önemli kuruluşlardan birisi, FOSI (Family Online Safety Institute-Aile Çevrimiçi Güvenlik Enstitüsü)'nin bir parçası olan içerik saęlayıcıların özdenetim kuruluşu ICRA (Internet Content Rating Association-İnternet İçerik Derecelendirme Derneęi)'dir. FOSI, çocuklar ve ailelerine online dünyayı daha güvenli hale getirmek için çalışan kar amacı gütmeyen uluslararası bir kuruluştur (FOSI, 2011a).

ICRA, uluslararası çapta uygulanan bir etiketleme sistemi geliştirmiştir. Bu sistem, uluslararası bir çalışma grubu tarafından belirlenmiştir ve web siteleri dışında kalan diğer dijital içeriklere de uygulanabilmektedir. Etiketlemeye tabi içerikler ise şunlardır: Çıplaklık, cinsel içerik, şiddet, dil, kullanıcı tarafından üretilen içerik ya da kontrollü içerik, kumar, ilaç ve alkol gibi diğer zararlı içerikler. Derecelendirme bizzat içerik saęlayıcılar tarafından yapılmaktadır. İçerik saęlayıcılar kendi sitelerinde var olan veya olmayan içerikleri göz önünde bulundurarak sitelerinin derecesini bir sorgu formu doldurarak kendileri belirlemektedir (FOSI, 2011b).

Söz konusu uluslararası derecelendirme kuruluşları dışında, AB, ABD, Avustralya, İngiltere, Almanya, Singapur, Güney Kore ve Danimarka gibi birçok ülkede genellikle öz düzenleme yaklaşımıyla faaliyet gösteren derecelendirme kurum ve kuruluşları bulunmaktadır.

c) İhbar merkezi uygulaması: Öz düzenleme yaklaşımında İnternet kullanıcılarının şikayetleri ile İnternet içeriğinin denetlenmesini ve böylece yasa dışı içeriğin sunuculardan kaldırılmasını sağlayan önemli bir araçtır. Örneğin, 1999 tarihli Eylem Planı çerçevesinde (EU, 1999) hem AB nezdinde hem de her ülke kendi bünyesinde İnternet içeriğini takip eden ve sakıncalı içeriğe ilişkin ihbarlar alan merkezler kurulmuştur.³³ Yine, bazı STK'larının girişi ve devletlerin işbirliğiyle, dünya genelinde faaliyet gösteren ihbar merkezleri arasında iletişimi sağlamak amacıyla bazı ana ihbar merkezleri kurulmuştur(Kaya, 2010:57). Bu birliklerden en yaygın ağı sahip olanı INHOPE (The International Association of Internet Hotline Providers) isimli birliktir. Birliğin, 37 ülkede 43 üye ihbar birimi vardır (INHOPE, 2012).

Bu ana ihbar merkezleri sakıncalı içerikle mücadele konusunda önemli bir olanak sağlamaktadır. Şöyle ki; herhangi bir sakıncalı içerik bir ülkede engellense bile, o içeriğin dünya genelindeki erişimi devam etmektedir. Söz konusu içeriğe erişimin tamamen engellenmesi için içeriğin barındırıldığı sunucuya ait erişimin, sunucunun bulunduğu ülkeye engellenmesi gerekmektedir. İşte bu tür ana ihbar merkezleri, üye ülkelere sakıncalı içerik olarak erişimi engellenen web sitelerine ilişkin verilerin ortak bir veritabanı üzerinden paylaşılmasına olanak sağlayarak, söz konusu içeriklerle mücadele konusunda ülkeler arasında işbirliği imkanı sunmaktadır. Örneğin, ABD'de barındırılan fakat Almanya tarafından erişimi engellenen bir içerik hakkında, bu ihbar merkezleri üzerinden ABD'ye haber verilmesi durumunda, içeriğin ABD tarafından tamamen engellenmesi ve bir suç varsa faillerin tespit edilerek cezalandırılması sağlanabilmektedir (Kaya, 2010: 58).

Bazı uzmanlar, söz konusu öz düzenleme araçlarının kullanımının gerekliliğini savunarak, bu yöntemin alternatif bir yaklaşım oluşturduğunu, uygulanabilirliğinin ve esnekliğinin daha fazla olduğunu ve devletin doğrudan müdahalesinin hantallığı ortaya çıkardığını belirtmektedir (Bakırcı, 2009: 15-16; Akdeniz, 2003: 55-56). Bu görüşlerin aksini savunanlar da bulunmaktadır. Bunlar, İnternet kullanıcılarının çeşitliliğinin fazlalığı, bu kuralların uygulanmasında herhangi bir yaptırımın

³³ AB'nde yer alan ihbar merkezleri için bkz., http://ec.europa.eu/information_society/activities/sip/projects/centres/index_en.htm (25.03.2012).

bulunmaması, sektör tarafından her zaman kamu yararının gözetilmeyeceği ve kullanılan araçların maliyetli olması gibi nedenlerin, hukuka aykırı ve zararlı İnternet içeriği ile mücadelede söz konusu araçların kullanım olanağını azalttığını ve bu alanda kuralların oluşturulup uygulanmasını güçleştirdiğini öne sürmektedir (Bakırcı, 2009: 14; Akdeniz, 2003: 56-58).

Bazıları ise konun hukuki boyutuna dikkat çekmekte ve öz düzenleme sonucu yapılan erişim engellenme ve içerik çıkarma uygulamalarının mahkeme kararına dayanmaması sebebiyle hukuka aykırı olduğunu ileri sürerken (Marzouki, 2006), yasa dışı ve zararlı içeriği belirlemede öz düzenleme araçlarından İSS'lar ve ihbar merkezlerinin yetkili olmadığını savunmaktadır (Akdeniz ve Altıparmak, 2008: 72).

Bu noktada, öz düzenleme ile devlet düzenlemesi yaklaşımlarının siyah ve beyaz gibi birbirlerine zıt iki kavram olarak görülmemesi gerektiği hatırlatılmaktadır. Buna göre, ikisi arasından birisini tercih etme anlayışından ziyade, ikisi arasında doğru bir denge kurmaya çalışma yaklaşımı daha çok tercih edilmelidir. Öz düzenleme ile bir kesimin ticari çıkarlarının, konunun içinde yer alan diğer aktör ve tarafların aleyhine korunmasına izin verilmemesi, tüm tarafların çıkarlarının mümkün olan en üst düzeyde korunması gerekmektedir. İşte bu denge ve işbirliği noktasının yakalanabilmesi ve sürdürülebilmesi için yasal düzenlemelerle desteklenen bir “birlikte düzenleme” yaklaşımına gerek vardır. Aksi halde, bir takım zayıflıklar, piyasalarda çarpıklıklar veya kamu güveninin olmadığı, etkin ve adil olmayan bir takım düzenleme ve uygulamalar ortaya çıkabilir (Akdeniz, 2003: 58).

2.2.3 Birlikte / Ortak Düzenleme (Co-Regulation)

“Birlikte/Ortak düzenleme (co-regulation)” olarak adlandırılan başka bir yönetim modelinde ise, kamu kurumları, sektör temsilcileri ve STK'lar işbirliği yaparak, birlikte aralarında kuracakları bir mekanizma ile İnternet içeriğini düzenlemeleri söz konusu edilmektedir. Bu şekilde, devlet düzenlemesi ile öz düzenlemenin birlikte uygulanabileceği ve birbirini destekleyebileceği bir ortak zeminde her iki yaklaşımın

tek başına uygulanmasından kaynaklanan dezavantajların bertaraf edileceği ve avantaja çevrileceği düşünülmektedir (Çağlar, 2011: 27).

Birlikte düzenlemenin amacı, sektörde söz sahibi olanlar ile devlet ve hukuk uygulayıcıları arasında güçlü bir işbirliği geliştirerek, yasalaştırmaların öngörülebilirliği ile bağlayıcı özelliğini, daha esnek olan öz-düzenleme yaklaşımıyla birleştirmektir. Birlikte düzenleme sisteminin uygulanmasıyla, bir yandan düzenlemelerin meşruiyeti güçlendirilerek kamusal sürecin açıklığı ve saydamlığı temin edilirken, diğer yandan, öz düzenleme sürecinin uzmanlık ve esnekliği düzenlemelerde yansımaları bulacaktır. Ayrıca, sorumlulukların taraflar arasında paylaşarak yerine getirilmesinin zemini de oluşacaktır. Dolayısıyla bu sistem, düzenlemelere ilişkin inanırlılığı artıracak, devletin idari giderlerini azaltacak, esnekliği sağlayacak, uygulanabilirliği güçlendirecek ve ihtiyaçlara ve sorunlara isabetli çözümler getirecektir (Akdeniz, 2003: 60-61).

Ortak düzenleme ile ilgili olarak iki farklı yaklaşımdan bahsedilmektedir. İlkinde, özel sektör tarafından oluşturulan öz düzenlemenin devlet tarafından kontrol edilmesi ve onanması şekliyle bir birlikte düzenleme öngörülürken; diğerinde, özel sektör ile devletin sorumluluk paylaşımına giderek kendi alanlarında kurallar oluşturması usulüyle bir birlikte düzenleme anlayışı söz konusudur (Bakırcı, 2009: 18-19).

Diğer yandan, ortak düzenlemenin, öz düzenleme yönteminin yetersiz kaldığı durumlarda devlet düzenlemesinin devreye alındığı sistem olarak görüldüğünü de vurgulamak gerekmektedir. Yani, İnternetin zararlı ve yasa dışı içeriği ile mücadelede STK'ların ve özel sektörün yetersiz kalması durumunda devletin aktif müdahalesi ve düzenlemesinin devreye girmesi söz konusu edilmektedir (Bakırcı, 2009: 18-19). Ancak, diğer düzenleme yöntemlerinin, devlet düzenlemelerini tamamlayan ek bir araç olarak da görülebileceği belirtilmektedir. Buna göre, sorunların çözümünde yasalaştırma yönteminin tek başına etkili olmaktan uzak olacağı, böylesi tek parçalı bir yasalaştırmayı desteklemek için öz veya ortak düzenleme uygulamalarının gerekli olduğu vurgulanmaktadır (Akdeniz, 2003: 51).

Sonuç olarak, içerik düzenlemesine ilişkin yönetsel yaklaşımlar bir bütün olarak değerlendirildiğinde bazı noktaların ön plana çıktığını görmekteyiz. Genelde İnternetle, özel de ise İnternet içeriğinin düzenlenmesi ile ilgili konularda, İnternetin kendine özgü yapısından dolayı devletlerin tek başlarına yeterli düzenlemeler yaparak sonuç almaları mümkün gözükmemektedir. Bu konuda yasal düzenlemeler her ne kadar var olan sorunların çözümünde en önemli belirleyici ve yönlendirici faktör olsa da, çağın gereği, bu alanda devletin tek başına düzenleme yapması ve yasalar çıkarması yerine; daha demokratik yaklaşımlarla hareket etmesi, işbirliği, koordinasyon, danışma, birlikte düzenleme ve öz düzenleme gibi yeni konulara da önem vermesi gerekmektedir. Devletler, bu alana ilişkin düzenlemeler yaparken ve politikalar belirlerken riskleri dikkatle değerlendirmeli, açık ve saydam olmalı ve konunun taraflarının sürece katılımını sağlamaya çalışmalıdır (Akdeniz, 2003: 63).

Gelinen bu noktada, yapılan tartışmalar ve değerlendirmeler tezin dokuzuncu alt hipotezini test edecek mahiyette ele alındığında, söz konusu hipotezin doğruluğunun ve geçerliliğinin ispat edildiği söylenebilir. Zira, eldeki veriler İnternet içeriğinin düzenlenmesi ve yasadışı ve zararlı içerikle mücadele konusunda, birlikte/ortak düzenleme yönteminin ve bu kapsamda yönetim modelinin en etkili ve isabetli yönetsel araç olduğu görülmektedir. Bunun yanında, tamamlayıcı ve mücadeleyi daha da etkin bir hale getirecek öz düzenleme girişim ve uygulamalarının desteklenmesi ve teşvik edilmesi de önem taşımaktadır. Buna göre, İnternet içeriğinin düzenlenmesiyle ilgili olarak devletlerin yönetim modelini esas alan kamu yönetimi politikalarını benimsemeleri en doğru seçenek olarak gözükmemektedir.

2.3 İÇERİK DÜZENLEMESİNDE TEMEL YÖNTEMLER

İnternette 650 milyona yaklaşan web sitesi içinde milyonlarca yasadışı ve zararlı içerik bulunmaktadır. Ülkeler, İnternetin güvenli kullanımı ve yasadışı ve zararlı kabul ettikleri İnternet içerikleriyle mücadele etmeye yönelik faaliyetlerinde farklı yöntemler kullanmaktadırlar. Bu yöntemleri, filtreleme ve erişim engelleme yöntemleri ile bunların dışında kalan pozitif yöntemler olarak ayırabiliriz. Filtreme ve erişimin engellenmesine ilişkin yöntemleri ise söz konusu engellemeleri aşmada

kullanılan karşı yöntemlerle birlikte ele almak konun gerçek boyutlarının daha iyi anlaşılması açısından faydalı olacaktır. Keza, söz konusu veriler, tezin onuncu alt hipotezinde savunulan görüşlerin tartışılmasına ve değerlendirilmesine yarayacaktır.

2.3.1 Filtreleme ve Erişim Engelleme Ve Engellemeyi Aşma Yöntemleri

Devletlerin birçok farklı sebeple ve yöntemle İnternet içeriğine müdahale ettikleri, kısıtlayıcı önlemler aldıkları; bu kapsamda İnterneti filtre ettikleri ve erişim engelleme uygulamalarına gittikleri görülmektedir (Roberts vd., 2009: 3). Hatta, vatandaşlarının İnternet aktivitelerini takip etme ve izleme yolunu da tercih edebilmektedirler. Devletlerin suç algılaması, ekonomik ve teknolojik gelişmişliği, insan hakları, demokrasi ve hukuk devleti konusundaki hassasiyetleri bu tür uygulamaların çerçevesini belirlediği gibi, müdahale yöntemi ve kapsamını da değiştirebilmektedir (Çağlar, 2011: 12; Kaya, 2010: 21).

İlk olarak, İnternet içeriğine müdahale, filtreleme ve erişim engellemede devletlerin kullandıkları yöntemler teknolojik ve ekonomik gelişmişlikleriyle doğrudan ilgilidir. Nitekim, filtreleme ve erişim engelleme tekniklerinin uygulanması ileri teknoloji gerektirirken, yüksek maliyetli altyapı yatırımlarının karşılanması için de devletlerin ekonomik gelişmişlikleri önem kazanmaktadır. Bunun da ötesinde kullanılacak yöntem, filtreleme ve erişim engellemenin hangi düzeylerde gerçekleştirilmesi istendiğine; diğer bir deyişle, engellemenin kapsamı ve oranı konusundaki istek ve iradeye göre de değişmektedir. Tüm bunlarla ilgili belirleyici olan husus ise, devletlerin demokrasi ve insan hakları konularındaki yaklaşımları olmakta; engelleme sürecinin saydamlığı, hesap verilebilirliği, etkin koruma mekanizmalarının işlerliği de bu durumdan doğrudan etkilenmektedir (Kaya, 2010: 21).

İşte bu etkenlere bağlı olarak, erişim engellemede kullanılan teknikler, engelleme süresi ve kapsamı, takip edilen süreçler devletten devlete değişmektedir. Bazı devletler bir tek yöntem kullanırken, bazıları birden çok yöntemi kombine şekilde kullanabilmekte ve hatta bazı baskıcı devletler hukuk dışı müdahale ve yöntemlere başvurabilmektedir (Kaya, 2009: 24). Örneğin, adına “Siber Çin Setti”denilen

benzersiz filtreleme sistemiyle (Wikipedia, 2011a) Çin, uluslararası sitelerin ve ülke içerisindeki İnternet sitelerinin filtreleneşinin kapsamlı ve karmaşık bir uygulamasını yapmaktadır (Çağlar, 2011: 12).

İnternette filtreleme ve erişim engelleme uygulamaları yaygın hale geldikçe, bu uygulamaları bertaraf etmeyi ve oluşturulan engelleri aşabilmeyi sağlayan araçların geliştirilmesi ve potansiyel kullanıcılara dağıtımı çalışmaları da hız kazanmıştır. Bu araçlar çoğunlukla İnternetin hükümetler tarafından yaygın bir şekilde filtrelendiği ülkelerde milyonlarca insan tarafından kullanılmaktadır (Roberts vd., 2009: 3).

2.3.1.1 Filtreleme ve Erişim Engelleme Yöntemleri

Filtreleme, yasa dışı veya zararlı İnternet içeriğinin süzülmesi ya da bu tür içeriği barındıran İnternet sayfalarının pasif hale getirilerek istenmeyen içeriğe erişimin herhangi bir şekilde engellenmesidir. Filtreleme programları kullanarak zararlı içerik barındıran İnternet sitelerinin tamamı filtrelenebildiği gibi, ilgili sitesinin sadece zararlı içerik barındıran bölümü de süzülebilmektedir. Keza filtreleme, ülke içerisinde veya ülke dışında yer sağlanan yasa dışı içeriğin kaldırılması, erişimin kısıtlanması veya içeriğe yönelik arama motorlarında sonuçların filtreleneşisi gibi çeşitli şekillerde ortaya çıkabilmektedir (Çağlar, 2011: 96). Filtreleme ve İnternet sitelerine erişimin engellenmesine ilişkin yöntemler, ana hatlarıyla teknik ve sosyo-ekonomik açıdan olmak üzere ikili bir sınıflandırmaya tabi tutulabilir.

2.3.1.1.1 Teknik Açıdan Erişim Engelleme Yöntemleri

Teknik açıdan filtreleme ve erişim engelleme yöntemlerini, engellenen kapsamı, uygulanan sistem ve kullanılan teknikler bakımından üçe ayırmak mümkündür.

2.3.1.1.1.1 Engellenen Kapsamına Göre

Filtreleme ve erişimin engellenmesi, İnternet ağı içerisinde bulunan İnternet omurgası, İSS'lar, kurumlar ve kişisel bilgisayarlar üzerinde yapılabilmektedir. Devletler, web sitelerine erişimi İSS'lar nezdinde teker teker engelleyebileceği gibi

ana İnternet omurgası üzerinden tek aşamada tüm ülke genelinde de engelleyebilirler. Devletlerin bu konudaki tercihlerini, coğrafi büyüklükleri, ülkede faaliyet gösteren İSS'ların sayısı, telekomünikasyon sektörünün özel sektöre açık olup olmaması gibi etkenler belirlemektedir (Kaya, 2010: 22).

İSS temelli engellemede, ülke genelinde faaliyet gösteren her bir İSS'in ilgili İnternet içeriğini engellenmesi sağlanmaktadır (Deibert vd., 2008: 12). Engellemenin etkili olabilmesi için, erişim engelleme kararının tüm İSS'lar tarafından aynı anda ve aynı teknikle uygulanması gerektiğinden, bu yöntem, ülke genelinde faaliyette bulunan İSS'ların az sayıda bulunduğu veya sektörün tamamının devlet tekelinde olduğu ülkelerde etkin bir şekilde kullanılabilir (Deibert vd., 2008: 33).

Bu yöntemde, erişim engellemelerinin tüm İSS'larca aynı anda, aynı tekniklerle ve aynı gelişmişlikte teknolojilerle uygulanmaması bazı sakıncaların ortaya çıkmasına neden olmaktadır. Bu durumda, engelleme kararlarının İSS'lar tarafından geç veya hiç uygulanmaması veya farklı teknikler ya da farklı gelişmişlikteki teknolojilerle uygulanması, farklı İSS'lara bağlı kullanıcılar için eşitsizliğe neden olabilmektedir. Bir İSS'ya bağlı kullanıcılar birçok web sitesine erişim engelleme sebebiyle ulaşamazken, diğer İSS'ya bağlı kullanıcılar aynı sitelere ulaşabilmektedir (Kaya, 2010: 22-23). Keza, İSS'lar dışında İnternet omurgasından özel hatlar çekerek kullanıcılarına İnternet hizmeti sunan üniversiteler gibi kimi kuruluşların, İSS'lar vasıtasıyla yapılacak engellemelerden etkilenmemeleri de başka bir eşitsizlik durumu oluşturmaktadır (Çağlar, 2011: 13).

Erişim engelleme için kullanılan diğer bir yöntem olan ana İnternet omurgası üzerinden engellenmede, İSS'lardan bağımsız olarak ilgili içeriğe tüm ülke genelinde erişim engellenmektedir (Deibert vd., 2008: 12). Genellikle ülkelerin tercih ettiği yöntem, İSS'lar yoluyla erişimin engellenmesidir, lakin, olağanüstü zamanlarda erişimin engellenmesi İnternet omurgası üzerinden de yapılabilir. Örneğin, 2011'de Tunus'da başlayan ve "Arap Baharı" olarak adlandırılan süreci başlatan halk gösterilerinden sonra, bu süreçten etkilenen birçok Arap hükümeti İnternet omurgasını kullanarak İnternete erişimi engellemiştir (Çağlar, 2011: 13).

İnternet omurgası üzerinden engellenme yönteminde, tüm ülke genelinde aynı anda ve seviyede içeriğe erişim engellenmektedir (Kaya, 2010: 23). Fakat, bu yöntemde bazen beklenmedik sorunlarla karşılaşılabilir. Mesela, her türlü erişim engellemenin hem İSS'lar hem de ana İnternet omurgasında yapıldığı Pakistan'da (Deibert vd., 2008: 13), 2008 yılında "kutsal değerlere hakaret eden" videolar nedeniyle Youtube'a İnternet omurgası üzerinden erişim engellenmeye çalışılırken yanlış bir ayarlamadan dolayı dünya genelindeki ana İnternet omurgasında teknik bir problem oluşmuş ve tüm dünyada iki saat süreyle Youtube sitesine girilememiştir (CNN, 25.02.2008). Keza, Suriye ve BAE'nin İsrail'in üst düzey alan adı olan ".il" uzantısını engellemesi, her üç ülkenin İnternet trafiğini etkilemiş ve İnternet sitelerine erişimde teknik aksamalara neden olmuştur (OpenNet, 07.08.2009a).

2.3.1.1.1.2 Engelleme Sistemine Göre

Engelleme sistemine göre, otomatik engelleme veya bireysel engelleme yöntemlerinden birisi kullanılabilir. Otomatik engelleme yönteminde, içeriğini doğrudan ilgili kamu kurumlarının oluşturduğu veya filtreleme yazılımları üreten şirketlerin belirlediği, sakıncalı görülen web siteleri için ulusal bir blok liste ve veritabanı oluşturulmaktadır (Deibert vd., 2008: 38). Düzenli olarak güncellenen bu veri tabanları, sakıncalı içerikler için referans kabul edilerek otomatik engellemeye tabi tutulmaktadır (Kaya, 2010: 29). Bireysel engellemede ise, her bir site için ayrı ayrı engelleme kararı alınmakta ve bu kararlar mahkemeler veya ilgili kamu yetkililerince uygulanması için ülkede faaliyet gösteren her bir İSS'ya veya yer sağlayıcıya gönderilmektedir (Kaya, 2010: 29).

2.3.1.1.1.3 Kullanılan Tekniğe Göre

Devletler, teknolojik gelişmişlikleri yanında benimsedikleri politikalara göre farklı filtreleme ve erişim engelleme teknikleri kullanmaktadır. Devletlerin uyguladıkları filtreleme ve erişim engelleme yöntemi ve yoğunluğunu, ülkenin içinde bulunduğu siyasal, hukuki, dini ve sosyal düzlemleri göz önünde bulundurarak değerlendirmek gerekmektedir (Deibert vd., 2008: 3). Tüm bu etkenlerin şekillendirmesine göre bazı

devletler IP veya alan adı engellemesi gibi yöntemlerle yetinirken, bazıları farklı katmanlardan oluşan kombine teknikler kullanmaktadır (Kaya, 2010: 31).

Şu da bir gerçektir ki, giderek artan eğilim daha sofistike teknikler kullanarak daha fazla yerde ve daha fazla engelleme yapmak yönünde olmasına rağmen, filtreleme ve erişim engellemede yüzde yüz başarılı bir teknik bulunamamıştır (Deibert vd., 2008: 34). Bu amaçla kullanılan her bir teknik kendi içinde güçlü ve zayıf yönler barındırmaktadır (Kaya, 2010: 31). Sonraki bölümlerde de görüleceği gibi, dünyanın en gelişmiş filtreleme ve erişim engelleme sistemlerine sahip olan Çin ve Suudi Arabistan devletleri bile birçok içeriği engellemede başarısız olmaktadır. İnternet içeriğinin hızla değişmesi ve içeriğin değişik web sitelerine yayılması çoğu zaman engellemeyi olanaksız kılmaktadır. Keza, her bir teknik engelleme ilgisiz web sitelerini engelleyebileceği için aşırı engelleme veya tam aksine ilgili web sitelerini engelleyememe nedeniyle de etkisiz engelleme riski taşımaktadır (Deibert vd., 2008: 66). Bu nedenlerle devletler kullandıkları teknolojinin mükemmel olmasından ziyade etkili olmasına önem vermektedir (Goldsmith ve Wu, 2006: 103).

Kullanılan tekniğe göre yaygın olarak kullanılan başlıca erişim engelleme yöntemleri şunlardır IP Yoluyla Engelleme, Alan Adı Yoluyla Engelleme, URL Yoluyla Engelleme, Proxy Engellemesi, İçerik Engellemesi, DDOS Atakları, Alan Adı İptali Yolu ile Engelleme, Fiziksel Sunucu Müdahalesi Yoluyla Engelleme ve Ağ Hatası Gösterme Yoluyla Engelleme (Kaya, 2010: 27-39).

2.3.1.1.1.3.1 IP Yoluyla Engelleme

Erişim engellemenin en kolay yöntemi, istenmeyen içeriğin bulunduğu sunucunun IP adreslerinin engellenmesidir (Roberts vd., 2009: 11). Bu yöntemde, kapsam bakımından tercihe göre ya her bir İSS nezdinde ya da ana İnternet omurgasında web sitesinin IP adresinin engellenmesi sağlanmaktadır (Kaya, 2010: 32). IP numarasını engelleme yönteminde, erişimin engelleneceği yer sağlayıcısına ait IP numaraları erişim sağlayıcılara gönderilmekte, erişim sağlayıcılar da bu IP numarasını

engellemekte veya gelen talepleri erişimin engellendiği belirtilen sayfaya yönlendirmektedir (Akgül, 2010: 291).

IP engelleme, büyük ağlarda filtreleme yapabilen basit bir yöntemdir (Roberts vd., 2009: 11). Basit bir yöntem olması ve ek bir donanıma ihtiyaç duymaması ve maliyet getirmemesi nedeniyle IP engelleme yöntemi, hem devletler hem de İSS'lar ve erişim sağlayıcılar tarafından genellikle tercih edilmektedir (Kaya, 2010: 32).

Bunun yanında, IP engellemesi yöntemi taşıdığı birtakım sakıncalardan dolayı etkin bir erişim engelleme tekniği değildir. Nitekim, istenmeyen içeriğin bulunduğu sunucunun IP'sinin engellenerek bu sunucuya erişimin tamamen durdurulması, aynı sunucuda bulunan belki binlerce masum siteyi de otomatik olarak engelleme sonucunu doğurmaktadır (Roberts vd., 2009: 11; Deibert vd., 2008: 59). Bu durumun, temel bir ceza hukuku ilkesi olan suçta ve cezada şahsılık ilkesinin açık bir ihlalini oluşturduğu dile getirilmektedir (Kaya, 2010: 32).

Diğer yandan, ilgili sitesinin kısa sürede başka bir sunucu ve IP adresi üzerinden yayın yapmasının mümkün olması, hatta bazı durumlarda, sunucu değiştirmeye bile gerek olmadan IP değişikliğine gitmenin teknolojik olarak mümkün olduğu gözönüne alınırsa, IP engelleme yönteminin etkin bir yöntem olmadığı görülecektir. Bu nedenlerle, IP engelleme yönteminin, engellenecek web sitenin özellikleri göz önüne alınarak diğer yöntemlerle kombine şekilde kullanılması durumunda etkin olabileceği söylenebilir (Kaya, 2010: 32).

2.3.1.1.1.3.2 Alan Adı Yoluyla Engelleme

Alan adları düz metinlerdir ve genelde son kullanıcılar tarafından bir web sitesine erişim için kullanılırlar (www.google.com gibi). DNS sunucuları, DNS adlarını IP adresine çevirir. Bu DNS sorgularını engellemek için ülkenin DNS sunucularından bu DNS bilgilerinin çıkarılması gerekir. Böylece kullanıcıların erişim istenmeyen sunucuların DNS adlarına bakılması engellenmektedir (Roberts vd., 2009: 12).

Diğer bir anlatımla, herhangi bir alan adına erişimi engellemek için kullanıcı tarafından bu sunucular üzerine gönderilen istekler sunucu üzerinde yapılacak bir konfigürasyon marifeti ile cevapsız bırakılır veya başka bir IP adresine yönlendirilir. Bu şekilde sunucu üzerinden beklenen yanıt alınamayacak ve siteye erişim gerçekleştirilemeyecektir (Çağlar, 2011: 20). Bazen de, DNS sunucularına alan adı ile ilgili farklı bir kayıt girilmekte, böylece ilgili alan adına ulaşmak isteyenler erişimin engellendiği belirtilen sayfaya yönlendirilmektedir (Akgül, 2010: 290-291). Sonuçta alan adı doğru IP adresine gitmediği sürece İnternetin bir değeri olmayacaktır (Goldsmith ve Wu, 2006: 168). Bu sistemin bir avantajı, her bir İSS nezdinde uygulanacak DNS engellemesi yöntemi ile, kullanıcı erişim sorgusunun İnternet trafiğine ulaşmadan önce sorgunun engellenmesi ve bu şekilde ağ trafiğinin hafifletilmesini mümkün kılmasıdır (Kaya, 2010: 30).

DNS engellemede de en büyük problem alan adını tüm alt içeriği ile erişime kapattığı için aşırı engelleme yapmasıdır. Engellenen sitenin sadece birkaç sayfası değil, sitenin tümü engellenmektedir (Roberts vd., 2009: 12; Deibert vd., 2008: 60). Bu nedenle, dünya ölçeğinde yayın yapan ve milyonlarca İnternet kullanıcısına ücretsiz blog, e-posta veya benzeri hizmetler veren web sitelerinin bu yöntemle engellenmesi bazen ağır sonuçlar doğurabilmektedir. Tüm alan adı engellendiği için belki de içeriğin büyük çoğunluğunu oluşturan sakıncalı olmayan içerik erişime kapatılmakta ve bu durum tıpkı IP engellemesinde olduğu gibi suçta ve cezada şahsılık ilkesinin ihlal edilmesine neden olmaktadır (Kaya, 2010: 30).

Bununla birlikte DNS engelleme aynı IP üzerinde barınan birden çok web sitesinin hepsinin engellenmesi problemini doğurmaz. Örneğin “aaa.com” ve “bbb.com” adlı iki site aynı IP adresi üzerinde host ediliyorsa, DNS engelleme “aaa.com”u engellerken “bbb.com”a erişim devam eder. IP engelleme ise bu durumda “aaa.com” ve “bbb.com”un her ikisini de engeller (Roberts vd., 2009: 12).

2.3.1.1.1.3.3 URL Yoluyla Engelleme

URL, bir İnternet sitesinde (<http://www.abc.com.tr>) ulaşmak istenilen belge, resim ve benzeri bir dosyanın üzerine tıklandığında adres çubuğunda (browser) beliren (<http://www.abc.com.tr/dokuman/alitesi.html>) adrestir. İnternet üzerinden erişilen URL uzantısının, belirli kurallar çerçevesinde ve özel yazılım veya donanımlar ile sınıflandırılması, daha sonra istenmeyen uzantıların bloklanarak erişiminin engellenmesi işlemi “URL yoluyla engelleme” olarak adlandırılmaktadır (Çağlar, 2011: 16). URL yoluyla engellemede, tüm kullanıcıların ortak kullandığı ağ geçitleri olan vekil sunucu (proxy server), yönlendirme cihazı (router) vb. üzerinden akan tüm trafik analiz edilir ve engellenmesi istenen adresleri içeren veritabanı kullanılarak erişimi engellenecek URL uzantıları tespit edilerek erişim engellenir. Yani bu yöntemde, belirli alan adları kara listeye alınır ve bu adreslere girildiğinde erişim sağlanamaz (Çağlar, 2011: 17).

Bu yöntemin en önemli avantajı, hukuka aykırı veya zararlı bir içerik için tüm sitenin erişiminin tamamen engellenmesi yerine, sadece ilgili URL uzantısında yer alan resim, yazı veya müzik gibi bir dosyanın engellenmesidir. Böylece, bir İnternet sitesinde yer alan ve engellenmek istenen bir veya birkaç dosya engellenirken, o sitesinin kullanımı tümüyle ortadan kaldırılmamış olmaktadır (Çağlar, 2011: 16-17).

Bununla birlikte, URL yoluyla erişim engellemenin bazı dezavantajları da vardır. Bu yöntem, çeşitli teknik nedenlerle yüzde yüz engelleme yapamadığı için genellikle yetersiz kalırken, İnternet trafiğini yavaşlatmakta ve ekstra yatırım yapmak ve fazladan insan kaynağı ayırmak gibi mali külfetler getirmektedir (Çağlar, 2011: 17). Ayrıca, URL engelleme, özellikle üçüncü şahısların verileri de dahil her verinin teker teker incelenmesini gerektirdiğinden kişisel verilerin gizliliğini ihlal sorunu da oluşturmaktadır. URL engelleme ile her veriye her İnternet noktasında hukuka uygunluk denetimi yaptırmış olunmaktadır. Bu nedenle protokolün detaylarına girilmekte, diğer bir ifade ile İnternet trafiğindeki her bir paket tek tek incelenmektedir. Bu durum özellikle İnternetin global ağ olmasını sağlayan "ağ tarafsızlığı" ilkesini de zedelemektedir (Berber ve Kaya, 01.12.2010). Diğer yandan,

bir sunucu üzerinden yayınlanan yasaklı URL adreslerinin birkaç saniye içinde değiştirilerek engellemeden kurtulabilmeleri bu yöntemin etkinliğini azaltmaktadır.

2.3.1.1.1.3.4 Proxy Yoluyla Engelleme

Proksi (proxy) İnternet içeriğine erişim için kullanılan bir ara sunucudur (Wikipedia, 2012b). Vekil sunucu olarak da bilinen proksi, kullanıcının bilgisayarını ile İnternet arasında yer alan bir aracı bilgisayardır (Java, 2011). Proxy sunucu erişilmek istenen veriyi önbelleğine aldığı için kullanıcılar web sitelerine daha hızlı şekilde erişirler ve gereksiz ağ trafiğinin kullanılmasının önüne geçilmiş olur (Kaya, 2010: 32). İnternetteki içeriğe doğrudan bağlanmak istenilmediği durumlarda, doğrudan bağlanmanın sakıncılarını bertaraf etmek için devletler proxy sunucu kullanmaktadır. Proxy sunucusu içerik ve kullanıcı arasında filtreleme görevi üstlendiği için kullanıcının istenmeyen içerikle veya virüs, solucan ve truva gibi kötücül yazılımlarla karşılaşma riskini ortadan kaldırmaktadır (Deibert vd., 2008: 61).

Ayrıca, vekil sunucular içerik ve kullanıcı arasında yer aldıkları için, asıl kullanıcının kimliğinin gizlenmesine de imkan sağlamaktadır. Bu avantajları nedeniyle, proxy sunucuları üniversiteler ve kütüphaneler gibi İnternetin ücretsiz ve ortak kullanıma açık olduğu alanlarda yaygın olarak kullanılmaktadır. Devletler de bu sunucuları İnternet bağlantı noktalarına konumlandırarak içeriğe müdahale edebilmekte; içeriği filtreleyebilmekte ve kişilerin hangi web sitesine veya ne tür içeriğe erişeceğini belirleyebilmektedir (Deibert vd., 2008: 61). Bu şekilde proxy sunuculardaki güvenlik duvarı erişim engellemesi amacıyla kullanılmaktadır (Java, 2011).

2.3.1.1.1.3.5 İçerik Engelleme

IP ve DNS engelleme teknikleri kullanılarak TCP/IP protokolü altında belirli bir noktaya gönderilen veya belirli bir noktadan alınan veri parçacıklarının engellenmesi sağlanmakla birlikte veri içeriğine müdahale edilmemektedir (Kaya, 2010: 32-33). Hem URL hem alan adı hem de veri içeriğine ağda otomatik olarak müdahale edebilmek için ağ sisteminin yazılımsal ve donanımsal olarak değiştirilmesi gerekmektedir (Deibert vd., 2008: 59).

Bir takım filtreleme programları kullanılarak veri içeriğine otomatik olarak müdahale edilebilmektedir. Nitekim, bu engelleme tekniğinde filtreleme amaçlı olarak router programlama sistemi kullanıldığında, routerların ağ üzerinde belirli kelimeleri içeren veri parçalarını denetlemeleri sağlanabilmektedir. Bu şekilde, kelime, URL veya alan adı temelli olarak inceleme yapılması ve tespit edilen içeriğin engellenmesi mümkün olmaktadır (Kaya, 2010: 33; Roberts vd., 2009: 12).

IP ve DNS engelleme ile kıyaslandığında, anahtar sözcük engelleme teknik olarak çok daha masraflı ve zordur. Bir anahtar sözcük filtresi, iletilen verinin bütününe incelemek ve bu büyük miktardaki verinin içinde metin araması yapmak zorundadır. Herşeye rağmen Çin’inde dahil olduğu bir kaç ülke, anahtar sözcük engellemesini geniş kapsamlı olarak yapmaktadır (Roberts vd., 2009: 12).

Diğer yandan, anahtar sözcük temelli içerik engellemesi aşırı engellemelere de sebep olabilmektedir. Örneğin, bu sistemde, İngiltere’de bulunan Essex ve Sussex Üniversiteleri alan adlarında yer alan “sex” kelimesi (<http://www.essex.ac.uk>., <http://www.sussex.ac.uk>.) nedeniyle cinsel içerikli web sitesi olarak erişim engellemeye uğrayabileceklerdir. Keza, cinsel hastalıklar konusunda bilgi veren bir sağlık sitesi de aynı tür bir engellemeye muhatap olabilecektir (Kaya, 2010: 34).

Nitekim, engellememesi gereken faydalı siteleri engellerken, engellememesi gerekenleri de başarılı bir şekilde engelleyememesi, performans ve hızın önemli ölçüde düşmesine neden olması, pratik olmaması gibi sebeplerle merkezi içerik filtreleme uygulaması sıkça eleştirilmektedir.³⁴ Diğer yandan, web sitelerinin içeriğinin filtrenin okuyamayacağı şekilde şifreli olarak sunulduğu durumlarda, anahtar sözcük engelleme sistemleri çaresiz kalmaktadır. Böylece şifresiz “http” isteği engellenirken, aynı veri şifreli “https” ile iletilirken engellenmesi mümkün olmamaktadır (Roberts vd., 2009: 12).

³⁴Bkz. http://www.uknof.org.uk/uknof5/Clayton-Content_filtering.ppt; <http://www.theage.com.au/news/web/isplevel-filters-unworkable/2007/08/10/1186530595566.html> <http://www.alia.org.au/advocacy/internet.access/internet.filtering.public.libraries.2007.survey.report.pdf>; <http://nla.gov.au/anbd.bib-an43012459>; http://www.efa.org.au/censorship/mandatory-isp-blocking/#SS_11.html (26.04.2012)

2.3.1.1.1.3.6 DDOS Atakları

Bazen devletler, ülke genelinde erişim engellemenin gereken faydayı vermediği veya siyasi muhaliflerin ya da terör örgütlerinin propagandalarını tamamen engelleme ihtiyacı duyduklarında, egemenlik alanları dışında kalan yabancı ağlarda barındırılan sitelerin erişimini tamamen engellemek istemektedir (Kaya, 2010: 34). Bu gibi durumlarda, kullanımı hukuka aykırı olsa da DDOS (Distributed Denial of Service- Dağıtılmış Hizmet Reddi) isimli ağ saldırı yöntemine başvurabilmektedirler (Deibert vd., 2008: 64).

DDOS atakları, bilişim sistemlerini işlemez hale getirmek için kullanılan ve ağ trafiğini tehdit eden en büyük siber saldırı yöntemidir. Bu yöntem, hem ağ sistemini çökertmek hem de sistemi gereksiz sorgularla meşgul edip normal işleyişini yavaşlatmak için kullanılmaktadır. DDOS saldırıları, virüs veya başka bir yöntemle birçok bilgisayarın belirlenmiş bir hedefe gereksiz komut göndermesiyle gerçekleştirilir. Aynı anda birden çok bilgisayarın hedefe saldırı yapması asıl saldırı yapanın kimliğinin tespit edilmesine de engel olur (Botfrei, 2012; Bora, 2008). Bazen haftalar hatta aylarca süren bu saldırılarda, aynı anda binlerce bilgisayardan milyonlarca sorgu alan ağ veya sunucu bu sorgulara yanıt vermekle meşgul olur ve saldırı sonucunda ya ağ tamamen çöker ya da bağlantı hızı yavaşladığı için erişim zorlaşır. Böylece, siteye erişim engellenmiş olur (Kaya, 2010: 35).

Nitekim, Kırgızistan'da 2005 seçimlerinde tüm muhalif partilerinin web siteleri, 2006 yılında da Belarus'daki seçimlerde 25 farklı İSS'da barındırılan 37 muhalif parti web sitesi DDOS atakları sebebiyle erişilemez hale gelmiştir. Muhalif partiler, bu saldırılardan dolayı iktidar partilerini suçlasalar da, bu tür saldırılarda failleri tespit etmek zor olduğu için bir neticeye varamamışlardır (Deibert vd., 2008: 41-42).

2.3.1.1.1.3.7 Alan Adı İptali Yolu ile Engelleme

Web sitesinin ülke kodlu üst-düzey alan adı kullandığı durumlarda (örn. .tr/.uk/.de vb.) alan adı iptali yolu ile erişimi engellemek mümkündür. Ülke üst-düzey alan adları ilgili devletler tarafından yönetilmektedir. Bir ülkeden İnternet hizmeti alan

birisinin o hizmetle ilgili ülkenin mevzuatını ve bu alanda yapmış olduğu düzenlemeleri kabul ettiği varsayılmaktadır (Kaya, 2010: 41). Bu çerçevede, bir ülkenin üst-düzey alan adını kullanan İnternet kullanıcısının, o ülkenin yasakladığı içerik nedeniyle alan adının iptali riskini de kabul etmiş olmaktadır (Deibert vd., 2008: 64). Nitekim, İngiltere’de çocukların cinsel istismarı ile ilgili alan adlarının, alan adı kayıt kuruluşlarınca iptali sağlanmakta ve bu içeriklerin arama motorlarında bulunması engellenmektedir (IWF, 2012).

2.3.1.1.1.3.8 Fiziksel Sunucu Müdahalesi Yoluyla Engelleme

İnternete bağlı her bir sunucunun fiziksel olarak bir mekanda barındırılması gerekmektedir. Sunucu barındırma hizmetleri ise devletlerin denetimi altında ülkelerin hukuk kurallarına göre gerçekleştirilmektedir. Bulunduğu ülkenin iç hukukuna göre aykırı içerik taşıyan bir web sunucusunun İnternet bağlantısı fiziksel olarak kesilerek barındırdığı içeriğe erişim engellenebilir (Deibert vd., 2008: 64).

2.3.1.1.1.3.9 Ağ Hatası Gösterme Yoluyla Engelleme

Web sitelerine erişilmeye çalışıldığında bağlantı hatası oluştuğunu gösteren mesajlar, erişim engelleme sıklıkla uygulanan başka bir yöntemi olarak karşımıza çıkabilmektedir (Deibert vd., 2008: 16). Ağ hatası oluştuğu mesajıyla karşılaşan ziyaretçiler, içerik ve hizmet sağlayıcılar siteye teknik bir sorundan dolayı erişilemediği yanılgısına düşmekte ve çoğu zaman sitelerinin erişim engellemeye uğradığının farkına dahi varamamaktadır. Özellikle, tüm İnternet ağının sadece devlet tarafından yönetildiği ve telekomünikasyon sektörünün devlet tekelinde olduğu ülkelerde bu yöntem etkin bir biçimde kullanılmaktadır. Devlet tekeli nedeniyle içerik veya İSS’leri, ağda ayrıntılı inceleme yaparak hatanın çözümlenmesini sağlayabilecek yetkilere sahip olmadığı için devlet müdahalesi ispatlanamamaktadır (Kaya, 2010: 36).

Bilinçli bağlantı aksamaları, olarak da adlandırılan bu yöntemde yukarıda bahsi geçen DDOS atakları da kullanılabilir. DDOS saldırıları ile kullanıcının

bağlanmak istediği siteye ya bağlanamıyor görüntüsü verilmekte ya da farklı bir siteye yönlendirme yapılarak erişim engellenmektedir (Botfrei, 2012).

2.3.1.1.2 Sosyo-Ekonomik Açıdan Erişim Engellenme Yöntemleri

Filtreleme ve erişim engelleme birbirini desteleyen ve güçlendiren sosyal, ekonomik, politik ve teknik metodları içermektedir (Roberts vd., 2009: 9). Bu nedenle devletlerin, filtreleme ve erişim engellemeye ilişkin politikalarında sosyo-ekonomik boyut önem arz etmektedir. Devletler, bazı nedenlerden dolayı doğrudan filtreleme ve engelleme yapmak yerine, bir takım başkaca sosyal ve ekonomik yöntemler kullanmak suretiyle sitelere erişimi fiilen zorlaştırmakta veya kullanıcıların oto-sansür uygulamalarını sağlamaktadır. Bireysel davranışlar üzerinde etkinlik kurularak sonuç alınmaya çalışıldığı için bu yöntemler sosyal teknikler olarak adlandırılmaktadır (Kaya, 2010: 36).

Filtreleme ve erişim engelleme uygulamaları ülkelerin vatandaşlarına hangi bilgilere erişmelerinin istenmediğini göstererek aslında bir tür sosyal baskı oluşturmaktadır. İnternetin sıkı takip altında olduğu ülkelere de kullanıcıların, istenmeyen sitelere eriştiklerinde tespit edilebileceklerini ve deşifre olabileceklerini bilmeleri sosyal baskıyı artırmaktadır (Roberts vd., 2009: 9).

Bahsi geçen sosyal yöntemlerin etkili olarak uygulandığı iki ülke, İnternet kullanıcılarının en yoğun kontrol edildiği Çin ve Güney Kore'dir. Çin'de İnternete giriş yapan her kullanıcı takip edilmekte ve kullanıcıların trafik kaydı tutulmaktadır. Bu durum kullanıcılara hatırlatılmakta ve kuralları ihlal edenlerin ihbar edilmesi gerektiği uyarısında bulunmaktadır.³⁵ Keza, benzer izleme ve kontrol etme yöntemleri Güney Kore'de de kullanılmaktadır.³⁶ Bu durum, her iki ülkede de İnternete bağlanan bireyler üzerinde psikolojik baskı oluşturulurken, girecekleri web sitelerine dikkat etmeye ve kendilerine oto sansür uygulamaya zorlamaktadır (Kaya, 2010: 37).

³⁵ “Çin Halk Cumhuriyeti” maddesine bkz.

³⁶ “Güney Kore” maddesine bkz.

Devletler, sosyal teknikleri uygularken erişim ve yer sağlayıcıları çeşitli usullerde takip ve kontrol ederek bir araç olarak kullanmaktadır. Bu çerçevede, birçok devlet erişim ve yer sağlayıcı olmayı izin sistemine tabi tutmuş, bunlara düzenli olarak faaliyetlerini devlete bildirme şartı getirmiş ve yürüttükleri hizmetlerle ilgili hukuki ve cezai sorumluluklar yüklemiştir (Kaya, 2010: 36). Sorumluluklarının artırılması erişim ve yer sağlayıcıları müşterileri kabul ederken daha seçici davranmaya zorlamaktadır (Deibert vd., 2008: 42). Öyle ki, erişim ve yer sağlayıcılar kendilerini hukuki sorumluluk altına sokmamak için muhalif web sitelerini barındırmaktan çekinmekte, forum sitelerinin yöneticileri de her türlü sakıncalı görülebilecek içeriği sistemden kaldırabilmektedir (Kaya, 2009: 38).

Aynı şekilde bazı web siteleri de bu sosyal yöntemlerin uygulanmasına gönüllü veya gönülsüz katkıda bulunabilmektedir. Şöyle ki; bu web siteleri kullanıcıların hangi ülkeden İnternete bağlandığını ya kullanıcıya siteye girişinde sorarak ya da IP dağıtım tabloları sayesinde kendileri tespit etmekte ve web sitesinde tespit edilen ülkeye özel sakıncalı bir içerik varsa, kullanıcının bu içeriğe erişmesini doğrudan engellenmekte veya içeriğin sakıncalı olduğunu kullanıcıya ihtar etmektedir (Kaya, 2009: 38). 2000 yılında, Nazi ürünlerinin satılmasına ilişkin olarak Yahoo aleyhine Fransa’da açılan davanın neticesinde, Mahkeme kararı gereği Yahoo’nun Fransız kullanıcılarına Nazi içeriğine erişimi zorlaştırması bu duruma bir örnektir.³⁷

Sosyal tekniklerin ne kadar etkili olduğunun diğer bir örneğini, filtrelenen ve erişimi engellenen içeriklere ulaşmak için mevcut engelleri aşabilmeyi sağlayan araçların kullanımının ülkesel yaygınlığı incelendiğinde görülmektedir. Buna göre, filtreleme ve erişim engelleme en yaygın görüldüğü ülkelerde, doğal olarak bu engelleri aşmaya yönelik teknolojilerin ve araçların, en azından girişim ve çabaların daha yaygın olması beklenir. Fakat aksine, aşılması zor filtreleme ve engelleme uygulayan ülkelerde, söz konusu engellemeleri aşabilmeyi sağlayan araçları kullananların toplam İnternet kullanıcıları içindeki oranının, daha az engelleme yapan ülkelerdeki oranlardan daha az olduğu görülmektedir (Roberts vd., 2009: 10).

³⁷ “Fransa” maddesine bakınız.

Bu konuda da en tipik örnek Çin'dir. Çin'in katı filtreleme ve erişim engelleme uygulamalarına rağmen, engellenen içeriğe ulaşabilmeyi sağlayan araçları kullananların sayısının az olması, yasaklı içeriğe erişen kullanıcıların nadiren de olsa tutuklanması veya yasaklarda ağır cezalar uygulanmasıyla toplum üzerinde oluşturulan sosyo-psikolojik baskıyla açıklanmaktadır (Roberts vd., 2009: 10).

Ayrıca, İnternete erişim ve bağlantı maliyetlerinin devlet politikası olarak yüksek tutulmasının devletlerin tercih ettiği ekonomik boyutlu erişim engelleme yöntemlerinden birisi olduğu da dile getirilmektedir. Bu çerçevede, İnternet abonelik ücretlerini arttırmak ve İnternetin hızını düşük tutmanın bir araç olarak kullanılabileceğine dikkat çekilmektedir (Çağlar, 2011: 22).

Diğer yandan, devletlerin erişim engelleme politikalarının bireyler üzerinde psikolojik etki meydana getirdiği bilinmekle birlikte, bu sonucu elde etmeye yönelik uygulanan sosyo-ekonomik tekniklerin etkinliğini, bireylerin bu konuda gösterdiği katılım ve direncin değiştirebildiğini de unutmamak gerekmektedir (Kaya, 2009: 39). Ayrıca, bahsi geçen sosyo-ekonomik teknikler, bu teknikleri kullanan devletlere, doğrudan engelleme yapmadıkları için ortaya çıkan durumdan sorumlu olmadıklarını ileri sürme imkanı da vermektedir. Fakat, kullanılan bu tekniklerin çoğu zaman, başta ifade hürriyeti, özel hayatın gizliliği, iletişim özgürlüğü olmak üzere çeşitli temel hak ve hürriyet ihlallerine neden olduğu görülmektedir (Kaya, 2009: 39).

2.3.1.2 Filtreleme ve Erişim Engellemesini Aşmada Kullanılan Yöntemler

İnternette filtreleme ve erişim engellemeler yaygın hale geldikçe, bunları aşabilmeyi sağlayan araçların geliştirilmesi ve potansiyel kullanıcılara dağıtım çalışmaları da hız kazanmıştır (The Citizen Lab, 2007). Söz konusu engelleri aşabilme teknolojisi halen etkilidir, çünkü İnternetin engellendiği ülkelerde bu araçlar, sayısı gittikçe artan İnternet kullanıcıları tarafından sıklıkla kullanılmaktadır (Roberts vd., 2009: 10). Keza, vatandaşların bu girişimleri kimi çevrelerce çevrimiçi itaatsizlik yöntemi-bilginin haksız kısıtlanmasına yönelik teknolojik bir direniş-olarak övgü almaktadır (Zeller, 2006: 2).

Devletler zararlı ve sakıncalı kabul ettiği içeriklere erişimi engellemek için teknolojiyi kullanırken, vatandaşlar da engelleme yapılan içeriklere ulaşmak için aynı şekilde teknolojiyi kullanmaktadır. Dolayısıyla, erişim engelleme teknolojileri ne kadar hızlı geliyorsa, engellemeleri aşacak teknolojiler de aynı hızda gelişmekte; web sitelerinin erişimleri değişik teknikler kullanılarak engellenirken, engellemelerin aşılmasında da bunlara mukabil farklı teknikler uygulanmaktadır. Yine, erişim engelleme yöntemleri kombine şekilde kullanıldığı gibi engellemeleri aşma yöntemleri de kombine olarak kullanılabilir (Kaya, 2009: 22; Çağlar, 2011: 30). Böylece, sanal alemdeki bu mücadele devam edip gitmektedir.

Filtreleme ve erişim engellemesini aşmada, temel prensipleri hedefi ve paketin içeriğini gizlemeyi içeren pek çok teknolojik yöntem kullanılmaktadır (Roberts vd., 2009: 13). Bu yöntemlerin en önemlileri, IP değiştirme yöntemi, alan adı sunucusu değiştirme yöntemi, URL gizleme yöntemi, proxy kullanma yöntemi, içerik aldatması yöntemi, kopya içerik kullanımı yöntemi ve önbellek kullanımı yöntemi'dir (Kaya, 2009: 41-46).

2.3.1.2.1 IP Değiştirme Yöntemi

Web sitesinin IP'den engellendiği durumlarda, IP değiştirme yöntemi kullanılarak erişim engelleme etkisiz hale getirilebilmektedir. Bu yöntem, sunucu yöneticisi tarafından web sitesinin barındırıldığı sunucunun IP adresinin değiştirilmesiyle gerçekleştirilmektedir. Bu, sunucunun barındırma şirketini değiştirmeden sadece IP değişikliği ile yapılabilir, sunucu ayarlarının yeni IP adresine göre yapılandırılmasında bazı teknik sorunlar oluşturma riski taşımakla birlikte, oldukça kolay ve maliyeti düşük olmaktadır. Şayet, engellenen site sahipleri sitelerini farklı bir barındırma şirketine taşıyarak IP engellemesini aşabiliyorlarsa, bu durum, yeni barındırma şirketiyle yeni bir hizmet sözleşmesi gerektirdiği için engellenenin aşılması daha zahmetli ve mali açıdan külfetli olacaktır (Kaya, 2009: 41).

Diğer yandan, barındırma şirketlerinin faaliyeti birçok devlet tarafından izin sistemine tabi tutulduğu ve kontrol edildiğinden, barındırma şirketleri herhangi bir

engellemeye uğramamak ve hukuki veya cezai sorumluluk altına girmemek için erişimi engellenmiş veya şüpheli içerikleri barındırmaktan çekinebilmektedir. Bu nedenle, bu yöntemin kullanılabilirliği daha da azalmaktadır (Kaya, 2009: 41-42).

2.3.1.2.2 Alan Adı Sunucusu Değiştirme Yöntemi

DNS engellemeden kurtulmanın yolu basittir. İstemci bilgisayarında, IP adreslerini elle atayarak filtreleme uygulanmayan bir ülkeden veya ülke içerisinde filtreleme uygulanmayan bir DNS sunucu adresi girilerek engelleme aşılabılır. (Roberts vd., 2009: 12). Diğer yandan, herhangi bir alan adının IP adresini bulmak için gönderilen her bir istek, öncelikle o kullanıcının bilgisayarında bulunan “hosts” adlı dosyayı kontrol ederek işe başlar. Yani, “selcuk.edu.tr” adresine girmek istediğinizde, önce talebinize ilişkin yanıtın “hosts” adlı dosyada bulunup bulunmadığı kontrol edilir; eğer erişilmek istenen alan adının IP adresi bu dosyada kayıtlı ise, isteğiniz buradaki bilgi kullanılarak yerine getirilir. IP adres bilgisi burada yoksa, kullanıcı bilgisayarının alan adı sunucusu ayarlarından kayıtlı sunucuya bu istek yönlendirilecek ve ulaşılmak istenen siteye erişim gerçekleştirilecektir. Bu yöntem, ülkemizde Youtube’a mahkeme kararlarıyla erişim engellemesinin uygulandığı dönem içerisinde, engeli aşmak için kullanılan en yaygın yöntem olmuştur (Çağlar, 2011: 34-35).

Ayrıca, İnternet sitesi sahipleri alternatif alan adları kaydederek (Örn: “www.ntv.com.tr”ye tıklanıldığında “www.ntvmsnbc.com” sayfasına ulaşılması) olası bir alan adı engellemesini etkisiz hale getirme yeteneğine sahip olabilmektedir (The Citizen Lab, 2007: 28). İnternet sitelerinin alternatif alan adı kullanmasının arka planında bir takım ticari nedenler olsa da, bunun doğal olarak alan adı engellemesini bertaraf edebilme imkanı sağladığı da görülmektedir (Çağlar, 2011: 35).

İnternete bağlı olan herhangi bir bilgisayarın alan adı sunucusu haline getirilmesinin çok kolay ve ücretsiz olması ve ayrıca kullanımı kolay olan alan adı sunucu yazılımlarının varlığı, alan adı sunucusu üzerinden gerçekleştirilen erişim engelini aşmayı daha da kolaylaştırmaktadır (Çağlar, 2011: 34).

2.3.1.2.3 URL Gizleme Yöntemi

URL gizleme, içerik sağlayıcı tarafından içeriğin URL'sinin değiştirilmesi sonucu engellenen içeriğe erişilmesini sağlayan yöntemdir (Willmaster, 2011). Bu yöntemde URL değişikliği bazen eski içerik aynen korunarak yapılırken, bazen de içerikte bazı değişiklikler yapılarak yeni URL'ler oluşturulmaktadır. URL masking olarak adlandırılan teknikler ile, gerçek URL'nin gizlenmesi ve içeriğe birden fazla URL'den ulaşma imkan dahilindedir (Washington, 2011). Bu yöntemle içeriğe bir URL'den erişilemezken, URL masking tekniğiyle oluşturulmuş kopya URL'den erişmek mümkün olmaktadır. Bir içeriğin URL'si içerik sağlayıcı tarafından kolayca değiştirilebildiği için URL engellemesi kolayca aşılabilmektedir (Kaya, 2010: 42).

2.3.1.2.4 Proxy Kullanma Yöntemi

Bir tür erişim engelleme aracı olarak kullanılan proxy sunucular, aynı şekilde kullanıcılara filtreleme ve engellemeleri bertaraf etme olanağı da vermektedir (Kaya, 2010: 42). İstenen içeriğe proxy sunucunun erişmesi ve eriştiği içeriği İnternet kullanıcısına aktarması özelliği sayesinde proxy sunucu, başka bir ülkede yer aldığı için içeriğe engelsiz bir şekilde erişebilmektedir. Bu nedenle özellikle IP ve alan adı engellemesini etkin bir şekilde aşmada kullanılmaktadır. Ayrıca, içeriğe ilk elden proxy sunucusu eriştiğinden İnternet kullanıcısı kimliğini gizleyebilmekte ve İnternette anonim olarak gezinebilmektedir (The Citizen Lab, 2007: 25).

Proxy sunucular hem engellemeleri aşmak için, hem de çeşitli suçlarda aracı olarak kullanılabildikleri için devletlerce sıkı takibe uğramaktadır (Kaya, 2010: 43). Buna rağmen, proxy sunuculara ait bilgilere ve vekil sunucu IP adreslerine ait listelere İnternette ücretsiz olarak erişilebilmektedir.³⁸ Ancak filtreleme uygulayan çoğu ülke, vekil sunucu benzeri araçlarla mücadelede aynı yöntemi kullanmakta ve bu araçlara erişim sağlayan veya bu araçlarla ilgili bilgi veren sitelere ve bilinen vekil sunucularının IP'lerine ve bu listeleri yayınlayan sitelere erişimi engellemektedir. Buna mukabil bu siteler, bu tür engellemelere karşı ya kullandıkları vekil sunucuların

³⁸ Örneğin, <http://www.samair.ru/proksi/> adresinden vekil sunucu adreslerine ulaşılabilir.

İP adreslerini çok sık deęiřtirerek ya da her bir kullanıcıya vekil sunucuların tüm İP listesinden sadece küçük bir kısmını verip dięerlerini gizli tutarak, tedbirler geliřtirmektedir (Roberts vd., 2009: 18).

İnternet kullanıcıları tarafından vekil sunucuları kullanmak çok zor olmamakla birlikte kullanıcıların bir takım ayar deęiřikliklerini yapması gerekmektedir. Yapılacak bu deęiřikliklerin kullanılan dięer İnternet uygulamalarında tespit edilemeyen bazı sorunlara neden olmasından dolayı da ayar deęiřiklikleri gerektiren vekil sunucuların kolay kullanımı için vekil sunucular havuzu içeren bazı programcıklar, kullanıcılar tarafından tercih edilmektedir. Bu programcıkların en bilineni ve yaygın kullanılanı “tor”dur(Torproject, 2011). Bu ve benzeri programlarla kullanıcılar tek tek vekil sunucu adresi bulmak zorunda kalmamakta; programın ayarlarından hangi ülke sunucularından erişim sağlamak istediğini belirterek farklı ülkelerden hızlı bir şekilde erişim sağlayabilmektedir (Çaęlar, 2011: 33).

Ancak, İnternette kolayca ulařılan ve hiçbir maliyeti yok gibi gözüken vekil sunucuların arka planda farklı amaçlara hizmet etmeleri mümkündür. Bu sunucular, banka, kredi kartı ve e-posta řifresi gibi birçok kiřisel gizli bilginin istenmeyen üçüncü kiřilerin eline geçmesinde kullanılabilir. Bu nedenle, güvenli olmayan, kimin tarafından kurulduęu ve iřletildięi bilinmeyen vekil sunucuların, güvenlik tehditleri de içerdiiine dikkat çekilmektedir (Çaęlar, 2011: 33-34).

2.3.1.2.5 İçerik Aldatması Yöntemi

İçerik engellemesi yoluyla gerçekleştirilen engellemeleri aşmak için çeřitli yöntemler kullanılmaktadır. Bu yöntemlerin en önemlisi olan içerik řifreleme yönteminde, web sitesinin ana temasını oluřturan anahtar kelimeler yerine ilgisiz kelimeler kullanılmakta ve bu řekilde web sitesinin engellenmesinin önüne geçilmektedir (Kaya, 2010: 43). Örneęin, Çin’deki bir insan hakları sitesinde “demokrasi” yerine “lahana”, “çok partili sistem” yerine “havuç” kelimesi kullanılmaktadır. Basit bir teknik olmasına rağmen bu yöntemi, dünyanın en gelişmiş erişim engelleme sistemine sahip Çin devleti bile engelleyememektedir. Fakat bu tekniğin en zayıf

noktası, hedef kitlenin şifreleme uygulamasından haberdar olmaması halinde içeriğin hedef kitleye ulaştırılamaması riski taşımaktadır (Goldsmith ve Wu, 2006: 103).

Aynı şekilde, içeriğin URL adresi veya web sitesinin alan adı için de içerik aldatmacası yöntemi kullanılabilir. Alan adlarında “ilk gelen alır” ilkesi geçerli olduğu için, pornografik içerikli hikayelerin yer aldığı bir web sitesine “www.insanhaklarivehurriyetleri.com” gibi bir alan adının alınmasında hiçbir engel yoktur. Web sitesinde kullanılan resimlerin tanıma bilgisi olan “tag” (Wikipedia, 2012c) kodları için de ilgisiz kelimeler kullanılarak resimlerin de engelleme sistemleri tarafından algılanmasına mani olunabilmektedir (Kaya, 2010: 43).

Bir başka içerik aldatmacası yöntemi ise, web sitesinde yer alan içerikteki kelimelerin arasına rastgele gizli karakterler eklenmesidir. Örneğin, “demokrasi” kelimesi “de-m.okras,i” şeklinde yazılarak harfler arasına eklenen karakterler “1 punto” gibi çok küçük boyutlara küçültülerek gizlenmektedir. Bu şekilde, İnternet kullanıcısı kelimeyi “demokrasi” olarak okurken, erişim engelleme programının kelimeyi demokrasi olarak algılamasının önüne geçilmektedir (Kaya, 2010: 43-44).

2.3.1.2.6 Kopya İçerik Kullanımı Yöntemi

Web teknolojilerinin gelişmesi ve yaygınlaşmasıyla, web sitelerinin etkileşimi artmış ve otomatik olarak içeriklerini güncelleştirebilmeleri nedeniyle bir içerik çok kısa süre içerisinde birçok web sitesinde yayınlanabilir hale gelmiştir. Bu nedenle, bir web sitesinin erişimi engellendiğinde, web sitesi içeriği başka web sitelerine hızla yayılmakta ve dolayısıyla, erişim engelleme kararıyla ulaşılmak istenen sonuç elde edilememektedir. Çünkü, kısa sürede engellenmek istenen içeriğin belki de milyonlarca kopyası, bir çok web sitesinde görüntüleniyor olmaktadır. Bu durum sakıncalı kabul edilen içeriğin erişiminin engellenmesini neredeyse olanaksız hale getirdiği gibi, bu içeriğe ait milyonlarca kopya verinin kaynağının tespitini ve bir suç işlendiği takdirde failini belirlemeyi de imkansız kılmaktadır. Bu nedenle devletler, bu durumda engellenmenin seviyesini artırarak ve farklı teknikleri kombine bir şekilde kullanarak bu içeriklerle mücadele etmeye çalışmaktadır (Kaya, 2010: 44).

2.3.1.2.7 Önbellek Kullanımı Yöntemi

Arama motorları ve bazı İnternet siteleri, İnternet içeriğini çeşitli amaçlarla kendi sunucularında saklamakta ve kullanıcılara bunu bir hizmet olarak sunmaktadır. Örneğin Google arama motoru bu şekilde bir hizmet sunarken (Googleguide, 2011), önbellek konusunda popüler olan “www.archive.org” web sitesi, 85 milyar web sitesini önbelleğinde tutmaktadır (Archive, 2011). Bir web sitesinin erişimi engellendiğinde, arama motoru veya ilgili sitenin önbelleğinde bulunan içerik bu engellemeden etkilenmemektedir (OpenNet, 30.08.2004). Web sitesinin önbelleğe alınması durumunda, erişim engelleme kararına rağmen, ek bir yazılım veya başkaca bir yöntemle gerek olmaksızın sitenin içeriğine ulaşmak mümkün olmaktadır (The Citizen Lab, 2007: 28). Böylece, Google ve “www.archive.org” benzeri arşivleme yapan siteler aracılığıyla erişimi engellenen siteye veya geçmiş tarihlerdeki bir sitenin görüntüsüne erişilebilmektedir.

Aynı şekilde, İnternette ücretsiz olarak sunulan “Google Translate”, “Babelfish” gibi popüler çeviri siteleri de önbellek işlemi yaptıkları için benzer bir imkan sunmaktadırlar. Bu çeviri siteleri bir web sitesini eşzamanlı olarak istenilen dile çevirirken, çeviri içeriğini çeviri sitesinin önbelleğine alarak gerçekleştirmekte ve içerik kullanıcıya buradan sunmaktadır. Böylece çeviri sitelerinin kullanılmasıyla engellenmiş web sitelerin içeriğine erişilebilmektedir (The Citizen Lab, 2007: 28).

Görüldüğü gibi, erişim engellemelerini aşmak için engelleme tekniğine göre farklı düzeylerde beceri ve çabalara gereksinim olmaktadır (Deibert vd., 2008: 34). Bazı engellemeleri aşmak uzun soluklu bir çabayı gerekli kılarken, bazıları kolay bir şekilde çok temel beceriler ile aşılabilmektedir (Kaya, 2010: 46). Nitekim, erişim engelleme için birden çok tekniğin kombine şekilde kullanılması engellemelerin aşılmasını zorlaştırırken, engelleme aşma yöntemlerinin de kombine şekilde kullanılmasını gerekli kılmaktadır. Örneğin, bir İnternet sitesi aynı anda farklı alan adları kullanarak DNS engellemesinden, farklı ülkelerde yer alan birbirinden bağımsız barındırma hizmetleri kullanarak IP engellemesinden, URL gizleme

yöntemiyle URL engellemesinden ve şifrelenmiş içerik kullanarak içerik engellemesinden kurtulabilmektedir (Kaya, 2010: 46).

Keza, erişim engelleme teknolojilerinin gelişmelerine mukabil engellemeyi aşma yöntemleri de hızla gelişmektedir. Her bir engelleme tekniğine paralel geliştirilen tekniklerle engellemeyi bertaraf etmeye yönelik yöntemler bulunmakta ve uygulanmaktadır. Bu nedenle, devletler, engelleme teknolojilerini takip ettikleri kadar, engellemeleri aşma tekniklerindeki gelişmeleri de yakından takip etmek gereği hissetmektedir. Dolayısıyla, devletler filtreleme ve erişim engelleme amacıyla kullandıkları tekniklerin ve kurdukları sistemlerin güçlü ve zayıf yönlerinin farkındadır. Bu nedenle, İnternet içeriğine yönelik engellemenin kolay aşılabilir olmasının tek nedeni olarak devletlerin teknolojik yetersizliğini görmemek gerekmektedir. Bazen de devletler, bilinçli olarak engellemelerin kolay aşılabilir noktada kalması politikasını benimseyebilmektedir (Kaya, 2010: 45-46).

Diğer yandan, her erişim engelleme kararından sonra hem İnternette hem de basında konunun geniş olarak yer aldığını ve engellemenin nasıl aşılabileceğinin ayrıntıları ile tartışılmakta olduğu da unutulmamalıdır (Akdeniz ve Altıparmak, 2008: 60). Dolayısıyla engelleme aşma teknikleri bir süre sonra halka açık bilgiler olmakta ve erişim engelleme kararları çok kısa bir sürede etkinliklerini yitirebilmektedir. Öyle ki, bazen erişim engelleme teknikleri o kadar etkisiz ve yetersiz hale gelmektedir ki, yasaklı web sitesi, erişim engelleme kararına rağmen, ülke genelinde reytingi en yüksek web siteleri arasında yer alabilmektedir (Kaya, 2010: 46). Nitekim, Yotutube'un erişiminin engellendiği dönemde Türkiye'de en çok ziyaret edilen web siteleri arasında bulunduğu bilinmektedir.³⁹

Fakat yine de İnternet bilgisi orta düzeyin altında olan ve en basit engelleme aşma tekniğini kullanamayacak kişilerin olacağı da malumdur (Kaya, 2010: 46). Bu

³⁹ Google tarafından İnternet üzerindeki arama eğilimlerinin yayınlandığı "Google Insights for Search" servisinden, ülkemizde Youtube erişim yasaklarının yoğun olarak uygulandığı 2008 ve 2009 yıllarına bakıldığında en çok aranan terimler sıralamasında Youtube'un 2008 yılında 4., 2009 yılında ise 6. sırada yer aldığı görülmektedir. Bkz. **Google Insights for Search**, <http://www.google.com/trends/explore#geo=TR&date=1%2F2008%2012m&cmpt=q>, <http://www.google.com/trends/explore#geo=TR&date=1%2F2009%2012m&cmpt=q>(1.2.2013)

nedenle, uygulanacak filtreleme ve erişim engelleme yönteminin ortalama İnternet kullanıcısına sınırlama getirmesi durumunda, güçlü ve etkili bir engelleme ve denetim düzeyine ulaşmış olacağı iddia edilmektedir (Bambauer, 2008). Zaten, filtreleme ve erişim engelleme yöntemleri ve bunları aşma teknikleri bir bütün olarak değerlendirildiğinde, devletlerin aldıkları filtreleme ve erişim engelleme kararlarının, erişime tamamen mani olmaktan ziyade erişimin zorlaştırılmasına hizmet ettiği söylenilmektedir (Akdeniz ve Altıparmak, 2008: 78; Dülger, 2007:1480).

Diğer yandan, Harvard Üniversitesi'nce hazırlanan “İnternet Erişim Engelini Aşma Durum Raporu”nda, erişim engelini aşabilmeyi sağlayan araçların güvenlikle ilgili bir takım zafiyetler taşıdıkları dile getirilerek, test edilen engellemeyi aşmaya yarayan tüm araçlarda ciddi güvenlik sorunlarının tespit edildiği belirtilmektedir (Roberts vd., 2009: 85-86).

Son olarak, konunun bir de yerindelik ve meşruiyet boyutuna değinilmesinde fayda vardır. Filtreleme ve erişim engellemesini aşma gayretleri, İnternet kullanıcılarının demokratik mücadelelerini ve politik baskıya karşı bilgi alışverişinde bulunmalarını desteklemek açısından sempatik gelse de, kullanıcıların çocuk pornografisi, ırkçılık, ayrımcılık, şiddet, kumar, uyuşturucuyu ve intiharı teşvik gibi içeriklere ulaşmasını sağlamaya yönelik olunca oldukça rahatsız edici gözükmemektedir (Lemos, 2007). Dolayısıyla, ülkelerin haklı gerekçelerle yasadışı ve zararlı kabul ederek mücadele ettiği ve engellediği içeriklere erişimi sağlayan engellemeyi aşma tekniklerinin kullanılmasını her durumda ve şartta “yerinde” ve “meşru” görerek, “sansüre karşı yürütülen özgürlük mücadelesi” gibi savunmak doğru olmayacaktır.

Nitekim, bilişim şirketlerinin katı sansür uygulayan ülkelere içerik filtreleyen ürün ve hizmetler sunması eleştirildiği gibi, meşru sınırlar içerisinde filtreleme ve erişim engellemesi yapılan ülkelere, o ülkenin kullanıcılarına, kısıtlamaları aşma fırsatını sağlayacak araçların dağıtımını gerçekleştiren şirket, şahıs ve kurumlar da aynı şekilde eleştirilmektedir. Bu işi yapanların, engelleme uygulayan ülke vatandaşlarına engellemeleri aşma fırsatı vermeden önce, söz konusu devletin engelleme rejimini değerlendirmesinin gerekliliğine vurgu yapılmaktadır (Bambauer, 2008).

Sonuç olarak, uygulamalar göstermektedir ki, tezin onuncu alt hipotezinde belirtildiği gibi, İnternetin kendine özgü yapısı ve teknik özelliklerinden dolayı, filtreleme ve erişim engelleme yöntemlerinin hiç birisi ne tek başına ne de kombine olarak yüzde yüz başarılı bir sonuç vermemektedir. Keza, erişim engelleme teknolojileri ne kadar hızlı geliyorsa, engellemeleri aşacak teknolojiler de aynı hızda gelişmekte; web sitelerinin erişimleri değişik teknikler kullanılarak engellenirken, engellemelerin aşılmasında da bunlara mukabil farklı teknikler uygulanmaktadır. Bunun yanında, bu yöntemler, engellenmek istenilmeyen içeriklerin engellenmesi ve sansür tartışmalarından, İnternetin yavaşlaması benzeri birçok teknik sorunlar ortaya çıkartmaktadır.

2.3.2 Filtreleme ve Erişim Engelleme Dışındaki Pozitif Yöntemler

Filtreleme ve erişim engelleme dışında yasadışı ve zararlı içeriğiyle mücadelede; uyar-kaldır, özel anlaşmalar yapma, bilinçlendirme ve İnternet etiğinin geliştirilmesi çalışmaları ile pozitif içerik oluşturma yöntemleri kullanılmaktadır.

2.3.2.1 Uyar-Kaldır

Uyar-kaldır (notice and take down) yöntemiyle engelleme de, yasadışı veya zararlı içeriğin kaldırılmasına yönelik idari bildirimler önce içerik veya erişim sağlayıcıya iletilmekte ve ilgili içeriğin kaldırılması için ihtarda bulunmaktadır. Belirlenen sürede kararın gereği yerine getirilmezse engelleme kararı uygulanmaktadır (Çağlar, 2011: 10). Bu yöntemin etkili bir şekilde uygulanabilmesi için içerik veya erişim sağlayıcıdan en az birinin yurt içinde bulunması gerekmektedir (Kaya, 2010: 24).

Bu yöntem, bazı olumsuz durumlar oluşmadan içeriklerin ilgililer tarafından kaldırılmasına olanak sağladığı için daha uygun ve makul bir yol olarak görülmektedir (Çağlar, 2011: 10). Uyar-kaldır yönteminin bir süreç gerektirmesi avantaj sağlamakta; bu süreç içerisinde, içerik veya erişim sağlayıcılar engelleme kararı uygulanmadan görevlilerle görüşme fırsatı bulabildikleri için, kendilerini savunabilmekte ve olası yanlışların ve erişim engelleme kararının olumsuz etkilerinin önlemesi mümkün olabilmektedir (Kaya, 2010: 27). Ayrıca, bir İnternet sitesinin

sadece bir kısmındaki sakıncalı içerik nedeniyle tamamının engellenmesi sakıncasını giderdiği için daha çok tercih edilen, daha uygulanabilir ve daha adil bir yöntem olarak kabul edilmektedir (Çağlar, 2011: 10; Kaya, 2010: 27).

Bu nedenle bu yöntem, içerik düzenlemesinde özellikle demokratik ülkelerde en yaygın kullanılan ve teşvik edilen yöntem olmuştur. Keza, içerik düzenlemesi yaklaşımının ilk ortaya çıkışı, 1990'lı yıllarda ABD'de telif hakları için bu yöntem bağlamında gündeme gelmiştir (O. Nihat Şen ile kişisel iletişim, 06.08.2013). Nitekim, ABD'de 1996 tarihli Digital Millennium Copyright Act ile uyar-kaldır yöntemi yasal güvenceye kavuşmuştur. Daha sonra Brezilya, Avustralya, Japonya ve Singapur'da bu yöntemi benimsemiştir. Yine, AB'nde e-Ticaret Direktifi ile uyar-kaldır yöntemine zemin oluşturulmuş ve İngiltere başta olmak üzere, Almanya, Avusturya, İsveç, Norveç, Danimarka, Finlandiya ve İtalya gibi AB üyesi ülkelerin birçoğunda bu yöntem uygulanmaktadır.

Uyar-kaldır yönteminin iki şekilde uygulandığı görülmektedir. İlkinde, bu yöntem devlet düzenlemelerine konu edilerek yasalarla uygulanmaktadır. Diğerinde ise, öz düzenleme yaklaşımı ile “gönüllülük” esasına göre daha çok meslek birlikleri ile İSS'ların oluşturduğu taraflar arasında yapılan anlaşmalar yoluyla hayata geçirilmektedir. Uygulamada, daha ziyade ikinci usulün tercih edildiği görülmekle birlikte, çoğu zaman sistemin tamamen öz düzenleme inisiyatiflerine bırakılmadığına şahit olunmaktadır. Nitekim, İngiltere gibi bir çok AB ülkesinde her ne kadar bu sistem “gönüllük” esasına dayalı gibi gözükse de, çoğunlukla hükümetlerin baskısı ile “zorunlu gönüllülük” sistemiyle yürümektedir (Bayzan, 2011: 69).

Uyar-kaldır yönteminin etkin bir şekilde kullanılabilmesi ve işletilebilmesi için sadece bir ülke içinde konuya ilişkin kurallar konulması yeterli olmamaktadır. Zira, illegal içeriklerin yurtdışı kaynaklı olması da mümkündür. Bu hallerde uluslararası işbirliği gerekmekte, uluslararası başvuruların yapılacağı veya ilgili yer ve servis sağlayıcılara aktarılacağı mercilerin varlığı önem kazanmaktadır.

Diğer yandan, yer ve servis sağlayıcılar, genel olarak bu tür uyar-kaldır sistemlerinde illegal içeriğe sahip olan sayfaların ihbar usulüyle belirlenmesini talep etmektedirler. Bu nedenle ve uluslararası işbirliğinin şartlarını oluşturmak açısından INHOPE benzeri uluslararası ihbar merkezleri birliklerinin varlıkları önemlidir. INHOPE, ülkelerdeki İnternet Bilgi ve İhbar Merkezleri tarafından gönüllü olarak üye olunan ve uyar-kaldır mekanizmasının uluslararası arenada işletilmesini geliştirmek üzere kurulmuş bir sivil inisiyatiftir (INHOPE, 2013).

2.3.2.2 Özel Anlaşmalar Yapma

İnternet içerik düzenlemesinde yeni trend özel anlaşmaların yapılmasıdır. Ülkeler, küresel arama motorları ve sosyal ağlarla, belli içeriklerle karşılaşıldığında şikayet etme ya da engelleme imkanları getiren özel anlaşmalar yapmaktadırlar. Bu uygulama tüm Dünyada giderek yaygınlaşmaktadır.

AB, bugüne kadar üç farklı özel anlaşma yaparak bu konuda aktif bir tutum sergilemektedir. Bunlardan ilkinde Avrupa Komisyonu, Avrupa mobil pazarının %96'sını oluşturan 91 mobil servis sağlayıcısı ile 6 Şubat 2007'de "Çocukların ve Gençlerin Güvenli Mobil Kullanımına İlişkin Avrupa Çerçeve Anlaşması" imzalamıştır. Bu kapsamda, söz konusu firmalar gönüllü olarak çocukların uygunsuz içeriklere ulaşmasını engelleyen önlemler almakta ve güvenli mobil kullanımına ilişkin bilinçlendirme kampanyaları düzenlemektedirler (EU, 2005).

AB, özel anlaşma yapma uygulamasının ikincisini Güvenli İnternet Günü (Safer İnternet Day)'nü kutladığı 10 Şubat 2009 tarihinde gerçekleştirmiştir. Avrupa Komisyonu ve çocuk hakları ile ilgili bazı STK'ların koordinasyonu ile dünyanın önde gelen 18 sosyal paylaşım sitesi "AB İçin Güvenli Sosyal Ağlar Prensipleri" metnini imzaladılar. İmzalanan prensip anlaşması ile sosyal ağ siteleri, içeriklerinin çocuklar ve gençler için uygun hale getirilmesini temin etmek için çalışmalar yapacak ve yasadışı içerik veya bu içeriğe yönlendirme raporlarını ilgili yasa uygulayıcı kurumlar ve/veya ihbar merkezleri ile paylaşacak düzenlemeler yapacaklardır. Bu kapsamda, 18 yaşın altındaki çocukların İnternette karşılaştıkları

zararlı içerikleri sosyal paylaşım sitelerinde bulunacak şikayet butonlarıyla ihbar etmesine ve bu tür içeriklerin anında kaldırılmasına da imkan sağlanacaktır.⁴⁰

AB'nin üçüncü özel anlaşma uygulaması ise, çocukların İnternette daha güvenli olabilmeleri için aralarında Microsoft, Samsung, Apple, Facebook ve Vodafone gibi isimlerinde bulunduğu sektör lideri 28 şirket ile gerçekleştirilmiştir. Buna göre, Avrupa Komisyonu ile söz konusu şirketler, hazırlanan bir eylem planı üzerinde 1 Aralık 2011 tarihinde mutabık kalmışlardır (EU, 2011a). Bahsi geçen eylem planı basit ve güçlü ihbar araçları, yaşa uygun gizlilik ayarları, daha geniş kullanımlı içerik kategorizasyonu, ebeveyn kontrolünde daha geniş ve kullanışlı yazılımların geliştirilmesi, çocuk istismarı içeriklerinin daha etkili bir şekilde kaldırılması gibi hususları kapsamaktadır (EU, 2011a).

Brezilya'da, 2 Temmuz 2008'de, bir STK olan SaferNet Brezilya, Federal Kamu Bakanlığı-Federal Devlet Başsavcılığı Ofisi (Ministério Público Federal/Procurador-Geral da República) ile Google firması arasında, "on-line çocuk güvenliği" üzerine bir anlaşma imzalanmıştır. Bu anlaşma ile Google Brezilya, Orkut servisi kullanılarak yapılmış olan mesajlaşma, video paylaşımı, imaj, foto işlemlerindeki trafik bilgilerini 180 gün süre ile saklamak, adli makamlardan veya soruşturmaya yetkili mercilerden gelecek talepler doğrultusunda bunları göndermek ve takibat konusu olan materyalleri daha uzun süre saklamak, Savcılar Ofisi ile aralarına on-line bağlantılar kurmak, ihbar edilen materyali 72 saat içerisinde yayından kaldırmak, web sayfasında yasal uyarılar ve ihbar hatları oluşturmak, çocuk pornosu ve istismarına ilişkin mücadelede yeni metodlar ve araçlar ortaya çıktığında bunları kullanmak, çocuk pornosu ve istismarıyla mücadele eden uluslararası kuruluşlarla iş birliği içerisinde olmak gibi yükümlülükler altına girmiştir (SaferNet Brasil, 2013a).

⁴⁰ Prensip kararını imzalayan kurum ve şirketler: Arto, Bebo, Dailymotion, Facebook, Giovani.it, Google, Hyves.nl, Microsoft Europe, MySpace, nasza-klasa.pl, Netlog, One.lt, Piczo, Skyrock.com, StudiVZ.de, Sulake/Habbo.com, Yahoo! Europe, Zap.lu'dur. (Office For Internetsafety, 10.02.2009). Sözleşme metni için bkz. **Safer Social Networking Principles For The EU**, https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/sn_principles.pdf (30.11.2012)

Almanya'nın ihbar merkezi olan "Jugendschutz.net" ile Youtube, 2007 yılında, yasadışı aşırı sağ videoların kaldırılması veya Almanya'dan erişiminin engellenmesini öngören bir anlaşma yapmıştır. Bu anlaşma sonrası Youtube, Jugendschutz.net'in düzenli olarak bildirmiş olduğu Nazi videolarını yayından kaldırmış veya Almanya'dan erişimini engellemiştir (Jugendschutz, 2007). Yine, Almanya'da Aile İşleri Bakanlığı aracılığı ile Federal Kriminal Polis Ofisi, ülkedeki İnternet erişiminin %75'ini sağlayan 5 büyük İSS ile 17.04.2009'da çocuk pornosunun DNS aracılığıyla filtrelenmesine dair sözleşme imzalamıştır (İHA, 2009).

4 Eylül 2008 tarihinde, Avrupa'nın en büyük, dünyanın 5. büyük IP trafik taşıyıcısı Teliasonera International firması, çocuk pornografisi ile mücadele amacıyla, İngiltere merkezli ihbar merkezi İnternet Watch Foundation ile kara liste konusunda işbirliğine gidip, müşterilerine (ISP'ler, mobil operatörler v.b.) kendi networkleri üzerinden bu sitelere erişimi engelleyecek ücretsiz bir çözüm sunmaya başlamıştır (Softpedia, 2008).

Benzer şekilde, New York Eyaleti Adalet Bakanlığı, 10 Haziran 2008 tarihinde, ABD'nin üç büyük İSS'sı olan Time Warner Cable, Sprint ve Verizon şirketleri ile çocuk pornosu içeren site ve özel web paylaşım gruplarına erişimin engellenmesini öngören bir eylem planı üzerinde anlaşma sağlamıştır. Buna göre, söz konusu servis sağlayıcıları, gelen şikayetler doğrultusunda tespit ettikleri illegal sitelere erişimi durdurdukları gibi, şekil değiştirmek suretiyle kendilerine alternatif güzergah arayacak olanlara da tolerans göstermeyecektir (Çehreli, 11.06.2008).

Keza Çin, devlet politikası olarak illegal kabul ettiği içeriğin engellenmesiyle ilgili olarak, sektördeki büyük firmalarla özel anlaşmalarla işbirliği yapma konusunda en ileri örnekleri vermektedir. Çin devleti, "Büyük Çin İnternet Duvarı" olarak adlandırılan (Goldsmith ve Wu, 2006: 92) ve ülkenin bütününde her bir İnternet noktasını kontrol altında tutan İnternet takip ve erişim engelleme sistemini CISCO, Yahoo, Google, Microsoft gibi Amerikan şirketlerinin çeşitli düzeylerdeki işbirliğiyle geliştirmiştir (Kaya, 2010: 62). Örneğin, ağda taşınan veriyi kaydetmek için ve zararlı sitelere girmeyi engellemek üzere, dünyanın en büyük router üreticisi

olan CISCO firmasıyla anlaşarak tüm Çin'i kapsayacak bir İnternet duvarının oluşumunun teknik şartlarını sağlamıştır (Goldsmith ve Wu, 2006: 93-94).

Yine, Çin; Yahoo, Google, Microsoft gibi büyük şirketlere, sistemlerini ülkenin İnternet politikalarıyla uyumlu hale getirmeleri şartıyla faaliyette bulunabilme izni vermektedir (Ifex, 2012). Buna göre, bu şirketler, bir suç şüphesi olması durumunda devlet yetkilileri ile işbirliğine giderek, talep edilen bilgileri verdikleri gibi, hizmet sundukları arama motoru, blog gibi servislerde belirli kelimelerin kullanılmasının yasaklanmasını da sağlamaktadır (Goldsmith ve Wu, 2006: 95). İletişimin ve özel verilerin gizliliği gibi temel özgürlükleri kısıtlamak için Çin hükümeti ile işbirliği yapmaları, bu dev şirketlere yönelik tepkilere neden olsa da, bu şirketler faaliyet gösterdikleri ülkedeki kanunlara uymak zorunda olduklarını gerekçe göstererek işbirliğine devam etmektedir (Kaya, 2010: 63).

2.3.2.3 Bilinçlendirme Faaliyetleri

İnternetin güvenli kullanımı konusunda zamana yayılmış en kalıcı önlem olarak ön plana çıkan bilinçlendirme faaliyetleri, zor ve uzun bir süreç gerektiren ancak en az eleştiri alan yöntem olarak Dünyada yaygın olarak kullanılmaktadır. Bilinçlendirme faaliyetleri dünyada kamu kurumları, STK'ları ve uluslararası örgütler ve özel sektör kuruluşları tarafından dört farklı platformda, temel hedef kitlesi çocuklar ve gençler olmak üzere, eğitimciler ve ailelere yönelik olarak yürütülmektedir.

Bilinçlendirme ve eğitim çalışmalarının genellikle ebevyn gözetimi, bilinçlendirme kampanyaları ve okullarda eğitim olmak üzere üç parçalı bir yapı içinde ele alındığı görülmektedir. Ebevyn gözetimi; ebeveynlerin çocukların İnternet kullanımını takip etmesi, zararlı içerik ve eylemlerden uzak kaldığından emin olması, İnternetin güvenli kullanımı ve riskleri konusunda bilinçlendirilmesi çalışmalarını kapsamaktadır. Bilinçlendirme kampanyaları ise; öğrenci, öğretmen, çalışanlar ve diğer gruplarda İnternetin riskleri konusunda farkındalık oluşturma ve güvenli İnternet kullanımına ilişkin beceri ve birikim artırıcı çalışmaların yapıldığı seminerler, eğitimler, atölyeler gibi aktivitelerle, toplumun tümüne yönelik yapılan

güvenli İnternet konulu kamu spotu, reklam, İnternet sitesi gibi çalışmalardan oluşmaktadır. Okullarda eğitim ise; öğrencilerin İnternetin riskleri konusunda bilinçlenmesi ve İnternetin güvenli kullanımı konusunda beceri ve birikimlerini artırıcı derslerin müfredata alınması ve öğrencilerin zararlı içerik ve eylemlerden uzak kalmasına yönelik filtreleme uygulamalarını kapsamaktadır (DPT, 2013a).

Bilinçlendirme faaliyetleri dünyada, kamu kurumları, STK'lar, uluslararası örgütler ve büyük İnternet firmalarının çalışma ve kampanyaları olarak tezahür etmektedir. Fakat şunu belirtmek gerekir ki, söz konusu faaliyetler ülkelerin kamu kurumlarınca bizzat yürütülmesi de yönetimlerden ciddi ölçüde yönlendirme desteği almaktadır. Nitekim AB, 1999'dan beri Güvenli İnternet Programı (Safer Internet Programme) çerçevesinde, başta aileler ve çocuklar olmak üzere kullanıcıların, İnterneti doğru, etkin ve güvenli kullanmalarına yönelik faaliyetleri desteklemektedir. Bu bağlamda, aileleri ve öğretmenleri İnternet üzerinden zararlı ve yasadışı içeriklerle ilgili bilgilendirmek ve uyarmak amacıyla bilinçlendirme aktivitelerini cesaretlendirmek, imkan sağlamak ve geniş çaplı bilinçlendirme aktivitelerini desteklemek kararı almıştır ve bu yönde uygulamalar gerçekleştirmektedir (EU, 2011c, 2011d, 2011e).

Avrupa Güvenli İnternet Ağı (INSAFE-European Safer Internet Network), Güvenli İnternet Programı'nın desteklediği ve finanse ettiği, gençler için İnternet ve mobil cihazların güvenli ve bilinçli kullanımını teşvik eden bir Avrupa farkındalık merkezi ağıdır. AB üyesi ülkeler ile Norveç, İzlanda, Arjantin, Avustralya, ABD ve Rusya'nın oluşturduğu 33 ülkenin farkındalık merkezidir (INSAFE, 2011).

Keza, INSAFE tarafından 2004 yılından itibaren her yıl Şubat ayında gerçekleştirilen ve üye ülkeler ile Avrupa Komisyonunca düzenlenen Güvenli İnternet Günleri, tüm İnternet kullanıcılarını hedef alan, farkındalık artırıcı uluslararası etkinliklerdir (INSAFE, 2011). Dünyanın birçok ülkesinde de devlet ve STK işbirliğine dayanan ve İnternetin güvenli kullanımına yönelik bilinçlendirme faaliyetleri, kampanyalarla veya geliştirilen projelerle hayata geçirilmeye çalışılmaktadır.

Diğer yandan, bilinçlendirme faaliyetlerinin önündeki en büyük engel bu faaliyetlerin büyük ölçüde İnternet üzerinden yapılıyor olmasıdır. Bu nedenle, bilinçlendirme faaliyetleri kapsamında hazırlanan içerikler ancak bilinçlenmeyi tercih eden kullanıcılara ulaşabilmektedir. Bu kısır döngünün kırılabilmesi için bilinçlendirme faaliyetlerinin hem içerik zenginliğinin arttırılarak cazip hale getirilmesi, hem de bu içeriklerin tüm kullanıcılara etkin ulaşımını sağlayacak yöntemlerin geliştirilmesi gerekmektedir.

Bilinçlendirme konusunda, yakın zamanda ortaya atılan ‘dijital yerli’ ve ‘dijital göçmen’ kavramlarına dikkat çekilmektedir. Buna göre, ‘dijital yerliler’ 1980’ler ve sonrası doğan, teknolojinin odağında büyüyen bir nesil olarak tanımlanırken, ‘dijital göçmenler’ dijital dünya ile sonradan tanışan bir nesli tarif etmektedir. Bu çerçevede, her biri farklı özelliklere sahip olan ‘X Nesli (1965-1979 arası doğanlar)’, ‘Y Nesli (1977-1994 arası doğanlar)’ ve ‘Z Nesli (21. Yüzyılda doğanlar)’nden bahsedilmektedir. Hatta bundan 10 yıl önce dijital yerli olarak adlandırılan ‘Y Nesli’ içinde bile dijital göçmenlerin oluşabileceği ve dijital yerlilik kavramının ‘Z Kuşağı’ ile daha da boyut değiştirmeye başladığı belirtilmektedir. Çünkü, Z kuşağı adeta İnternet teknolojisi ile büyüyen, aynı anda birden fazla iş yapabilen, deneme-yanılma yolunu tercih eden, duyu yetenekleri daha da gelişmiş olan, yazılı metinler yerine görselliğe daha fazla önem veren bir nesildir ve bu özellikleri ile kendisinden önce gelen X ve Y Neslinden farklılaşmaktadır. Bu çerçevede dijital vatandaşlık yaklaşımının, hem dijital yerlilerin hem de dijital göçmenlerin ihtiyaçlarını ve kuşak farklılıklarını gözetecek şekilde ele alması ve dijital vatandaşlık bilincinin bu bağlamda geliştirilmesi gerekmektedir (Çubukcu ve Bayzan, 2013: 151).

Bilinçlendirme çalışmaları kapsamında gündeme getirilen diğer iki kavram ise “medya okur-yazarlığı” ve “bilişim okur-yazarlığı”dır. Medya okur-yazarlığı, “yazılı ve yazılı olmayan, büyük çeşitlilik gösteren formatlardaki (televizyon, video, sinema, reklamlar, İnternet gibi) mesajlara ulaşma, bunları çözümleme, değerlendirme ve iletme yeteneği kazanabilmek” olarak tanımlanmaktadır (RTÜK, 2013). Bilişim okur-yazarlığı ise, bilgisayardaki programları kullanabilme, bilgisayar veya İnternet ortamında ihtiyaç duyulan bilgilere ulaşabilme ve bu ortamlarla ilgili sorunlarını

kendi başına etkili bir şekilde çözebilme becerisine sahip olabilmeyi ifade etmektedir (Geçer ve Dağ, 2010: 21).

Avrupa ülkelerinde bilişim ve İnternet teknolojileri becerilerini geliştirmek ve bilinçli İnternet kullanıcısı bireyler yetiştirmek için 1970’li yıllardan itibaren ders müfredatlarına bu ihtiyacı karşılamaya yönelik olarak medya okur-yazarlığı veya bilişim okur-yazarlığı gibi yeni dersler ve konular eklenmiştir (TBMM, 2012: 536).

2.3.2.4 İnternet Etiği Çalışmaları

İnternetin neden olduğu sorunlara çözüm bulma, yasadışı ve zararlı içerik ile mücadele kapsamında gündeme getirilen konulardan birisi de İnternet etiğidir. İş dünyasında, aile hayatında, bireysel yaşamda özel bir ahlaki sorumluluğun gereği olarak ifade edilen etik anlayış, İnternet alanında da insanlık değerleri için bir takım tehlikelerle mücadele etmek, korumacılık ve düzenleme anlamında duyulan ihtiyaca cevap verebilecek bir imkan olarak görülmektedir (Arıkan, 2011: 1).

Bu yaklaşımda, toplum içinde kabul gören ahlaki-gayri ahlaki ayrımlarıyla temelinde bulunan dürüstlük, doğruluk, doğaya saygı, hak, adalet, yapılan haksızlıklara karşı tepki gösterme gibi evrensel değerleri temsil eden etik anlayışın, İnternet alanına uyarlanması ile İnternet kaynaklı tehditlerin ve risklerin azalacağı umulmaktadır (Arıkan, 2011: 2).

İnternet toplumunda, İnternet içeriğinden ve yanlış kullanımından ortaya çıkan sorunların birçoğu aslında aynı zamanda etik sorunlarıdır. Bu çerçevede, başta telif hakları olmak üzere, sakıncalı içeriklerin İnternette barınması ve paylaşılması, güvenlik ve mahremiyet sorunları birer etik sorunu olarak görülebilir. Nitekim, konuya bu yönü ile yaklaşarak ihtiyaçları karşılamak için İnternette “netiquette” olarak adlandırılan ve bizzat İnternet kullanıcılarının gönüllülük temelinde kendi kendini düzenleme ve denetlemelerini amaçlayan çalışmalar yapılmaktadır.

Gönüllü olarak, İnternet kullanımını kontrol eden ve yöneten ortak kurallar belirleyip, geliştirme ve yaygınlaştırma çalışmaları olarak tanımlanabilecek

“netiquette” sistemi (Sınar, 2001: 31), aynı zamanda İnternet etiği anlayışını ve etik kurallarını oluşturma ve olgunlaştırma faaliyeti olarak görülebilir. Her türlü içerik için telif haklarına saygı gösterme, spam olarak da adlandırılan istenmeyen e-postalar göndermeme kuralları bunların en yaygın olanlarından (Kaya, 2009: 9).

Dünya’da sadece İnternet etiği değil, genel olarak (kamu-özel) hayatın her alanında etik anlayışının ve etik kurallarının gelişmesi için devletlerin de çalışmaları vardır. Devletler, ülkelerinde bu türden çalışmaları desteklemek, teşvik etmek ve standartlar oluşturmak için etik kurulları oluşturmuşlardır. İngiltere’de The Comity Of Standards In Public Life, ABD’de United States Office of Government Ethics, Kanada’da The Office Of Ethics Council, Japonya’da National Public Service Ethics Board, Avustralya’da The Public Service And Merit Protection Commission ve İrlanda’da The Public Office’s Commission bunlardan bazılarıdır.

Bunların dışında devletler, İnternet etiği oluşturulması çalışmaları bağlamında münhasıran bu konuyla ilgili bazı birimler de meydana getirmişlerdir. Örneğin Güney Kore’nin İnternetle ilgili düzenleyici kurumu KCSC (Korea Communications Standards Commission) bünyesinde bir alt komisyon olarak bulunan ve içeriklerle ilgili genel etik ilkeleri ve kodları geliştirmek için çalışan Bilgi İletişim Etiği Komitesi bunlardan birisidir (KCSC, 2013). İnternet etiği konusuna önem veren Brezilya’da ise, Nética platformu (İnternet+Ethic=Nética), “SaferNet Brasil” ve diğer ortaklar tarafından oluşturulmuş ve “new.netica.org.br” web adresinden yayın yapmaktadır. İnternet etiği çalışmaları bu Platform üzerinden Brezilya’daki İnternet yönetişimi sistemi içinde yer alan tüm paydaşların desteği ve katılımı ile yürütülmektedir (Netica, 2013).

Diğer yandan, İnternet etiği anlayışının yaygınlaşması ve etik kurallarının uygulama alanının genişletilmesi konularında faaliyet gösteren, bilişim alanında çalışan bazı meslek örgütleri ve STK’lar da bulunmaktadır. Dünya çapında faaliyet gösteren uluslararası meslek kuruluşlarından, ACM (Association for Computing Machinery), AITP (The Association of Information Technology Professionals), IEEE (The Institue of Electrical and Electronics Engineer) ve İngiltere’deki BCS (British

Computer Society) bunlardan bazılarıdır. Lisanslama ve telif hakları konusunda faaliyet gösteren Creative Commons adlı STK'da bu konuda çalışma yapmaktadır. Bu STK, fikir ve sanat eserlerinin İnternette paylaşımı konusunda çeşitli netiquette kuralları oluşturmaktadır (Creativecommons, 2011).

Bilişim şirketleri bazen de herhangi bir örgütsel çatı altında bir araya gelmeden kendi aralarında İnternet etiği bağlamında değerlendirilebilecek bazı ilkesel kurallar konusunda anlaşarak uygulama kararı alabilirler. İnternet liderleri olan Google, Yahoo ve Microsoft'un İnterneti aşırı kısıtlayan hükümetlere karşı ifade özgürlüğünü ve kişisel mahremiyetin korunmasını esas alan davranış kuralları konusunda görüş birliğine varmaları bu türe bir örnektir (Akcan, 2008).

Bazen de büyük bilişim şirketleri kurum politikaları gereğince müşterilerine ve çalışanlarına yönelik olarak etik kuralları/ilkeleri belirleyebilmektedir. Microsoft ve Faceebook bunlardan ikisidir. Microsoft, MSN ve Windows Live hizmetleri kullanım kurallarını belirlemiş ve deklare etmiştir (Explore Live, 2011). Keza, Facebook'da "Hak ve Sorumluluklar Bildirimi"ni yayınlamıştır (Facebook, 2011).

İnternet etiği çalışmalarının öz düzenleme ve bilinçlendirme çalışmalarıyla yakın bir ilgisi bulunmaktadır. Bu kapsamda, öz düzenleme ve bilinçlendirme konularının etik kurallarla paralel bir seyir izlediğini söylemek mümkündür. Nitekim İnternetin güvenli kullanımı ile ilgili yapılan çalışmalar, evrensel etik değerlerinin benimsetilme çabası olarak da görülmektedir (Arıkan, 2011: 3). Dolayısıyla, öz düzenleme, bilinçlendirme ve İnternet etiği çalışmalarını birbirinin tamamlayıcısı ve destekleyici unsurları olarak ele almak ve uygulamak daha isabetli olacaktır.

2.3.2.5 Pozitif İçerik Oluşturma

Yakın zamana kadar içerik düzenlemelerinin genellikle erişim engelleme ve filtreleme merkezli olarak gerçekleştirildiği bilinmektedir. Bu uygulamaların ortaya çıkışında İnternetin zararlarından korunmak, yasadışı ve zararlı içeriğin önlenmesi gibi İnternet hakkında olumsuz bir algıyı besleyen negatif bir motivasyon olduğu görülmektedir. Son dönemde biraz da bu yanlış ve sevimsiz algıyı değiştirmek ve

İnternetin sempatik yönünü ortaya çıkarmak için yeni bir içerik düzenleme yöntemi olarak pozitif içerik oluşturulması ve çoğaltılması konusu gündeme gelmiştir.

Bu çerçevede, AB'nin, çocukların İnternet kullanımını daha etkin ve güvenli hale getirecek stratejileri ortaya koyduğu “Çocuklara Daha İyi İnternet için Avrupa Stratejisi” belgesinde, geliştirilen dört temel stratejiden birisini de “Genç ve çocuklara yönelik kaliteli içeriğin teşvik edilmesi” konusu oluşturmuştur. Bu kapsamda çocukların pozitif içerik üretiminin teşvik edilmesi ve çocuklar için eğitici içeriğin artırılmasına yönelik adımların atılması kararı alınmıştır (DPT, 2013b).

Keza, OECD'nin 2011 tarihli Çocukların Çevrimiçi Korunması Raporu'nda; İnternetin risklerini azaltma konusunda, pozitif içerikler ve çocuklara özgü güvenli alanlar oluşturma yaklaşımı ayrı bir önlem olarak zikredilmiştir. Rapor'a göre, bir kamu politikası aracı olarak pozitif içerik, onların İnternet ortamında karşılaştığı risklerin azaltılması stratejisinin tamamlayıcısı olabilir. Bu kapsamda, çocuklara yönelik web siteleri ve arama motorları ile çocukların yaşlarına uygun içeriklere erişebilecekleri kapalı ortamlar (walled gardens) oluşturulmaktadır. Bu süreçte, kamu kurumları, STK'ları ve özel şirketler yer almaktadır (OECD, 02.05.2011: 73).

Nitekim, Avrupa Konseyi bu yaklaşımı kabul etmiş ve “Wild Web Woods” isimli eğlence portalını (www.wildwebwoods.org) farklı dil seçenekleri ile çocukların hizmetine sunmuştur. AB ve birçok ülke de, çocuklar için pozitif içeriğin oluşturulmasına fon sağlamak ve yerel kültür ve dilleri destekleyen yerel içerikleri teşvik etmektedir. Örneğin Almanya, çocuklar için üretilecek yüksek kaliteli ve yenilikçi İnternet içeriklerini desteklemek için yıllık 1,5 milyon Avro büyüklüğünde bir fon tahsis etmiştir (OECD, 02.05.2011: 74).

Literatürde çok fazla yer almamakla birlikte mülakat yaptığımız uzmanların hepsi özellikle pozitif içerik oluşturma ve içerik düzenlemesinin en önemli unsuru olması gerektiği yönünde ortak görüş beyan etmişlerdir. Nitekim Şen, İnternetin yarar-zarar düzlemine indirgenerek olumsuz bir algının oluşmasına neden olan negatif içeriğine karşılık, pozitif içeriği çoğaltma yaklaşımının önemine dikkat çekmektedir. Keza,

İnterneti yarar-zarar indirgemeciliğinden kurtarmak için bilerek yararlı içerik yerine pozitif içerik teriminin tercih edildiğini dile getirmektedir (O. Nihat Şen ile kişisel iletişim, 06.08.2013).

Şen, pozitif içeriği artırma ve zenginleştirme uygulamalarının aynı zamanda bir içerik düzenleme yöntemi olarak yaygınlaştırılması ve teşvik edilmesi gerektiğini belirtmektedir. Bu bağlamda, çocuklara özel bazı içerikler üretilebileceği gibi, gençler ve ailelerin de rahatlıkla kullanabileceği, içerisinde rahatsız edici unsurların bulunmadığı web siteleri, web uygulamaları ve çocuklara yönelik arama motoru kullanıcıların hizmetine sunulabilir (O. Nihat Şen ile kişisel iletişim, 06.08.2013).

Keza Aydın da, pozitif içerik oluşturma'nın önemine vurgu yapmaktadır. Aydın'a göre, yasadışılığın kol gezdiği karanlık sokaklarda yapılacak en iyi mücadele ışıktır. Yani faydalı içeriği artırmak ve zenginleştirmektir. İşin önlem almayı değil de geliştirmeyi gerektiren zor kısmı da burasıdır; yıkmak değil yapma kısmı. Biz arka sokaklarda lamba yakarsak şehirde gezilecek kısım artacaktır. İşin bu kısmına yoğunlaşmak gerekmektedir (E. Sadık Aydın ile kişisel iletişim, 25.07.2013).

İçerik düzenlemelerinde kullanılan yöntemlerle ilgili bu bölümde sonuç olarak tezin onuncu alt hipotezinde savunulan görüşün doğruluğunun teyit edildiği görülmektedir. Zira, uygulamalar ve konu hakkındaki uzmanların görüşü, söz konusu hipotezde belirtildiği gibi, İnternetin kendine özgü yapısından dolayı, filtreleme ve erişim engelleme yöntemlerinin yasadışı ve zararlı içeriğe yüzde yüz erişimi engelleme sonucunu doğurmadığını ortaya koymaktadır. Çünkü, erişim engelleme teknolojileri ne kadar hızlı geliyorsa, engellemeleri aşacak teknolojiler de aynı hızda gelişmekte; web sitelerinin erişimleri değişik teknikler kullanılarak engellenirken, engellemelerin aşılmasında da bunlara mukabil farklı teknikler uygulanmaktadır. Buna mukabil, bu yöntemlerin, masum içeriklerin engellenmesi ve sansür tartışmalarından, İnternetin yavaşlamasına kadar birçok sorunlara da neden olduğu görülmektedir.

Bunun yanında, içerik düzenlemelerinde uyar-kaldır, öz düzenleme uygulamaları, özel sektör ile özel anlaşma ve işbirliği geliştirme, bilinçlendirme ve İnternet etiği

faaliyetleri, pozitif içerik oluşturma gibi yöntemlerin hem daha sempatik ve demokratik hem de sonuç almada daha etkili olduğu müşahade edilmektedir. Dolayısıyla, söz konusu hipotezde vurgulandığı gibi, içerik düzenlemelerinde, pozitif düzenleme yöntemlerinin tercih edilmesi, filtreleme ve erişim engelleme en son tercih edilen yöntem olması gerektiği sonucuna ulaşılmaktadır.

2.4 İÇERİK DÜZENLEMESİNİN ÖLÇÜTLERİ

Ülkelerin farklı gerekçelerle, farklı konularda, farklı yönetsel yaklaşımlarla ve farklı yöntem ve tekniklerle İnternet içerik düzenlemelerine gittikleri görülmektedir. Özellikle filtreleme ve erişim engelleme uygulamalarında, söz konusu kısıtlamaların meşruiyetini değerlendirme noktasında yoğun tartışmalar yaşanmaktadır. Son dönemde, işte bu çevrimiçi kısıtlamaların meşruiyetini normatif olarak değerlendirmede faydalanılacak elverişli, tutarlı ve isabetli bazı ölçütlerin belirlenmesinin gerekliliği gündeme getirilmiştir (Bambauer, 2008).

Bambauer’ın açıklık, şeffaflık, kısıtlılık ve sorumluluk olarak belirlediği bu ölçütlerin, devletlerin filtreleme ve erişim engelleme uygulamalarının normatif olarak değerlendirilmesi için alternatif ve süreç odaklı bir çerçeve sunmaya yarayacağı, bunun yanı sıra bu sürece ilişkin kurumsal işlemlerin analizine olanak vereceği ve böylece, devletlerin İnternet kısıtlamalarının meşruiyetini ölçmeye yönelik analitik bir yöntemin ortaya çıkacağı düşünülmektedir (Bambauer, 2008).

2.4.1 Açıklık

Devletlerin filtreleme ve erişim engelleme uygulamalarının analizinde kullanılacak ilk ölçüt “açıklık”tır. “Açıklık” ölçütü, bir devletin İnternete kısıtlama uyguladığını kabul edip etmediğini ve bunun nedenini irdelemektedir. Engellemeyi yapan güç, filtrelemeyi kabul ediyor ve bu engelleme gereğini açıkça belirtiyor mu? Filtreleme ve erişim engellemesinin yetkililerce açıklanması ve kısıtlamaların gerekçelerinin dikkatle ve açık bir biçimde belirtilmesi, yapılan uygulamaların meşru olma ihtimalini yükseltmektedir. Gizli veya yetersiz gerekçelere dayalı engellemelerin kabul edilebilirliği normatif açıdan daha azdır (Bambauer, 2008).

Diğer yandan, açıklanmamış kısıtlamaların hiçbir gerekçeyi güçlendirmedeği, aksine, devletin erişimi engellediğinin ilan edilmesinin ve gerekçelerinin açıklanmasının, söz konusu içeriğin zararlılığına ilişkin kanaati ve bu içeriğin yasaklanmayı hak ettiğine dair toplum görüşünü artırdığı söylenebilir (Bambauer, 2008). Ayrıca, yapılan kısıtlamaların ve gerekçelerinin deklare edilmesinin, yönetimin ve yöneticilerin karar ve uygulamalarının denetlenmesi ve korunması açısından elverişli bir zeminin oluşmasına neden olacağı açıktır.

“Açıklık” ölçütü açısından Suudi Arabistan ile Çin uygulamaları karşılaştırılabilir. Suudi Arabistan’da İnternetin yönetiminden sorumlu İletişim ve Bilgi Teknolojileri Komisyonu bağlantı verdiği web sitesinde yasaklama konularını ve uyguladığı filtreleme sistemini açıklamaktadır (Internet.sa, 2013a). Komisyon pornografinin sosyal zararlarını anlatan destekleyici materyaller sunmakta, dini, hukuki ve bilimsel kaynakları ve çalışmaları referans göstererek uygulamalarını gerekçelendirmektedir (Internet.sa, 2013b). Keza, 2001 yılında, Suudi Arabistan Bakanlar Konseyi “kamu ahlakını ihlal eden”, “İslam’ın kutsallığına hakaret eden” ve “devlete veya devlet sistemine karşı gelen” içerikler barındırdığı için yasaklanan İnternet sitelerini açıklayan bir kararı ilan etmiştir (Al-bab, 2001). Ayrıca, engellenmiş bir siteye erişmek isteyen kullanıcıların karşlarına, bu siteye erişimin engellendiğini bildiren bir “engellenmiş sayfa” uyarısı çıkmaktadır (Internet.sa, 2013c). Bu örneklerde de görüldüğü gibi, Suudi Arabistan devleti, İnternet filtreleme ve erişim engelleme karar ve uygulamalarının varlığını ifşa etmekte ve bu kısıtlamalara ilişkin gerekçelerini açıklamakta ve savunmaktadır.

Çin devleti ise, Suudi Arabistan’ın aksine, dünyanın en kapsamlı ve kompleks İnternet sansür sistemini işletmekle birlikte, bu gerçeği nadiren kabul etmektedir. Keza, Çin’de kullanıcılara erişmek istediklerinde yasaklanmış sitelerle ilgili herhangi bir bildirimde bulunulmamakta, bunun yerine geçici teknik hata sayfaları görüntülenmektedir. Google veya Baidu gibi arama motorlarında, yasaklı kelimeler için yapılan aramalarda genellikle, içerisinde engellenen siteleri bulundurmayan sonuçlar sunulmaktadır. Hatta, hangi içeriğin neden engellendiğini belirleme girişimleri dahi engellemeye uğrayabilmektedir (OpenNet, 09.08.2012a).

Çin’de açıklık prensibinin olmayışı olumsuz sonuçlar doğurmaktadır. Resmi makamların ülkede filtrelemeye izin vermediklerine ilişkin beyanlarının hilafına, kullanıcılar, devlet tarafından sterilize edilmiş ve çarpıtılan bir bilgi ortamında bulunduklarını genellikle bilmemektedir (Bambauer, 2008). Açıklık ölçütü ile değerlendirildiğinde Çin uygulaması, en kötü ve meşruiyet konusunda en sorunlu örneklerden birisini oluşturmaktadır. Bu nedenle, Çin, İnternete yönelik uyguladığı sansür nedeniyle dünyada en çok eleştirilen ülkelerin başında gelmektedir.

Benzer şekilde açıklık ölçütü açısından ABD’nin özellikle ulusal güvenlik ve terörizm ile mücadele kapsamında İnternetin izleme ve denetimine ilişkin uygulamaları oldukça sorunludur. Ülkede terörle mücadele gerekçesiyle istihbarat kurumlarının kimlerin, ne kadar ve hangi süre ile İnternet trafiğini izlediği veya kaydını tuttuğu, bu bilgileri ne yaptığı, büyük İnternet firmaları ile veri paylaşımı konusunda ne oranda işbirliği içerisinde olduğu tam olarak bilinmemektedir. Nitekim, devlet yetkililerinin bu konuyla ilgili kabul etmediği bir çok iddianın daha sonra gerçek olduğu ortaya çıkmaktadır.

2.4.2 Şeffaflık

Devletlerin filtreleme ve erişim engelleme uygulamalarının analizinde kullanılacak ikinci ölçüt “şeffaflık”tır. Engelleme yapan devlet, hangi tür içeriklerin engellendiği konusunda açık mıdır ve engellemeyi belirleyen kriterler ne kadar belirgindir? Engellenen içeriklerin tipleri ve kategorileri ile engelleme kriterleri ne kadar şeffaf ise uygulamaların meşruluğu o kadar yüksek olacaktır (Bambauer, 2008).

Ayrıca, uygulamaların “şeffaflık” ölçütüyle değerlendirilmesinden ortaya çıkan sonuç, engellemelerin gerekçelerine ne kadar uygun olduklarını test etmeye de imkan verecektir. Diğer bir anlatımla, “şeffaflık” ölçütünün test edilmesiyle, ilk yapılan “açıklık” ölçütünün analizi daha da genişletilmekte ve derinleştirilmektedir. Yani, ilk aşamada engelleme yaptığını ve yaptığı engellemelerin gerekçelerini kayda geçiren devlet, ikinci aşamada engellediği içerik tipini ve kullandığı kriterleri beyan ederek kendisini bağlamakta; engelleme gerekçeleri ile engellenen içerik türü ve kullandığı

kriterler arasında herhangi bir uyumsuzluğun veya uygunsuzluğun olup olmadığı konusunda değerlendirmeler yapılabilmesine olanak tanımaktadır (Bambauer, 2008).

“Açıklık” testi bir devletin içerik engellemesi uygulamalarının nedenlerini beyan edip etmediğini değerlendirirken; “şeffaflık” testi, devletin neyi engellediğini tanımlayıp tanımlamadığını değerlendirmektedir (Bambauer, 2008). Bir devlet filtreleme ve erişim engelleme konusunda “şeffaf” olmaksızın “açık” olabilir. Mesela Tunus, İSS’lerden “kamu düzenine ve ahlakına aykırı içerikleri” engellemelerini isteyerek (OpenNet, 07.08.2009b), engelleme yapacağını ve gerekçesini ortaya koymakla “açıklık” ölçütüne uygun davranmış fakat; engellenen içeriklerin tipleri ve engelleme kriterleri konusunu muğlak bırakarak (Villeneuve, 2005) İnternet sansürünü gizlemiş ve “şeffaflık” ölçütüne uymamıştır.

“Şeffaflık” ölçütünde, engellenen içeriğin türü veya tipinin net olarak belirlenmiş olması ne kadar önemliyse, engellenen içeriği tanımlamak için kullanılan kriterler de en az o kadar önemlidir. Engellenen içerik ne kadar açık, belgelendirilmiş ve kesin olursa, hükümet yetkilileri veya ISP’ler de yasaklanan alan içerisindeki diğer siteleri tanımlamak için daha az takdir yetkisine sahip olacaklardır. Bu nedenle, yasaklanmış içeriğe ilişkin detaylı tanımlanmış kriterlerin yer aldığı resmi belgeler, “şeffaflık”ı ve dolayısıyla meşruiyeti daha da artıracaktır (Bambauer, 2008).

Özetle, “şeffaflık” analizi bir devletin engellemek istediği materyali ne kadar net biçimde tanımladığını belirler. Bu analiz, “açıklık” analizini daha da derinleştirerek, deklare edilen engelleme gerekçeleri ile bunlara dayanarak engellemeyi hedeflediği içerik arasında bir karşılaştırmayı mümkün kılar (Bambauer, 2008).

2.4.3 Kısıtlılık

Devletlerin filtreleme ve erişim engelleme uygulamalarının analizinde kullanılacak üçüncü ölçüt “kısıtlılık”tır. Devletin yapmış olduğu engelleme uygulamalarına ilişkin iddia ve beyanları ile gerçekte ortaya çıkan ampirik veriler ne kadar uyushmaktadır? Bu test bir devletin içerik filtreleme ve erişim engelleme uygulamaları konusundaki iddialarının geçerliliğini denetlemektedir. Bu ölçüt ile test edilen husus, ilgili

devletin engellemeye ilişkin iddiaları ile yaptıkları arasındaki uyum ve uygunluktur. “Kısıtlılık” ölçütünde, filtreleme ve erişim engellemesi uygulamalarının engellemeye ilişkin beyanlarda belirtilen sınırlar içerisinde yapılıp yapılmadığı, uygulamaların dar veya geniş kapsamlı olup olmadığı incelenmektedir. “Açıklık” ve “şeffaflık” bir ülkenin engelleme uygulaması konusundaki iddia ve beyanlarını değerlendirirken; kısıtlılık ise fiili durumu ve uygulamaları incelemektedir (Bambauer, 2008).

Filtreleme ve erişim engelleme sistemlerinin tamamı olmasa da çoğunun kapsamı ya hedeflenenin ötesinde içeriği engellediği için fazla geniş/aşırı ya da engellenmek istenen içeriği engelleyemediği için fazla kısıtlı/dardır. Geniş/aşırı kapsamlı filtreleme, kullanıcıların zararlı veya yasak olarak tanımlanmayan içeriğe erişimlerini engelerken; kısıtlı/dar kapsamlı engelleme devletin zararlı gördüğü içeriği engelleyemediği anlamına gelmektedir. “Kısıtlılık” ölçütü açısından bunlardan her ikisi de sorunludur ve engellenmenin meşruiyetini zedelemektedir. Çünkü, her iki durum da bir devletin erişimi kısıtlama için geliştirdiği ve beyan ettiği gerekçelendirmeye temelden zarar vermekte; engelleme karar ve çabalarının doğruluğu, inanırılılığı ve uygulamanın ciddiyeti konusunda şüpheler uyandırmakta ve engelleme sistemi üzerinde güvensizlik oluşturmaktadır (Bambauer, 2008).

Devletler, bazen istemedikleri halde teknik yetersizlikten veya başka bir sebepten bu iki sorunlu durumla karşı karşıya kalabilmektedir. Fakat, özellikle geniş/aşırı kapsamlı engellemede çoğu zaman, devletler kasten ve bilinçli olarak sonuçlarının ne olacağını bildikleri filtreleme ve erişim engelleme tekniklerini tercih etmek suretiyle bu sorunlu durumların oluşmasına neden olmaktadır (Bambauer, 2008). Örneğin, Vietnam yalnızca pornografik veya çocuklar için sosyal anlamda zararlı web sitelerini filtrelediğini iddia ederken, engelleme sistemini politik muhalefet ve reform sitelerinin erişilememesini sağlamaya odaklamıştır. Bu, devletin tek partili Komünist sistemini korumayı amaçlayan kasıtlı bir stratejidir (OpenNet, 07.08.2012).

Bazı durumlarda kısıtlı/dar kapsamlı engelleme, yani yasaklı tüm içeriğin değil de bazı içeriklerin engellenmiş olması, hükümetlerin engellenecekler arasından seçici denetim yaptıklarına bir işaret olabilmektedir. Örneğin Mısır geçmişte, ulusal

emniyeti tehdit eden sitelerin engellenmesini onaylayan bir mahkeme kararına dayanarak birçok rejim muhalifi siteyi engelleyebilecekken, bu kararı özellikle ülkenin en büyük politik muhalefet hareketi olan Müslüman Kardeşler Cemaati'nin web sayfasını sansürlemek için kullanmıştır (Human Rights Watch, 2005).

Bir devletin engelleme uygulamalarının dar veya geniş kapsamlı, ya da her iki özelliğe de sahip olup olmadığı ampirik testlerle anlaşılabilir. Fakat bunu gerçekleştirmek oldukça güçtür. Web sayfalarının sayısının hızla artması nedeniyle temsil niteliğinde bir örneğin test edilmesi dahi neredeyse imkansızdır. Ancak, Açık Erişim İnisiyatifi (OpenNet Initiative-ONI), İnsan Hakları İzleme Örgütü (Human Rights Watch-HRW) ve Sınır Tanımayan Gazeteciler (Reporters Without Borders-RSF) gibi gözlemci kuruluşlar bu konuda bir takım yöntemler geliştirerek bu sorunu aşmaya ve ampirik veriler elde etmeye çalışmaktadır (Bambauer, 2008).

Şu ana kadar açıklanmaya çalışılan üç ölçütten “açıklık”, bir devletin engelleme konusundaki gerekçelerini ve eylemlerini ne kadar açıkça beyan ettiğini değerlendirirken, “şeffaflık” devletin engellemek istediği içeriğin türünü ve kriterlerini gösteren haritayı çıkartmaktadır. “Kısıtlılık” ise ilk iki ölçüt çerçevesinde ortaya konulan beyan ve iddiaların, devletin eylemlerinde ne kadar yansıma bulduğu; iddia edilen ile uygulama arasında, engellemenin kapsamı açısından tam bir örtüşmenin olup olmadığını test etmektedir (Bambauer, 2008).

2.4.4 Sorumluluk

Devletlerin filtreleme ve erişim engelleme uygulamalarının analizinde kullanılacak dördüncü ve son ölçüt “sorumluluk”tur. Kullanıcıların engelleme sistemi ve politikalarını etkileyebilme düzeyleri ne kadardır? Ne tür önlemler veya yapılar yetkilileri konunun tarafı olanlara karşı cevap vermeye zorlamaktadır? Yanlışlıkla engellendiklerini iddia eden içerik sahipleri hangi makama başvurabilirler? Bu ölçütle, bir devletin engelleme politikalarının vatandaşlarının talep ve görüşlerine ne kadar yakın olduğu yanında, engelleme sisteminin kusursuz olmayacağı ön kabulüyle, devlet yetkililerinin görev ve sorumluluk alanlarının belli olup olmadığı

ve engellemelere karşı itiraz yollarının bulunup bulunmadığı test edilmektedir. Dolayısıyla, “sorumluluk” ölçütünün dört önemli yönü ortaya çıkmaktadır; engelleme kararlarına katılım, yetki tanımlama, engellemeye karşı çıkma imkanı ve çoğunluğun tercihlerine aykırı sınırlamalar (Bambauer, 2008).

Engelleme kararlarına katılım, vatandaşların ve her ülkede İnternet dünyasının en kalabalık paydaşını oluşturan kullanıcıların, engelleme karar ve uygulamalarına ilişkin talep ve görüşlerinin demokratik bir iklim içerisinde karşılık bulmasıdır. Tabiatıyla bu durum, ülkelerin genel olarak demokratik ve katılımcı bir siyasal sisteme sahip olmalarıyla yakından ilgilidir. Genel olarak siyasal katılıma değer veren siyasal rejimlerde, engellemeye ilişkin karar ve uygulamalar konusunda da elverişli bir ortamın bulunacağı düşünülebilir. Aksine, sansürün yaygın olduğu otoriter ve totaliter rejimlerde, erişim engelleme politikalarına vatandaşların ve kullanıcıların katılım yoluyla etkide bulunmaları pek mümkün olmayacaktır.

Ancak, katılım bazen demokratik bir hükümete sahip olmayan devletlerde dahi görülebilmektedir. Örneğin, vatandaşlarının sınırlı siyasi katılımına izin veren Suudi Arabistan, İnternet kullanıcılarına, engellenmesini istedikleri içeriklerle ilgili ihbarda bulunma imkanı sağladığı gibi, engelleme kararlarına ve engelleme uygulanan sitelere ilişkin itirazda bulunma hakkı (Internet.sa, 2013d) da tanımıştır. Kullanıcıların itirazları iki gün içerisinde gözden geçirilmekte (Internet.sa, 2013e) ve engellenmenin hükümet komitesince belirlenmiş kurallar çerçevesinde olmadığına karar verilirse engellemeye son verilmektedir (Arabnews, 02.10.2005).

Bu “ihbar” ve “itiraz” sistemi, katılım açısından olumlu bir etkiye sahip olmakla birlikte, engelli sitelerin sayısının giderek daha da artması sonucunu da doğurmaktadır. Örneğin, yetkililerce 2001 yılında sitelerin engellenmesine yönelik taleplerin %30’u haklı bulunurken, engellenen içeriğe yapılan itirazların sadece %3’ü kabul edilmiştir (Al-Zoman, 2001). Buna rağmen, Suudi Arabistan’da vatandaşların ülkelerinin erişim engelleme sistemine etki edebilmesi açısından önemli bir imkana sahip oldukları dile getirilmektedir (Bambauer, 2008). Nitekim, bu uygulamaların kullanıcılar nezdinde kısmi bir olumlu etkiye sahip olduğu söylenebilir. Yapılan bir

araştırma bu görüşü destekler mahiyettedir. Araştırma, kullanıcıların %41'inin engelleme düzeyinden memnun olduklarını, %45'inin kısıtlamaları çok ağır bulunduğunu ve %14'ünün de daha fazla kısıtlama getirilmesini istediğini ortaya çıkarmıştır (ISU, 1999).

“Sorumluluk” ölçütünün ikinci önemli yönünü ise, erişim engelleme sisteminde yer alan aktörlerin ve özellikle kamu kurum ve görevlilerinin yetki ve sorumluluklarının açıkça belirtilmesi oluşturmaktadır. Engelleme süreci, yetki ve sorumlulukların sınırları çizildiğinde ve içerik engellemeye ilişkin esaslar kanun veya kurallar çerçevesinde resmi olarak tanımlandığında büyük ölçüde kolaylaşan bir süreçtir. Engelleme işlemlerinin ve kriterlerinin belirlenmesiyle, sadece vatandaşların ve diğer paydaşların konuya ilişkin bilgilenmesi temin edilmiş olmayacak, aynı zamanda engelleme kararlarına, uygulayıcılarına ve uygulamalarına net sınırlar da çizilmiş olacaktır. Böylece, uygulamaların “sorumluluk” açısından hukuki ve siyasi denetiminin yapılmasını sağlamaya elverişli bir zemin oluşacaktır (Bambauer, 2008).

“Sorumluluk” ölçütünün üçüncü önemli yönü ise, erişim engelleme kararlarına itiraz yolunun açık olmasıyla ilgilidir. Engelleme karar ve işlemlerinin hatalar içermesi veya içerik sahipleri tarafından böyle algılanabilmesi mümkündür. Bu gibi durumlarda engellemeye maruz kalan içerik sahibinin veya engellenenin uygun olmadığı kanaatinde olan kullanıcıların itiraz hakkının olması gerekmektedir. Erişim engellemelerine karşı itirazlar, devleti kararlarını gerekçelendirmeye veya belirlemiş olduğu kriterlere uymaya zorlarken, içerik oluşturucuların içeriklerinin yasallığını savunmalarına izin vererek meşruiyeti geliştirmekte ve engelleme sistemini daha da güçlendirmektedir (Bambauer, 2008). Nitekim, demokratik ülkelerin çoğu bağımsız mahkemeler aracılığıyla bu imkanı sağlamaktadır.

“Sorumluluk” ölçütü bağlamında erişim engellemeye itiraz edebilme konusunda en kötü uygulamaya sahip ülkelerden birisi Çin'dir. Devlet sansür politikalarını, kanunlar, idari yönetmelikler ve gayri resmi önlemlerle birlikte, Cisco, Yahoo! ve Google gibi ABD firmalarının da destek sağladığı resmi yasal kısıtlamalar ve sözsüz işbirliği uygulamalarıyla yürütmektedir. Bu karmaşa içinde sansüre nasıl karşı

çıkılacağı ve kimin sorumlu tutulacağı belirlenmesi neredeyse imkansızdır (OpenNet, 09.08.2012a; ISC, 2002). Keza, gayri resmi baskılardan Çin’de sansüre itirazda bulunmak cesaret istemektedir. Bu nedenle, vatandaşlar resmi itirazları nafîle çabalar olarak görmektedir (Fallows, 2008).

“Sorumluluk” ölçütünün dördüncü önemli yönü ise, engelleme uygulamalarında azınlığın korunması ve çoğunluk tercihlerine karşı kısıtlamaların varlığıdır (Bambauer, 2008). Özellikle antidemokratik yönetimlerde azınlıklara ilişkin içeriğin sansürlenmesi yaygın bir uygulamadır. Örneğin Vietnam, Central Highlands bölgesindeki yerli bir grup olan Montagnardlarla ilgili içerikleri engellemektedir. Montagnardlar, Vietnam Savaşı’nda ABD’ye yardım ettikleri için siyasi, çoğunluğu Hristiyan olduğu için de dini bir azınlıktır (Human Rights Watch, 2006). Keza, Suudi Arabistan, Bahai inancı ve Sünni olmayan mezheplere ait içeriklere erişimi engellemektedir (OpenNet, 2004). Benzer şekilde, Pakistan Belucistan ve Sindh illerinin bağımsızlığını savunan siteleri engellemektedir (OpenNet, 10.05.2007).

Halbuki, ileri demokrasinin koşullarından birisi de çoğunluk karşısında azınlığın korunması ve ayrımcılığın önlenmesidir. Erişim engelleme uygulamaları için çoğunluğa karşı azınlık grup, görüş ve düşüncelerin korunması daha da önem kazanmaktadır. Bu nedenle, içerik engellemelerinde çoğunluk kararı üzerindeki denetimlere yönelik daha büyük bir ihtiyaç ortaya çıkmaktadır (Bambauer, 2008).

Bambauer, bu dört ölçütlü çerçeveye, devletlerin erişim engelleme uygulamalarını analiz etme ve meşruiyetlerini ölçme konusunda analitik bir model sunmaktadır. Bu çerçeveyi uygulamanın en iyi yolu bir devletin dört kriterden her birine nasıl uyduğunu ölçen nicel ölçütler oluşturmaktır. Bu ölçütler kullanıldığı sürece kaçınılmaz olarak kurumlar birbirleriyle rekabet edecek; bu rekabet de ölçümlerini ve dolayısıyla uygulamaları iyileştirecek ve geliştirecektir. Söz konusu ölçütler İnternetin kısıtlanmasına dair kurumsal kararları ve hükümet düzenlemelerini yönlendirebilir ve yönlendirmelidir (Bambauer, 2008).

Devletlerin İnternet içerik düzenlemeleriyle ilgili sağlıklı değerlendirmeler yapılabilmesi için kamu kuruluşları, özel sektör kuruluşları ve gözlemci STK'larının ortak çalışmalarıyla, farklı uzmanlar ve analizciler kullanılarak, gerek bahsi geçen dört ölçüt çerçevesinde, gerekse bu çalışmalarla ortaya çıkacak yeni ölçüt ve modellerle uzun soluklu çalışmalar yapılmasına ihtiyaç vardır. Söz konusu çalışmalar uzun soluklu olmalıdır, çünkü, içerik düzenlemesini değerlendirebilmek için gerekli ilkelerin ve ölçütlerin belirlenmesine dair çabalar çok yavaş gelişmektedir (Ganesan, 2008).

Halbuki, devletlerin içerik düzenlemesi uygulamaları konusunda nesnel, ölçülebilir ve kıyaslanabilir bir analiz yapabilmek için bu ve benzeri ölçütlerin ortaya konulmasının ve bunların sayısal değerlerle ölçülebilir hale getirilmesinin önemi büyüktür. Bu türden çalışmalarda söz konusu ölçütler, içerik düzenleme kararlarının açık hale getirilerek devletlerin farklı testler altında değerlendirilmesi ve belki de ülke uygulamaları konusunda fikir birliğine varılması için bir araç oluşturabilirler. Tıpkı, İnternet'in geçerli dilini oluşturan protokoller gibi bunlarda karşılıklı mutabakata dayalı standartlar olarak geçerlilik kazanabilirler (Bambauer, 2008).

Bu durum, ülkelerin sübjektif ve keyfi değerlendirmeler ile töhmet altında bırakılarak peşinen “sansürcü” veya “özgürlükçü” yaftalamalarına maruz kalmasının önüne geçecektir. Halen, bazı uluslararası STK'larının ülkelerin öznel ve nesnel gerçekliklerini görmezden gelerek, bir takım önyargılar ile bazı ülkeleri İnternet düşmanı veya bazılarını İnternet dostu olarak ilan ettiği ve dünya kamuoyu önünde mahkum ettiği görülmektedir.

Bu değerlendirme ve yorumların kimi zaman isabet ettiği fakat, bazen ise, haksız nitelemelere neden olduğu gözlemlenmektedir. Söz konusu haksız nitelemelerin bazı durumlarda ülkelerin farklı sosyal, siyasal, kültürel ve tarihsel özelliklerini ve dolayısıyla, içerik düzenlemelerine ilişkin ortaya çıkan farklı uygulamalarını tam olarak anlayamamaktan kaynaklandığına tanık olunmaktadır. Bazı örnekler ise, kasıt ve artniyet ihtimalini gündeme getirmektedir.

Nitekim, Human Rights Watch, OpenNet Initiative, Reporters Without Borders ve Freedom House gibi her türlü devlet sansürüne karşı mücadele veren uluslararası örgütlerin İnternet özgürlüğü konusunda bazı durumlarda ABD ve AB ülkeleri lehine çifte standart uyguladıkları görülmektedir. Dünya uygulamaları başlığı altında birçok örneğine rastlandığı gibi, ABD, İngiltere, Fransa ve Almanya’da ulusal güvenlik ve terörizmle mücadele gerekçesi ile İnternetin ulusal ve uluslararası ölçekte resmi ve gayriresmi yöntemlerle sıkı şekilde izlendiği, trafiğinin takip edildiği ve doğrudan İSS’lar üzerinden “zorunlu gönüllülük” ile filtreleme uygulamaları gerçekleştirildiği görülmektedir. Özellikle, ABD’nin İnternet üzerindeki hakim gücünü ve ülkesindeki küresel İnternet şirketlerini de kullanarak çok sofistike yöntemlerle tüm ülkelere yönelik İnternet üzerinden bilgi topladığı, iletişimi kontrol ettiği ve İnterneti denetlediği bilinmektedir. Bütün bunlara rağmen söz konusu İnsan hakları ve İnternet özgürlüğünü savunan uluslararası örgütlerin çoğu zaman bu durumu görmedikleri veya yeterince gündeme getirmedikleri gözlemlenmektedir.

Diğer yandan, konuyla ilgili olarak, İnternet sansürü tartışmalarının, tıpkı nükleer silahlara sahip olma konusunda yaşanan tartışmalara benzer nitlikte, ülkelerin ulusal güvenliklerini ilgilendiren bir başka bir boyutunun daha olduğu üzerinde durulmaktadır. O da, söz konusu gelişmiş batılı ülkelerin, zorunluluk durumunda İnterneti tümünden veya kısmen durdurabilecek ya da izleme, kontrol ve denetim altına alabilecek teknik altyapıya sahip olmalarına rağmen, diğer ülkelerin bu altyapıya sahip olmalarını istememe yönündeki politikalarıdır.

Kendileriyle mülakat yaptığımız TİB uzmanlarının bir kısmı sansür tartışmaları konusunun özellikle bu yönüne dikkat çekmektedir. Buna göre, ülkesel çıkarları için İnterneti diğer ülkelere nüfuz etme ve bu ülkelerdeki sosyal ve siyasal operasyonlarda bir araç olarak kullanma eğiliminde olan İnternetin hakim güçleri,⁴¹ bu imkandan mahrum olmamak amacıyla, söz konusu ülkelerin bu tür operasyonları etkisiz kılacak İnternet altyapısına sahip olmasının önüne geçmek için “sansür” kozunu kullanmaktadır. Bu kapsamda, İnternet özgürlüğünü savunan bahsi geçen

⁴¹ Bu noktada Arap Baharı süreci, yakın zamanda Mısır’da gerçekleştirilen Askeri Darbe öncesi ve Türkiye’deki Gezi Parkı olayları hatırlatılmaktadır.

uluslararası örgütleri de doğrudan veya dolaylı yollarla işin içine sokarak, diğer ülkelerin İnterneti kontrol ve denetim altına almaya yönelik altyapı çalışmalarını, içerik düzenlemesi girişimlerini ve uygulamalarını bloke etmeye çalışmaktadırlar. Bu yolla, bazen haklı bazen ise haksız olarak, söz konusu ülkelerin içerik düzenleme ve uygulamaları İnternette sansüre sebep olma gerekçesiyle uluslararası kamuoyu nezdinde mahkum edilmektedir.

Bahsi geçen şüphe, tartışma ve sakıncaların giderilebilmesi için ondördüncü alt hipotezde belirtildiği gibi, devletlerin içerik düzenlemesi uygulamaları konusunda nesnel, ölçülebilir ve kıyaslanabilir bir analiz yapabilmeye imkan tanıyan ilkelerin ve ölçütlerin belirlenmesi önem taşımaktadır. Uluslararası işbirliği çerçevesinde bu konuda yapılacak çalışmalar süreç içinde, ülke uygulamaları konusunda fikir birliğine varılması için bir araç da oluşturabilir.

2.5 DÜNYADA İÇERİK DÜZENLEMESİ UYGULAMALARI

İnternet içerik düzenlenmeleri, doğu-batı, güney-kuzey, demokratik-totaliter, gelişmiş-az gelişmiş hemen hemen dünyadaki bütün ülkelerde giderek daha da yaygınlaşmaktadır. Konuya ilişkin uygulamalar, ülkelerin ekonomik, teknolojik, kültürel gelişmişlik düzeylerine ve sosyolojik ve siyasal kodlarına, inanç haritalarına göre farklılık göstermektedir. Başka bir deyişle, bazı ortak noktalar bulunmakla birlikte, ülkelerin özelliklerine göre, içerik düzenleme politikaları, kullanılan araçlar, teknikler ve kriterler, düzenlemelerin kapsamı, süreçleri farklılık arz etmektedir. Bu çerçevede, bazı uluslararası toplulukların ve belli başlı ülkelerin İnternet içerik düzenlemesine ilişkin yaklaşımları ve uygulamaları bu kısımda irdelenecektir.

2.5.1 Uluslararası Kuruluşlar

İnternet düzenlemelerinin gereğini farkedenden uluslararası kuruluşlar, bilişim suçları ve sakıncalı içerikle mücadele boyutuyla ilgili olarak bir takım çalışmalar yapmaktadır. Avrupa Konseyi, AGİT ve AB gibi uluslararası organizasyonların yürütmüş olduğu bu çalışmaların odak noktasını, uluslararası işbirliği ve bu alanda ortak bir dil ve uygulama usulü geliştirilmesi konusu oluşturmaktadır (Turan, 2006: 75).

2.5.1.1 Avrupa Konseyi

Avrupa Konseyi (AK), İnternet ve bilişim sistemleri kullanılarak gerçekleştirilen suçlar ve ortaya çıkan sorunlarla mücadele etmek amacıyla çalışmalar yürütmektedir. AK, İnternete ve İnternet içeriğine ilişkin politikalarını da ortaya koyan üç önemli uluslararası belge yayınlamıştır. Bunlar, “Siber Suç Sözleşmesi”, “İnternette İletişim Özgürlüğü Deklarasyonu” ve “Bilgi Toplumunda İnsan Hakları ve Hukukun Üstünlüğü Bakanlar Komitesi” Bildirgesi’dir.

2.5.1.1.1 Siber Suç Sözleşmesi

AK, İnternetin küresel özelliği nedeniyle ulusal düzeydeki hukuki düzenlemelerin yetersiz kaldığından, İnternet üzerinden işlenen suçlarla mücadelede uluslararası bir düzenlemeye ihtiyaç olduğundan hareketle, 1980’li yılların sonunda bu konuyla ilgili olarak Uzmanlar Komitesi’ni kurmuştur. Böylece, ceza kanunları ile düzenlenmesi gerekli olan eylemlerin hangileri olduğu tespit edilmeye çalışılırken, özgürlüklerle güvenlik arasındaki çizginin de doğru bir şekilde belirlenmesi konusunda üye ülkelere yol gösterilmesi amaçlanmıştır (Yıldız, 2007:133; Gürkaynak vd., 2010).

Beş yıllık bir çalışmadan sonra ortaya çıkan Sözleşme (COE, 2001), 23.11.2001 tarihinde Budapeşte’de yapılan toplantıda imzaya açılmıştır (Helvacıoğlu, 2004:278). Bugüne kadar Sözleşme’yi, 39 AK üyesi ile üye olmayan Kanada, Japonya, Güney Afrika ve ABD imzalamıştır. Türkiye Sözleşme’yi 10.11.2010 tarihinde imzalamış, ancak henüz TBMM onayından geçirmemiştir (Altınay, 2011: 29). Ayrıca, kişisel verilerin korunması için gerekli düzenlemeler yapılmadığından ek protokol imzalanmamıştır (Dülger, 2004: 105).

Sözleşme’nin hedefi, ortak bir ceza politikasının oluşturulması ile toplumun siber suça karşı korunması ve uluslararası işbirliğinin geliştirilmesidir. Sözleşme’de, telif hakkı ihlalleri, bilgisayarlarla ilişkili sahtecilik fiilleri, çocuk pornografisi, ağ güvenliği ihlalleri ve siber suçla mücadelede kullanılacak olan yetki ve prosedürler ele alınmıştır (Yıldız, 2007:134). Diğer yandan, Sözleşme’de içerikle ilgili sadece çocuk pornografisi ve telif haklarına ilişkin yaptırım öngörülmüştür (COE, 2001).

Sözleşme'nin 9. maddesinde yer alan çocuk pornografisi ile ilgili düzenlemede, ilk olarak, çocukları özellikle cinsel sömürüden koruyacak önlemlerin güçlendirilmesi hedeflenmektedir. Buna göre, Sözleşme'ye taraf ülkelerin ulusal ceza hukuku düzenlerinin ilgili maddelerinin bu Sözleşme çerçevesinde yeniden düzenlenmesi, hatta bu konuya ilişkin herhangi bir düzenleme bulunmuyorsa bunların yapılması ile çocuklara yönelik cinsel suçlarda bilişim sistemlerinin kullanılmasına karşı daha etkin hükümlere yer verilmesi istenilmektedir (Dülger, 2011).

Daha sonra bu çerçevede cezalandırılması istenilen çocuk pornografisine yönelik fiiller; materyali üretmek, sunmak, erişim sağlamak, dağıtmak, yaymak, temin etmek ve bulundurmak şeklinde sıralanmıştır (COE, 2001). Bu hüküm ile çocuk pornografisinin ve bu yolla çocukların sömürülmesinin önüne geçilebilmesi için, olayın kaynağının kesilmesi amaçlanmıştır. Böylece Sözleşme'yi düzenleyenlere göre çocuk pornografisine olan arz ve talep tamamen sona erecektir (Dülger, 2011).

Sözleşme'nin aynı maddesinde, “çocuk pornografisi” teriminin neleri içerdiği de belirlenmiştir. Buna göre, cinsel anlamda müstehcen bir eyleme “reşit olmayan”, veya “reşit görünmeyen” bir kişinin katılımını gösteren görüntülerin yanı sıra, bu eyleme “reşit olmayan bir kişiyi katılmış gibi gösteren gerçekçi görüntüler” de çocuk pornografisi kapsamına alınmıştır (COE, 2001). Bu şekilde çocuk pornografisi kavramının içerisine; resim, film, çizgi film, yapay resim ve hatta yapay canlandırmalar (simülasyon) da girmektedir (Dülger, 2011).

Sözkonusu madde, ‘reşit olmayan’ tabirini, “18 yaşından küçük kişiler” olarak belirlemiş fakat, taraflardan herhangi birisinin reşitlik yaşıyla ilgili olarak 16’dan küçük olmamak üzere farklı bir yaş sınırı belirleyebileceğini düzenlemiştir (COE, 2001). Diğer yandan, “cinsel anlamda müstehcen eylem” her ne kadar Sözleşme içerisinde kesin bir ifadeyle tanımlanmamışsa da bunun ne anlama geldiği Sözleşme'nin açıklayıcı metninde belirtilmiştir.⁴²

⁴² Buna göre, “cinsel organ-cinsel organ, oral-cinsel organ, anal-cinsel organ veya oral-anal” olmak üzere, reşit olmayan kişiler arasındaki, bir yetişkin ve bir reşit olmayan kişi arasındaki, aynı ya da

Sözleşme'nin özellikle elektronik alana ilişkin düzenlemelerde gözönünde bulundurulması gereken şartlara ve önlemlere atıfta bulunduğu 15. maddesinde, yapılacak düzenlemelerin AİHS'nden, 1966 tarihli Sivil ve Siyasi Haklar Hakkındaki Uluslararası BM Anlaşması'ndan, ayrıca yürürlükte bulunan diğer uluslararası insan hakları belgelerinden kaynaklı yükümlülüklerden doğan hakların gerekli ölçüde korunmasını temin edecek ve hakkaniyet ilkesini tesis edecek şekilde yapılması istenilmektedir (COE, 2001).

Zamanla, hortlayan ırkçılık ve yabancı düşmanlığının örgütlü hale gelmesi ve bu örgütlerin birbirleriyle iletişime geçme, propaganda yapma ve organize olma konusunda İnterneti etkin bir şekilde kullanmaya başlaması, bu hususta tarihsel acılar yaşamış coğrafyanın kuruluşu olarak AK'ni harekete geçirmiştir (Dülger, 2004: 108). Nitekim AK, Avrupa Siber Suç Sözleşmesi'ne ek Protokol hazırlayarak 28 Ocak 2003 tarihinde bu metni imzaya açmıştır. "Bilişim Sistemleri Aracılığıyla İşlenen Irkçı ve Yabancı Düşmanı Eylemlerin Suç Haline Getirilmesi İçin Avrupa Siber Suç Sözleşmesi'ne Ek Protokol" olarak adlandırılan bu protokol ile Siber Suç Sözleşmesi'nin benimsediği İnternet suçları arasına bir içerik suçu olarak ırkçılık ve yabancı düşmanlığı da girmiştir (COE, 2003a). Siber Suç Sözleşmesi, İnternet ve diğer bilişim ağları aracılığı ile işlenen suçlara yönelik ilk ve tek uluslararası sözleşme olması nedeniyle tarihsel öneme sahiptir.

2.5.1.1.2 İnternette İletişim Özgürlüğü Deklarasyonu

28 Mayıs 2003 tarihinde AK Bakanlar Komitesi tarafından imzalanan İnternette İletişim Özgürlüğü Deklarasyonu'nda, üye devletlerin İnternet içeriği ile ilgili yapacakları yasal düzenlemelerde uymaları gereken ilkeler belirlenmiştir. Buna göre Deklarasyon'da, şu ilkelere yer verilmiştir (COE, 2003b):

farklı cinsiyetler arasındaki cinsel ilişki, hayvanlarla cinsel ilişki, mastürbasyon, cinsel anlamda sadistik ya da mazoşistik kötü muamele ve reşit olmayan bir kişinin cinsel organlarının ya da cinsel bölgesinin şehvet uyandırıcı biçimde teşhir edilmesi bu kapsamda değerlendirilmektedir.(Dülger, 2011)

- İnternet içeriği sunanlara, diğer içerik sunan araçlara getirilen düzenlemelerin üstünde bir sınırlama ve özel izin prosedürü getirilmemelidir.
- İnternette yayınlanan içerikle ilgili olarak öz-denetim teşvik edilmelidir.
- Kamu makamları, filtreleme veya erişim engelleme tedbirlerine başvurarak, İnternette bilgiye ve diğer iletişimlere erişimi engellememelidir. Fakat, bu durum, kamu makamlarının içeriğin yasa dışılığı ile ilgili geçici veya nihai bir karar vermesi halinde bu içeriğin kaldırılması veya siteye erişimin engellenmesi yönündeki önlemlere mani değildir. Ayrıca, özellikle okul ve kütüphaneler gibi çocukların İnternete erişim sağlayabileceği yerlerde, çocukların korunması amacıyla filtreleme sistemlerinin kurulabileceği belirtilmektedir.
- İSS'lara, erişim sağladıkları, ilettikleri veya depoladıkları İnternet içeriğini izlemeleri yönünde veya söz konusu içeriğin yasal olmadığını gösteren olaylar veya koşulların aktif olarak araştırılması yönünde bir sorumluluk yüklenmemelidir. İçerik sağlayanın ifade özgürlüğü ile kullanıcıların bilgi edinme haklarına azami önem ve dikkat gösterilmelidir. Bunun yanında İSS'ların, yasalarda belirtildiği şekilde içeriğin yasadışı olduğunun tespit edilmesi veya bir tazminat talebi halinde, bu içeriği hemen kaldırma veya erişimi engelleme yönündeki sorumlulukları devam etmektedir.
- Bilgi ve düşüncenin özgürce ifade edilmesini teşvik etmek ve İnternette izlenmeyi engellemek için, İnternet kullanıcılarının kimliklerini açıklamama (anonimlik hakkı) isteklerine saygı gösterilmelidir. Diğer yandan, uluslararası sözleşmeler ve ulusal hukuk kuralları çerçevesinde belirtilen kısıtlara uygun olarak, suçun işlenmesini önlemek veya suçluların izlerini takip edebilmek amacıyla İnternet kullanıcılarının kimlikleri kullanılabilir.

2.5.1.1.3 Bilgi Toplumunda İnsan Hakları ve Hukukun Üstünlüğü Bakanlar Komitesi Bildirgesi

13 Mayıs 2005 tarihli Bildirgede AK üye devletlerine, insan hakları, demokrasi, hukukun üstünlüğü, sosyal uyum, kültürel çeşitlilik gibi değerlere dayanan taahhütleri hatırlatılarak, tüm bunların bilgi toplumu dönemi için de geçerli olduğu vurgulanmaktadır. Bilgi ve iletişim teknolojilerinin insan hakları açısından hem

olumlu hem de olumsuz güçlü bir etkisinin bulunduğu farkında olarak olumsuz etkilere korunmak gerektiği; bunun içinse AİHS’nde güvence altına alınan temel hak ve özgürlüklerin tamamen bilgi çağında da geçerli sayıldığı ve korunmaya devam etmesi gerektiği teyit edilmektedir. Ulusal düzenlemelerde bunların göz önüne alınması gerektiği dile getirilmektedir (COE, 2005).

Bildirgeye göre, bilgi toplumunda şartlar, insan hakları kısıtlamaları için yeni önlemler almayı doğuruyorsa, bu önlemlerin uluslararası insan hakları standartlarına uyarak; mümkün olduğunca yasal ve tanımlı, gerekli ve hedeflediği amacı ile orantılı ve yargı denetimine tabi olarak gerçekleştirilmesi gerekmektedir. Ayrıca, ifade özgürlüğünün temini için, üye ülkeler, ırkçılık, ırk ayrımcılığı ve çocuk pornografisi gibi yasal olmayan İnternet içeriğiyle mücadele için, bu tür suçlara eşit olarak uygulanabilecek ulusal düzenlemeleri sağlamalıdır. Bu konuda, Siber Suç Sözleşmesi’ne uymayı temin etmelidirler (COE, 2005).

Diğer yandan, üye ülkeler, öz ve birlikte düzenleme için İSS’lar, yazılım şirketleri, içerik sağlayıcıları, meslek kuruluşları gibi sektör temsilcilerinden oluşan ilgili paydaşların, düzenleme yapma ve karar alma süreçlerine katılımını sağlamalıdır. Bu yaklaşım ifade ve iletişim özgürlüğünü temin edebilir (COE, 2005).

2.5.1.2 Avrupa Güvenlik ve İşbirliği Teşkilatı

2011 yılında, AGİT tarafından üye ülkelerin mevzuatındaki İnternet içerik düzenlemeleri, devlet uygulamaları ve ifade özgürlüğü ile ilgili yaklaşımları belirlemek amacıyla bir çalışma yapılmıştır. Bu çerçevede 56 üye ülkeden bilgi toplanmak istenilmiş fakat, bu ülkelerin 10’undan herhangi bir bilgi elde edilememiştir. Bu çalışmaya göre, ülkelerin; %30’unda İnternet’e erişim hakkının yasal hükümlerce belirlendiği, %2’sinde ağ tarafsızlığını (net neutrality) garanti altına alan veya düzenleyen özel yasal hükümlerin bulunduğu, %12,5’inde İnternete erişimi kısıtlayan yasal hükümler bulunduğu, %80’inde ırkçı içerik veya söylem, yabancı düşmanlığı ve nefret dolu söylemlerin yasal düzenlemeler ile kontrol altına alındığı, %76’sında çocuk pornografisini suç unsuru sayan yasal hükümler

bulunduğu, %30’unda İnternet içeriklerinin veya web sayfalarının engellenmesi veya kapatılmasını sağlayan belirli yasal hükümler bulunduđu, %2’sinde Web 2.0 tabanlı uygulamalar ve hizmetler için erişim engelleme gerektiren belirli yasal hükümler bulunduđu, %44’ünde İSS’lar ve %7’sinde İnternet arama motorları veya içerik sağlayıcıları için özel yasal sorumluluk ve lisans zorunlulukları bulunduđu, %32’sinde uyar-kaldır ilkesine ilişkin yasal hükümler bulunduđu anlaşılmıştır (Akdeniz, 2011).

2.5.1.3 Avrupa Birliğı

368 milyon İnternet kullanıcısı ve %73’lük kullanıcı oranı ile dünyadaki İnternet kullanıcılarının %15’ini oluşturan AB, önemli İnternet aktörlerinden birisidir (internetworldstats, 2012c). AB, İnternetteki yasadışı ve zararlı içeriklerle mücadele konusunda aktif bir yaklaşım sergilemektedir (Çağlar, 2011: 117). Buna göre bir yandan üye ülkelere yol gösterecek çerçeve kurallar oluşturmaya çalışırken, diğer yandan İnternetin kendine özgü yapısını göz önünde bulundurarak esnek ve uygulanabilir içerik politikaları geliştirmeyi amaçlamaktadır.

2.5.1.3.1 Norm Oluşturma Çalışmaları: Kararlar, Tebliğler, Direktifler, Eylem Planları, Programlar

İnternette yer alan zararlı unsurlarla mücadele konusu AB’nin gündemine ilk olarak, 1990’lı yıllarda İnternernet üzerinden işlenen suçların hızla artması sonucu girmiştir. Zamanla önemini daha da artıran bu konuyla ilgili olarak AB, üye ülkeler için temel ilkeleri ortaya koymayı hedefleyen çerçeve normlar belirlenmeye çalışmış ve bazı kararlar almış; tebliğler, direktifler, eylem planları ve programlar yayınlanmıştır.

AB, İnternet gibi yeni gelişen teknolojileri ve bunların neden olduđu sorunları Avrupa Bilgi Toplumu kapsamında değerlendirmektedir (Kaya, 2010: 55). Birlik, Avrupa Bilgi Toplumu’nun esaslarını 1994’te Avrupa Komisyonu Eylem Planı’nda belirlemiştir (EU, 2011f). Planda, sakıncalı içeriğin İnternet ortamında yayılmasından dolayı çocukların korunmasının gerekliliğine ilişkin ilkeler yer almakla birlikte, konuyla ilgili kesin bir çözüm önerisi veya çözüme yönelik bir

yöntem belirlenmemiştir (Campbell and Machet, 1999:144). Çözümüne yönelik düzenleme esasları daha sonraki çalışmalarda ele alınmıştır.

2.5.1.3.1.1 “Haberleşmede Hukuka Aykırı ve Zararlı İçerik” ve “ Yeşil Kitap” Tebliğleri

AB’inde, İnternetin ortaya çıkardığı sorunlara yönelik çözüm bulma, yöntem geliştirme ve bu alanla ilgili düzenleme yapma gereksinimi, ilk olarak 24 Nisan 1996’da Bologna şehrinde yapılan İletişim ve Kültür Bakanları Gayriresmi Toplantısı’nda gündeme gelmiştir. Bu toplantıda, İnternetin yasadışı kullanımı ile mücadele etmek üzere, AB üyesi ülkelerin İletişim Bakanlıkları temsilcileriyle, erişim ve servis sağlayıcılar, içerik endüstrileri ve kullanıcı temsilcilerinden oluşan “Avrupa Komisyonu Çalışma Grubu”nun kurulması kararlaştırılmıştır (İçel vd., 2000: 117). Çalışma grubu hazırladığı raporu 1996 Kasım ayında kamuoyuna sunmuştur. Raporda, özellikle İnternet üzerindeki davranış kuralları ihlallerini belirlemek ve değerlendirmek üzere sektör ve kullanıcı temsilcilerinden oluşacak bir öz düzenleyici sistem kurulmasının gerekliliği dile getirilmiştir (ECHO, 1996).

AB tarafından yasadışı içeriğe karşı ilk genel inisiyatif,⁴³ 1996’da Maastricht Anlaşması’na dayandırılarak alınmıştır (Eur-lex, 1996). Buna göre ilk olarak 1996 Ekim’inde, Avrupa Komisyonu tarafından, bu alandaki ilk düzenlemelerden birisi olan COM(96)487 sayılı “Haberleşmede Hukuka Aykırı ve Zararlı İçerik” adlı tebliğ yayınlanmıştır (ISPO, 1996a). Bu Tebliğ’de, İnternetin geleneksel medya araçlarından farkına değinerek bu alandaki düzenlemenin zorluğuna dikkat çekilmekte ve İnternetin ortaya koyduğu olumsuzluklar şu başlıklarda değerlendirilmektedir: *Ulusal Güvenlik*: Terörist faaliyetler, terörizmle ilgili içeriklerin bulunduğu ulusal güvenlik açısından tehdit oluşturan siteler, *Küçüklerin Korunması*: Küçüklerin fiziki, ahlaki ve zihinsel gelişmelerini olumsuz etkileyen

⁴³ AB’nin çocuk pornografisine karşı harekete geçmesinde, 1996 yılında Belçika’da gerçekleştirilen ve dört küçük kız ile iki genç kadının tecavüz edilerek öldürüldüğü cinayetin etkili olduğu söylenilmektedir. Olayın AB’nin birçok temel kurumun yer aldığı Belçika’da gerçekleşmesi, Birlik’in çocukların istismarının önlenmesine yönelik girişimlerini artırmasına neden olmuştur. (Campbell and Machet, 1999: 140)

şiddet ve ahlaka aykırı içerikteki yayınlar, *İnsan Onurunun Korunması*: Belli bir ırk, millet veya cinsiyet ayrımı yapan içeriklerin barındırılması. Özellikle Yahudi karşıtı eylemler tanımlanmıştır, *Ekonomik Güvenlik*: Banka hesaplarına izinsiz girilerek işlem yapılması, kredi kartları bilgileri ile yapılan dolandırıcılık, *Gizliliğin Korunması*: Erişim noktalarına karşı yapılan zararlı eylemler (hacking). İnternette iletilen verilerin izinsiz olarak ele geçirmesi gibi eylemler, *Özel Hayatın Korunması*: Özel yaşamın gizliliğini ihlal eden içeriklerin yer aldığı yayınlar, *Kişiliğin Korunması*: Hakaret veya diğer kişiliğe zarar veren içerikler, *Telif Haklarının Korunması*: Fikri veya sınai haklar ile ilgili kanunlarla korunan eserlerin izinsiz olarak dağıtılması ve çoğaltılması (ISPO, 1996a). Daha sonra aynı yıl içinde, benzer bir muhtevaya sahip “Küçüklerin ve İnsan Onurunun Korunmasına İlişkin Yeşil Kitap” adıyla anılan başkaca bir tebliğ daha yayınlamıştır (ISPO, 1996b).

2.5.1.3.1.2 Yasadışı ve Zararlı İçeriklerle İlgili Hükümet Temsilcileri Kararı

26-27 Eylül 1996’da, Dublin’de yapılan Adalet Bakanları toplantısında Avrupa Komisyonu Çalışma Grubu’nun İnternet ve benzeri network ağlarının yasadışı kullanımı ile mücadele etmek üzere somut öneriler ve tedbirler üzerinde çalışmalar yapması karara bağlanmıştır (İçel vd., 2000: 118). Çalışma Grubu’nun Raporu doğrultusunda 17 Şubat 1997 tarihli “İnternette Yayınlanan Yasadışı Ve Zararlı İçeriklerle İlgili Üye Hükümet Temsilcileri ve Avrupa Konseyi Kararı”nda üye devletler aşağıda yer alan tedbirleri almaya çağırılmıştır (Eur-lex, 1997):

- İSS’ları ve kullanıcı temsilcilerinin de yer aldığı bir öz düzenleyici sistemi teşvik etmek. İnternetin diğer aktörleri ile birlikte işbirliği yapmak.
- Vatandaşlar için yardım hattı kurmak, etkin yönetim kuralları ve rapor verme mekanizmalarını, vatandaşlar için ulaşılabilir kılmak.
- Kullanıcılar için filtreleme ve derecelendirme sistemlerinin hazırlanması ve kurulmasını teşvik etmek.

AB Komisyonu’nun 1996 yılındaki çalışmalarına binaen Avrupa Parlamentosu (AP) 1997 Nisan ayında yasa dışı ve zararlı içeriklerin bloke edilmesinin teknik olarak

imkanı üzerine bir çalışmayı yayınlamıştır (EU, 1997). Bu çalışmaların akabinde çocukların cinsel sömürüsü ve çocuk pornografisi ile mücadele konulu 13 maddelik Çerçeve Karar (2004/68/JHA) 22.12.2003 tarihinde yayınlanmıştır (Eur-lex, 2003).

2006 yılı Mayıs ayında da AB, terörizmle mücadele konusunda bir Eylem Planı'nı revize ederek bu konuda devletlerarasında işbirliğinin artmasını ve İnternetin bu amaçla kullanımının önüne geçilmesini öngörmüştür. Bunlar dışında AB Konseyi, 28.11.2008 tarihinde, ırkçılık ve yabancı düşmanlığı ile mücadele konusunda bir Çerçeve Anlaşma oluşturmuştur. Bu çerçevede nefret, şiddet, soykırım suçlarının inkarı ve insanlık ve savaş suçlarıyla mücadele amaçlanmıştır (Eur-lex, 2008).

2.5.1.3.1.3 Güvenli İnternet Eylem Planları ve Programları

AB Komisyonu, 1998 yılında bağımsız düzenleme mekanizmasına ilişkin genel bir çerçeveyi içeren ve güvenli İnternet kullanımını destekleyen bir uygulama planı (İnternet Eylem Planı-Internet Action Plan) hazırlamış ve AP'nun 276/1999/EC numaralı kararı olarak kabul edilmiştir. 1.1.1999 ile 31.12.2002 arası dönemi kapsayan Plan, 25 milyon ECU bütçe ile İnternet ortamında işlenen suçlar ve İnternet kullanımında karşılaşılan olumsuzluklarla mücadeleyi, düzenleme gerektirmeyen inisiyatifleri destekleyerek gerçekleştirmeyi amaçlamıştır (EU, 1999).

Eylem Planında mücadele edilmesi gerekli görülen konular şöyle sıralanmıştır (EU, 1999): *Ulusal güvenlik* (bomba yapımını öğretme, yasa dışı ilaç üretimi, terörist faaliyetler), *Küçüklerin korunması* (şiddet ve porno), *İnsan onurunun korunması* (ırk nefretini teşvik, ırk ayrımcılığı), *Ekonomik güvenlik* (dolandırıcılık, kredi kartı korsanlığı), *Bilgi güvenliği* (kötü niyetli bilgisayar korsanlığı), *Mahremiyetin korunması* (kişisel verilere izinsiz erişim, elektronik taciz), *İtibarın korunması* (iftira), *Telif hakkı* (telif eserlerinin izinsiz dağıtım, örneğin; yazılım ya da müzik).

Eylem Planının 2. maddesi gereğince üye devletler, Avrupa genelinde daha güvenli bir İnternet kullanımı sağlamak ve İnternet endüstrisinin gelişimine uygun bir ortam hazırlamak amacıyla şu tedbirleri almakla sorumlu tutulmuştur: Yasa dışı ve zararlı içeriğe ilişkin bir Avrupa yardım hattı ağı kurulması, İnternet alanında öz denetim ile

çocuk pornografisi, etnik, din ve cinsiyet temelli nefret uyandıran içeriklere yönelik içerik izleme sistemlerini temin etmek, filtreleme ve içerik derecelendirme sistemlerinin kurulması, bilinçlendirme faaliyetlerine zemin hazırlama ve faaliyetleri teşvik etme, İnternetin güvenli kullanımına ilişkin yasal yaptırımların araştırılması, yapılacak düzenlemede uluslararası işbirliğinin teşvik edilmesi, benzer uluslararası girişimlerle koordinasyonu sağlama, birlik tedbirlerinin etkilerini değerlendirmek.

31.12.2002 tarihinde sona eren Eylem Planı'nın yerine 2002-2005 arası dönemi kapsayan yeni bir eylem planı hazırlanmıştır. Genişlemiş İnternet Eylem Planı (Safer Internet Action Plan Extension) olarak anılan bu Plan, AP'nun 1151/2003EC sayılı kararı ile işlerlik kazanmıştır. Önceki planın devamı niteliğinde olan bu planın kapsamına, aday ve katılım sürecinde olan ülkeler de alınmıştır (EU, 2011g).

Daha sonra 01.01.2005-31.12.2008 arasında geçerli olan ve 45 milyon Avro'luk bir bütçe öngören “Safer Internet Plus Programı”, AP'nun 854/2005/EC sayılı kararı ile yürürlüğe konulmuştur. Plan, kullanıcıların, özellikle çocukların, ailelerin ve bakıcıların eğitimi için İnternet ve diğer iletişim teknolojilerinin güvenli kullanımını desteklemekte ve bu amaçla halkın bilinçlenmesini sağlamayı ve zararlı içerikler ve yönlendirmelerle mücadele etmeyi hedeflemektedir (EU, 2011d).

Son olarak ise, “Safer Internet Programme”, 2009-2013 yılları arasında uygulanmak üzere AP'nun 1351/2008/EC sayılı kararı olarak kabul edilmiştir. “Daha Güvenli İnternet Programı” olarak da anılan ve 55 milyon €'luk bütçesi olan bu Program'ın önceki eylem planlarından ve programlardan fazlalığı, sadece yasadışı içerikle mücadeleyi değil, aynı zamanda suça özendirme ve siber saldırganlık gibi zararlı yönlendirmelerle mücadeleyi de hedeflemesidir. Ayrıca, online ortamın riskleriyle mücadele için ortak bir bilgi tabanı oluşturmayı da öngörmektedir (EU, 2011e).

2.5.1.3.1.4 İnternette İfade Özgürlüğü Konusunda AP Kararı

6 Temmuz 2006 tarihinde gerçekleşen, AP toplantısında İnternette ifade özgürlüğü konusu görüşülmüş ve şu tespitler yapılmıştır (EU, 2006):

- Günümüzde İnternet gibi yeni elektronik ortamlar büyük ölçüde ifade özgürlüğünün kullanımının yeni aracıdır.
- İnternet demokrasinin güçlenmesini sağlayabilecek bir unsurdur. Bu nedenle bazı erişimleri sınırlandırmanın ifade özgürlüğünü engelleyeceği görülmelidir.
- İnternet kullanımı ile ilgili sınırlandırmalar, sadece nefrete çağrı, şiddet ve ırkçılık, totaliter propagandalar, çocukların pornografiye erişimleri ya da cinsel istismarı gibi yasal olmayan eylemler için var olabilir.
- Sınır Tanımayan Gazeteciler Örgütü Raporu'na göre otoriter hükümetler ve rejimler İnterneti kontrol ve daha yakından takip etme yöntemleri geliştirmek için çalışmaktadır. Özellikle daha kompleks filtreleme teknolojileri ve siber-polis örgütleri ile elektronik iletişimi yakın gözetime almaktadırlar.
- Demokratik ülkelerin büyük bilişim şirketleri kısmen bu ülkelere elektronik gözetim ve web için sansür araçları sağlamaktadır. Örneğin Çin'e Yahoo, Google, Microsoft ve Cisco'nun teknik destek sağlaması gibi.

Bu tespitlerden sonra şu sayılanların yapılması önerilmiştir:

- Yeni teknolojik tartışmalara karşı daha dengeli, çoğulcu ve devletlerin temsilini içeren İnternet yönetişimi anlaşmalarının geliştirilmesi gerekmektedir.
- İster bilgi yaymak isterse bilgiye ulaşmak için olsun, ilgili hükümetlerce İnternet içeriği ile ilgili alınan ve ifade özgürlüğünü engelleyen sınırlandırmaların kaldırılması için önlemler alınmalıdır.
- Baskıcı ülkelerdeki şirketlerin eylemlerine sınırlandırmalar getirilerek gönüllü davranış kuralları oluşturulmasına çalışılmalıdır.
- Üçüncü dünya ülkelerine yardım programlarında gerektiğinde, ilgili ülkenin vatandaşlarına İnternet erişimlerini sınırlandırmasıyla ilgili bir kriter uygulanabilir.
- İnternette arama, sohbet, yayıncılık ya da diğer hizmetleri sağlayanların kullanıcı haklarına saygı göstermeleri gerekmektedir.

2.5.1.3.1.5 E-Ticaret Direktifi

AB, İnternet aktörlerinin sorumluluğunu 8 Haziran 2000 tarihli ve 2000/31/EC sayılı E-Ticaret Direktifi ile belirlemiştir. İnternet aktörlerinin “hizmet sunucusu” olarak belirtildiği Direktifte, hizmet sunucusu “bir bilgi toplumu hizmeti sunan her türlü gerçek ve tüzel kişi” olarak tanımlanmış ve erişim, yer ve içerik sağlama hizmetlerine göre sorumlulukları düzenlenmiştir (Eur-lex, 2000).

Direktifin 3. maddesine göre üye devletler, prensip olarak başka bir üye devletin sunduğu bilgi toplumu hizmetlerini kısıtlamayacaktır. Fakat, şu şartların oluşması halinde bu hizmetleri kısıtlayıcı önlemler alınabilecektir: Kamu politikası gereği olarak özellikle suçların önlenmesi, soruşturulması, yakalanması ve dava edilmesi nedenleriyle, küçüklerin korunması ve ırk, cinsiyet, din, milliyet temellerinde nefreti kışkırtacak her türlü faaliyete karşı mücadele amacıyla ve insan haysiyetine yönelik ihlallerin önlenmesi, kamu sağlığının korunması, ulusal güvenlik ve savunmanın güvence altına alınması da dahil olmak üzere, kamu güvenliği, yatırımcılar da dahil olmak üzere, tüketicilerin korunması (Akgün, 2002).

Direktifin 4. maddesinde İSS’ların hizmete başlamadan önce veya hizmetin icrası esnasında izin şartına bağlanamayacağı belirtilmiştir. Ancak bu düzenleme, 10 Aralık 1997 tarihli ve 97/13/EC sayılı telekomünikasyon hizmetleri alanında genel izinler ve bireysel lisanslar konusundaki AP ve Konsey Direktifindeki izin sistemlerine aykırılık oluşturmamaktadır.

Direktifin 5. maddesine göre üye devletler, İSS’lardan şu bilgilerin kolay, doğru ve sürekli olarak hizmet alıcılarına ve yetkili makamlara ulaştırılmasını temin eder: Hizmet sunucunun adı, adresi, iletişim bilgileri, ticari sicil veya sicil kayıt numarası, faaliyetin bir izin sistemine tabi olduğu durumlarda ilgili denetim makamına ilişkin hususlar, kayıtlı olduğu meslek örgütü veya benzeri kuruluş, mesleki unvan ve verildiği üye devlet, yerleşik bulunulan üye devlette uygulanan mesleki kurallara ve bunlara ne şekilde ulaşılabileceğine dair bir atıf (Eur-lex, 2000).

Direktif'in 12. maddesine göre İSS iletişimi kendisi başlatmamışsa, iletişimde yer alan karşı tarafı seçme yetkisi yoksa ve iletişime konu olan bilgiyi seçmiyorsa ve değiştiremiyorsa iletilen bilginin içeriğinden sorumlu olmayacaktır (Eur-lex, 2000).

Direktif'in 13. maddesinde İSS'ların bilgi iletişimini gerçekleştirmek üzere belirli şartlarda bilgiyi makul bir süre için otomatik olarak depolayabileceği düzenlenmiştir. Ancak, her iki maddede için de geçerli olmak üzere ilgili idari makam ya da mahkeme tarafından bu bilginin kaldırılmasına karar verilirse derhal kaldırılacağı veya bu bilgiye erişiminin engelleneceği belirtilmiştir (Eur-lex, 2000).

Direktifin 14. maddesi, yer sağlayıcılara, sadece İnternet erişimi, kaşeleme ve yer sağlama hizmetlerinin sunumu sırasında, yayınladıkları veya sakladıkları bilgiyi denetlemeleri veya yasadışı faaliyete işaret eden maddi olay ve şartları aktif olarak araştırmaları hususunda genel bir yükümlülük getirilemeyeceğini öngörmektedir. Ancak, yasadışı içerikten haberdar edilmesi veya fark etmesi halinde içeriğe erişimi engellemekle ve istenilen bilgileri iletmekle sorumludur (Eur-lex, 2000).

Direktifin 15. maddesine göre üye devletler, İnternet içeriğinde yer alan ulusal mevzuatlarında belirtilmiş olan kanun dışı faaliyet türleriyle ilgili materyalleri kaldırma veya erişimi engellemeye yönelik özel düzenlemeler yapma yetkisine sahiptirler. Buna göre, yetkili makam tarafından servis ve yer sağlayıcılara onlardan beklenen tedbirler çerçevesinde hareket etmeleri istenebilir ve hukuka aykırı içeriği bildirme veya saklama yükümlülüğü getirilebilir (Eur-lex, 2000).

Direktif'in 17. maddesi, ortaya çıkabilecek uyuşmazlıkların yargı dışı yollarla elektronik ortamda çözülmesi gerektiğini belirtmiştir. Üye devletlerden bu yöntemi zora sokabilecek tüm hukuki düzenlemelerin, uyuşmazlıkların çözümüne ilişkin yöntemlerin etkili şekilde kullanılmasını mümkün kılacak şekilde değiştirilmesini istemiştir (Eur-lex, 2000).

Böylece Direktif, yasadışı ve zararlı içeriklerle mücadele konusunda servis, yer ve içerik sağlayıcılara ilişkin genel anlamda sınırlı ve uyarı temelli bir sorumluluk

rejimi oluřtururken, 17 ve 14. maddesi ile “uyar-kaldır” tarzı, uyuřmazlıkların yargı dıřı yollarla çözümlmesine yönelik yöntemlere yer açmıřtır (Eur-lex, 2000).

2.5.1.3.2 İçerik Düzenleme Politikası

Görüldüğü gibi, AB, İnternet içeriğinin düzenlenmesi ve bu kapsamda hukuka aykırı ve zararlı içerikle mücadele konusunda aktif bir tavır geliřtirmektedir. Fakat AB, bu alanda tüm üye ülkeleri bağlayıcı bütünsel bir düzenleme yapmak yerine, önce bir takım normlar oluřturarak temel ilkeleri belirlemeyi ve bu ilkeler çerçevesinde üye ülkelerin ulusal mevzuatlarını geliřtirmelerini sağlamayı amaçlamaktadır. İçerik düzenlemesinin alanları, kapsamı ve yöntemi gibi hususlarda belirlenecek bu ilkeler ve ulusal tecrübeler çerçevesinde ortak bir anlayıř ve hareket birliğı geliřtirildikten sonra bütünsel düzenlemelere gidilmesine iliřkin adımlar atılması beklenebilir.

AB’nin bu yaklařım tarzının temelinde iki neden olduğı düşünölmektedir. İlk neden, İnternetin yeni ve geliřmekte olan kendine özgü evrensel bir sistem olmasının da etkisiyle üye ülkelerin İnternete farklı açılardan yaklařmasıdır. Bu nedenle, içerik düzenlemesinde hangi alanlarda ve hangi yöntemin kullanılması gerektiğı konusunda ortak sonuca ulařmadan tüm üye ülkeler için bağlayıcı yasal bir düzenlemenin yapılması doğru bulunmamaktadır. İkinci neden ise, AB’nin temel hak ve özgürlükler ve özellikle ifade hürriyeti konusunda elde edilen kazanımların zarar görebileceğı endiřesi taşımasıdır (Campbell and Machet, 1999: 141; Berber ve Kaya, 01.12.2010:4-5).

Nitekim bu nedenlerle, AB üyesi ülkelerin yasadıřı ve zararlı içerikle mücadeleye yönelik önlemlerin kapsamı, türleri ve yöntemleri konusunu düzenleyen mevzuat ve politikalarında bazı müřterekler bulunsa da önemli bazı farklılıklar da görölmektedir. Örneğın, AB üyesi Danimarka, Fransa, Finlandiya, İtalya, Hollanda ve İngiltere’de konuyla ilgili yasal düzenlemeler mevcutken; Avusturya, Belçika, Yunanistan, İrlanda ve İspanya gibi bazı ülkeler özel düzenlemelere gitmemiřlerdir (Bulut, 2009).

Fakat, bu durum, konuya iliřkin özel düzenleme bulunmayan AB ülkelerinde yasadıřı ve zararlı içerikle mücadele edilmediğı anlamına gelmemektedir. Bu

lkelerin oęu, “gerek hayatta su olan her Őey İnternette de sutur” anlayıŐıyla mevcut mevzuatı İnternete de uyarlayarak, zel yasal dzenlemeler yapmaksızın farklı yntem ve uygulama biimleriyle yine AB’nin belirledięi genel politikalar ve ilkeleri hayata geirmeye alıŐmaktadır (Campbell and Machet, 1999: 145).

Tm bu ekincelere ve ye lkelerde grlen farklılıkla raęmen, AB, yasadıŐı ve zararlı ierięe mdahalede belirli koŐullar altında ifade hrriyetini korumaktan daha baskın bir kamu yararı olduęunu kabul etmektedir (Campbell and Machet, 1999: 146). Buna gre AB, İnternet ortamındaki sakıncalı ierięi “yasadıŐı” ve “zararlı” ierik Őeklinde ikiye ayırmaktadır (EU, 1999). AB, ocuk pornografisi ve cinsel istismarı, ırkılık ve terr ieriklerini yasadıŐı olarak kabul ederek su kapsamına almakta ve cezai dzenleme yapılmasını istemektedir. Zararlı ierik ise, yayınlanması su olmamakla birlikte, 18 yaŐından kklerin pornografik veya Őiddet yer alan ierięe ulaŐmalarının engellenmesi gibi bazı kısıtlayıcı hkmler getirilmiŐ olan ierięi ifade etmektedir (Oęuz, 2008). AB, zararlı ieriklere iliŐkin mcadeleyi gerekli grmekle birlikte cezai bir dzenleme yapılmasını zorunlu kılmamıŐ; toplumlar arasındaki kltrel farklılıklar nedeniyle toplumsal aktrlerce yrtlmesini, bu alanda dzenleme ve kısıtlamaya gidilmeden, kklerin zararlı ierikten filtreleme veya kontrol gibi aralarla uzak tutulmasını tavsiye ederek, konuyu ye devletlerin inisiyatifine bırakmıŐtır (İnternet Kurulu, 2011).

Bu noktada son dnemde AB’nde ve ye lkelerde yetiŐkin pornografisi konusunda politika deęiŐiklięine gitme ynndeki bazı iŐaretlerden bahsetmek gerekmektedir. İlk olarak İzlanda’da baŐlayan ve daha sonra dięer ye lkelere yayılan ve en sonunda AB’nin karar organlarına taŐınan pornografinin zellikle kadınları “cinsel zne” olarak kullandıęı, cinsiyet ayrımcılıęını krkledięi ve kadına ynelik cinsel Őiddeti artırdıęı ynndeki tartıŐmalar, bu tr ieriklere karŐı tedbirler geliŐtirilmesini gndeme getirmiŐtir. Nitekim AP, ye lkelerin medya, İnternet ve reklam sektrnde zel denetim mekanizmaları oluŐturarak seks ve pornoyu yasaklamasını ngren bir Tasarı’yı tartıŐmaktadır. Hollandalı parlamenter Tamara Liotard’un Tasarısında medya, iletiŐim ve reklam sektrlerinde cinsiyete baęlı ayrımcılık yaŐandıęı ve kadınlara ‘cinsel zne’ olarak kullanıldıęı grŐne yer verilmekte ve

“her geçen gün daha da kabul gören bir unsur” haline gelen pornografinin bu konudaki olumsuz etkisine vurgu yapılmaktadır (Radikal, 11.03.2013).

AB yasadışı ve zararlı içeriklerle mücadelesini Safer Internet Programları ile yürütmektedir. Bu Programların ise iki ayağı vardır. Bunlar; güvenli İnternet kullanımı konusunda eğitim ve bilinçlendirmeye yönelik çalışmalar ile İnternet içerik ihbar merkezlerinin kurulması ve yaygınlaştırılmasıdır. Bunların yanında, yasa dışı ve zararlı İnternet içeriklerinden etkilenenler için yardım hatları kurulması da AB’nce teşvik edilmektedir (Bozkurt, 2012: 4).

AB’nin İnternet içerik düzenlemesi politikasında en çok öne çıkan konulardan birisi de “öz düzenleme” uygulamalarını teşvik etmesidir. Öz düzenleme ile, öncelikle yasadışı içeriğin yayınlanmasını önlemek; ikinci olarak ise, yayınlanan zararlı içeriğe çocukların filtreleme yazılımları gibi yöntemlerle ulaşmasını engellemek hedeflenmektedir (Berber ve Kaya, 01.12.2010). AB’nin içerik düzenlemesine ilişkin yayınladığı neredeyse tüm belgelerde “öz düzenleme” vurgusu göze çarpmaktadır. Bu çerçevede Birlik, söz konusu belgelerde en çok İSS’lerini yönlendirmek için kurallar geliştirilmesi, uygun derecelendirme ve filtreleme sistemleri ile ihbar merkezleri ve bilinçlendirme faaliyetlerini gerçekleştirecek ulusal öz düzenleme sistemleri kurulması konularını ele almakta ve üye devletleri bu konularda desteklemektedir. AB, Güvenli İnternet Programları ile bu nevi yapılacak faaliyetler için finansal yardım sağlamaktadır.

Benzer şekilde, e-Ticaret Direktifi ile uyuşmazlıkların yargı dışı yollarla çözülmesine yönelik “uyar-kaldır” tarzı yöntemlere imkan sağlanmış ve üye devletlerin İnternet sektörlerinin öz düzenleme çerçevesinde bunu sağlayacak mekanizmalar geliştirmeleri teşvik edilmiştir. Keza, Direktifte yasadışı içerik için genel anlamda sınırlı ve uyarı temelli bir sorumluluk getirilmiş, daha çok üye devletler ve Komisyon’un ilgili sektörler için geçerli olacak davranış kurallarının belirlenmesi ve teşvik edici rol oynaması istenmiştir (Akdeniz ve Altıparmak, 2008: 81).

Yasadışı veya zararlı içeriğin filtrelenmesi, AB için içerik düzenlemesine yönelik, öz düzenleme uygulamalarının önemli araçlarından birisidir. İçerik filtrelemeye ilişkin düzenleme esasları, tüm iletişim araçlarında insan haysiyetinin ve çocukların korunması amacıyla hazırlanan “Küçüklerin ve İnsan Onurunun Korunmasına İlişkin Yeşil Kitap” da yer almıştır (ISPO, 1996b). AB, PICS (İnternet İçerik Seçimi Platformu) standardı olarak bilenen ve İnternet ile ilgili temel politikaların belirlenmesine yardımcı olmak için oluşturulan World Wide Web Consortium tarafından belirlenen filtreleme sistemini kullanmaktadır (w3.org, 2011).

Küresel standartlar oluşturmak için sektördeki firmalara ait bir girişim olarak ortaya çıkan PICS, filtreleme standartları yanında İnternet derecelendirme çalışmaları da yapmaktadır. Etiketleme sistemiyle siteleri kategorilere ayrılmakta ve ebeveynlerin site erişimlerine ilişkin kararlarına kaynaklık etmektedir. PICS’in sınıflandırmaları, çıplaklık, cinsel içerik, şiddet vb. içerik değerlendirme boyutlu ya da işaretler (farklı abonelerin ilgi ve uğraşlarına göre içeriğin belirlenmesi) gibi farklı bilgi tiplerine dayanmaktadır. Dikkat çekici bir öz düzenleme örneği olan PICS, İnternet sitelerini düzenlemek ve İSS’ların müdahalesi olmaksızın içeriğin kontrol edilmesini sağlamak konusunda önemli bir işleve sahiptir (Bakırcı, 2009: 12; w3.org, 2011).

AB ölçeğinde önemli bir öz düzenleme uygulamasını da dijital oyun sektöründe görmekteyiz. AB üyesi devletlerin interaktif oyun üreticileri, gönüllü olarak bir araya gelerek kendi ülkelerinde kullandıkları oyun derecelendirme ve sınıflandırma sistemlerini PEGI (Pan-European Game Information/Pan-Avrupa Oyun Danışma Kurumu) adıyla tek bir çatı altında toplamışlardır (Güneş, 2012: 54). PEGI sisteminde, oyunlar şiddet, cinsellik, ayrımcılık, uyuşturucu madde, korku, kötü dil ve kumar gibi kriterlere göre sınıflandırılmaktadır. Avrupa’da yaygın bir şekilde kullanılmakta olan bu sistemi bazı devletler yasa ile ulusal mevzuatlarına almışlardır. PEGI sistemi, formatı veya oyun platformu ne olursa olsun Avrupa’daki sistemin standartlarına imza atan şirketlerce satılan veya dağıtımı yapılan bütün interaktif yazılımlara ve dijital oyunlara uygulanmaktadır (PEGI, 2012).

PEGI sistemi 1998’de kurulan Belçika merkezli ISFE’ye bağlıdır. ISFE, PEGI sisteminin yönetimini NICAM eliyle yürütmektedir (PEGI, 2012). NICAM ise, ürünlerin belirli yaş gruplarına uygun olup olmadığını anlamalarına yardımcı olmak için tüketicilere yönelik sınıflandırma rehberleri yayınlar, şikayetlerle ilgilenir, filmler, TV programları, dijital oyunlar ve video yayınları için açıklayıcı bilgiler hazırlar (Güneş, 2012: 55).

Bütçesi üye aidatları ile karşılanan PEGI’nin karar organı, anne ve babalar, psikolojik uzmanlar, basın uzmanı, gençleri koruma yasası ile ilgili bir hukuk uzmanı ve ISFE üyesinden oluşan Kurul’dur. PEGI tüzüğünün amacı küçükleri ve gençleri uygun olmayan yazılım ürünlerinden korumak ve bu yazılımların onlar için sorumluluk duygusuyla üretildiğini belgelemektir (PEGI, 2012).

AB’nin önemli öz düzenleme araçlarından birisi de ihbar merkezi uygulamasıdır. İnternet kullanıcılarının şikayetleri ile İnternet içeriğinin denetlenmesini ve böylece yasadışı ve zararlı içeriğin sunuculardan kaldırılmasını sağlayan öz düzenleme yaklaşımı olarak ihbar merkezi uygulaması, 1999 tarihli Eylem Planı çerçevesinde hem AB nezdinde hem de her bir ülkenin kendi bünyesinde faaliyete geçirilmiştir.

Keza, sırasıyla Hollanda, Norveç, Belçika, İngiltere, Avusturya, İrlanda, Finlandiya, İspanya ve Fransa’da kurulan ilk ihbar merkezlerinin bir araya gelmesiyle INHOPE, bir Hollanda şirketi olarak 1999’da Amsterdam’da kurulmuştur. İçerik ihbar merkezleri arasında koordinasyon sağlamak amacıyla bilgi ihbar merkezleri birliği olarak kurulan INHOPE bugün, 37 ülkede faaliyet gösteren 37’si tam, 6’sı izleme durumunda olmak üzere 43 üyesi bulunan bir organizasyona dönüşmüştür. INHOPE’un ABD ve AB ülkeleri başta olmak üzere Avrupa, Kuzey Amerika, Asya, Afrika ve Avustralya kıtalarından üyeleri bulunmaktadır (INHOPE, 2012a).

INHOPE, başta çocukların cinsel istismarı içerikleri olmak üzere, nefret ve şiddet içeriklerinin İnternette ayıklanması ve çocuklar ve gençlerin İnternetteki yasal olmayan zararlı içeriklerden korunmasını ve İnternet suçları ile ilgili yeni eğilimlerin önceden tespiti ve bunlara uygun çözümler üretilmesini amaçlamaktadır. Bu

çerçeve, dünyadaki tüm İnternet içerik ihbar merkezlerini desteklemekte ve bunlar arasında bilgi, tecrübe ve uzmanlık paylaşımı ve koordinasyon sağlamaktadır. Bu bağlamda, en iyi uygulamalar ve istatistiklerin paylaşılması, teknik destek ve eğitim gibi aktiviteler gerçekleştirmektedir (INHOPE, 2012b).

INHOPE beş kişilik bir yönetim kurulu bulunmaktadır. Ayrıca 2009 yılında bir danışma kurulu oluşturulmuştur ve bu kurul sürekli büyümektedir. Amacı INHOPE'un aktivitelerini desteklemek ve ona rehberlik etmek olan bu kurulda, Microsoft, Vodafone, News Corporation, AOL, GSMA, TeliaSonera, Telefonica gibi dünyaca ünlü teknoloji şirketlerinin temsilcileri ve Interpol temsilcisi bulunmaktadır. INHOPE ağırlıklı olarak AB Safer Internet Plus Program tarafından yapılan bağışlarla finanse edilmektedir. Ayrıca üyelerden de senelik olarak belli miktarda bir aidat toplanmaktadır. Örneğin, INHOPE 2009'da Safer Internet Plus Program'dan yaklaşık 550 bin Euro, üyelerinden 190 bin Euro ve diğer bağışlardan da 8 bin Euro gelir elde etmiştir (INHOPE, 2010: 22). INHOPE'nin 2011 yılı bütçesi 614.101 Euro, 2012 bütçesi ise 556.019 Euro olarak gerçekleşmiştir (INHOPE, 2012c: 31).

INHOPE üyeleri 2005-2010 yılları arasında her ay ortalama yaklaşık 60 bin ihbar almıştır. Bu ihbar içeriklerinin incelenmesi neticesinde %51'i yasadışı olarak tespit edilmiştir. Yasadışı olduğu tespit edilenlerin de %66'sı çocukların cinsel istismarı materyalleri, %18'i yetişkin pornosu ve %13'ü çocukları ilgilendiren diğer içerikler ile ilgilidir (INHOPE, 2012d). Yine, INHOPE üyeleri 2012'de toplam 1.059.758 ihbar almıştır (INHOPE, 2012c).

Keza, 2002 yılında Hollanda'da kurulan Siber Nefrete Karşı Uluslararası Birlik (INACH) de INHOPE gibi bir ihbar merkezleri birliğidir. INACH, İnternet ortamındaki nefret, ırkçılık, ayrımcılık içeriklerine ait ihbarları kabul etmektedir. Farklı ülkelerdeki 20 adet ayrımcılıkla mücadele merkezi INACH üyesidir. INHOPE üyelerinin bir kısmı aynı zamanda INACH üyesidir (INACH, 2012).

AB, 2011 yılı Şubat ayında, üye ülkelerden, çocukların cinsel istismarı içeriklerinin, içeriğin başka bir ülkede barındırılması nedeniyle kaldırılmadığı durumlarda

erişiminin engellenmesini isteyen bir yasa değişikliği teklifini tartışmaya açmasını istemiştir. Bu değişiklik yasalaştığında uygulamanın gönüllülük esasına göre olmayacağı ve düzenlemenin zorunlu olarak uygulanacağı teklifte özellikle belirtilmiştir. Teklif ayrıca çevrimiçi grooming fiilini AB ülkelerinin tümünde bir suç olarak tanımlamaktadır. Teklif alt komisyondan oybirliği ile geçmiştir. Yasalaşması beklenen Teklif'in, yasalaşmasından sonra 2 yıl içinde üye ülkelerin konu ile ilgili kendi yasal düzenlemelerini yapmaları gerekecektir (Spletno, 2012).

AB'nin öz düzenleme bağlamında önem verdiği ve teşvik ettiği bir diğer konu da bilinçlendirme faaliyetleridir. Birlik, Güvenli İnternet Programı çerçevesinde, başta aileler ve çocuklar olmak üzere kullanıcıların, İnterneti doğru, etkin ve güvenli kullanmalarına yönelik bilinçlendirilme faaliyetlerini desteklenmektedir (Bayzan, 2011: 77-79). Bu amaçla, özellikle gençler ve aileler arasında farkındalık oluşturmak, gelişen trendleri izlemek ve güvenli İnternet kullanımı standartlarını arttırmak amacıyla INSAFE isimli bir merkez kurmuştur. Bu merkez, üye ülkelerin bu konularla ilgili örgütleri ile işbirliği ve koordinasyon sağlayarak "Güvenli İnternet Günü" gibi etkinliklerle İnternet kullanımıyla ilgili bilinç düzeyini arttırmayı hedeflemekte, zararlı ve yasadışı içeriklerin bildirilmesini sağlamaya yönelik çalışmalar yürütmektedir (Safer İnternet, 2012).

Yine, öz düzenleme yöntemi ile devlet müdahalesinin asgariye indirilmesinde bir araç olarak kullanılan ve günümüzde içerik düzenlemesi konusunda yeni bir trend olarak karşımıza çıkan, sektörde yer alan önemli şirketler ile özel anlaşmalar yaparak yasadışı ve zararlı içerikle mücadele etmeyi öngören bazı uygulamalar AB'nce de gerçekleştirilmektedir. Daha önce bahsi geçen, Avrupa Komisyonu ile Avrupa mobil pazarındaki 91 mobil servis sağlayıcısı arasında 2007 yılında gönüllü olarak imzalanan "Çocukların ve Gençlerin Güvenli Mobil Kullanımına İlişkin Avrupa Çerçeve Anlaşması", Komisyon'la Dünyanın önde gelen 17 sosyal paylaşım sitesinin 2009 tarihinde imzaladıkları "AB İçin Güvenli Sosyal Ağlar Prensipleri" metni ve

2011’de Komisyon’un sektör lideri 28 şirketle İnternetin güvenli kullanımı kapsamında mutabık kaldığı eylem planı bunlardandır.⁴⁴

Diğer yandan, AB’nin öz düzenleme uygulamalarının her zaman “gönüllülük” esaslı yürütülmediği görülmektedir. Çoğunlukla hükümetlerin, sektör temsilcilerini, içerik düzenlemeleri ile ilgili “zorunlu gönüllü” işbirliği yapma konusunda yasama yapmaksızın oluşturdukları baskılar ile zorladıkları; hükümet temsilcilerinin, “gönüllülük” esaslı tesis edilemediği takdirde başka yaptırımların uygulanacağına yönelik beyanları doğrultusunda, İSS’ların gerekli tedbirleri “zorunlu gönüllü” olarak uygulamakta oldukları belirtilmektedir (Bayzan, 2011: 72-74).

AB’de İSS’lara, yasadışı içeriğin bildirilmesi halinde yayından kaldırılması sorumluluğu getirilmesinin bu durumun ortaya çıkmasına neden olduğu; farklı yaptırımlarla karşılaşmak istemeyen İSS’ların gönderilen kara listelere erişimi engellemekte oldukları dile getirilmektedir (Nebil, 2009). Böylece, birçok AB ülkesinde farklı şekillerde ve genellikle şeffaf olmayan yöntemlerle, mahkeme kararı olmaksızın, idari birimler tarafından oluşturulan gizli kara listelerin erişim sağlayıcılara gönderilmesiyle erişim engellemelerinin gerçekleştirildiği belirtilmektedir (Berber ve Kaya, 01.12.2010: 8).

Nitekim, bu duruma ilişkin bazı somut örnekler gösterilmektedir. Örneğin, İngiltere’de çocuk pornografisi ve ırkçılıkla mücadele etmek amacıyla bir STK olarak kurulan IWF’un üst düzey yöneticilerini emekli emniyet mensupları oluştururken, bünyesinde hiçbir hukukçu barındırmamasına rağmen oluşturduğu kara listeler, ülkedeki tüm erişim sağlayıcılar tarafından “gönüllü” olarak kullanılmaktadır (Nebil, 2009; TİB, 2008). Benzer şekilde Danimarka, İsveç ve Norveç’te İSS’lar, Polis teşkilatlarının sağlamış oldukları kara listelere erişimi engellemektedir. Keza, Almanya’da Federal Hükümet, İSS’lara pornografi, şiddet ve neo-Nazi aktivitelerine yönelik yasadışı web sitelerini içeren kara liste sağlamaktadır (Nebil, 2009).

⁴⁴ Bkz. “Özel Anlaşmalar yapma” maddesi.

Benzer şekilde, Finlandiya’da 2006’da kabul edilen, çocuk pornografisinin dağıtımını önlemeye yönelik bir kanun ile, ülkede uluslararası ve organize suçla mücadele birimi olarak faaliyet gösteren Ulusal Araştırma Bürosu, yabancı sitelerden oluşan gizli bir kara liste oluşturma konusunda yetkilendirilmiştir. Belirli aralıklarla güncellenen bu kara listedeki siteler ülkedeki İSS’larca gönüllü olarak alan adı engelleme yöntemi ile erişime kapatılmaktadır. Finlandiya’da yoğun tartışmalara neden olan ve Anayasa’ya aykırılığı ileri sürülen bu Yasa’nın daha hazırlık aşamasında taslak halindeyken, Hükümetçe İSS’lara baskı yapıldığı ve filtreleme işlemini gönüllü olarak yapmadıkları takdirde, sansürün zorunlu olarak uygulanacağını ima edildiği dile getirilmiştir (Puolamäki, 2008).

Yine, İSS’lar üzerinde oluşturulan baskı nedeniyle birçok firmanın yaptırımlardan etkilenmemek amacıyla hükümetlerin hassas olduğu konularda otomatik filtreleme gerçekleştirmek ve müşterilerini belirlerken seçici davranmak suretiyle otosansür uyguladığı görülmektedir. Örneğin, Fransa’da sözde Ermeni Soykırımı Yasası yürürlüğe girdikten sonra başta OVH firması olmak üzere ülkedeki birçok ISS, Türkçe içerikli web sitelerini barındırma sözleşmelerini iptal etmiştir (Çamlı, 2010a).

Ayrıca, AB’de suçluları takip etmek ve ceza soruşturmalarında suçu delillendirme amacıyla İSS’lara 6 aydan az ve 2 yıldan çok olmamak üzere İnternet trafik verilerini saklama zorunluluğu getiren uygulamanın daha çok istihbarat amacıyla kullanıldığı ifade edilmektedir (Berber ve Kaya, 01.12.2010:9). Nitekim, 2007’de İsveç hükümeti, merkezi istihbarat birimine, herhangi bir mahkeme kararı olmaksızın tüm İnternet trafiğini ve e-mail yazışmalarını takip etme yetkisi vermiştir. 2009 yılında bu yetki tüm dünyadaki İnternet ağında kelime temelli arama yapılmasını ve yazışmaların takip edilmesini sağlayacak şekilde genişletilmiştir (Berber ve Kaya, 01.12.2010:8-9).

Bu ve benzeri uygulamalar, AB’nde her devletin kendi iç dinamiklerine göre İnternet içeriğine Türkiye’den daha fazla müdahale etmesine rağmen sanki “Avrupa’da İnternete müdahale edilmeyormuş” gibi bir yanılgı olduğu görülmektedir. Nitekim, bu durum bazı AB üyesi ülkelerin ulusal güvenlik, kamu yararı gibi muğlak gerekçelerle müdahale alanını geniş tutarken, bazılarının ise müdahale yetkisini

tamamen idari kurumlara bıraktığı eleştirilerini güçlendirmektedir (Korkmaz, 2010). Keza, en temel sorunun ise şeffaflık olduğu; Avrupa'nın içerik politikalarının Türkiye'deki gibi seffaf olmadığı, gizli politikalarla İnternet içeriğine müdahale edildiği, İSS'lar ve bilişim şirketleri üzerine baskı yapılarak gerçekleştirilmesi sebebiyle devletlerin doğrudan tepkilere maruz kalmadıkları ve böylece sorumluluktan kurtuldukları dile getirilmektedir (Berber ve Kaya, 01.12.2010: 9).

Sonuç olarak, AB'nde, İnternet düzenlemeleri ile ilgili bir takım ilkesel kurallar belirlenmiş olmakla birlikte tüm üye ülkeleri bağlayıcı genel/ortak bir düzenlemenin olmadığı söylenebilir. Birlik, yasadışı ve zararlı içeriğe karşı genel düzenlemeler yapmak yerine, genelde üye ülkeler arasında işbirliğinin artırılmasını amaçlamakta, bilinçlendirme, ihbar mekanizmaları kurma, özel anlaşmalar yapma gibi öz düzenleme uygulamalarının yaygınlaştırılması ve filtreleme sistemlerinin kullanılmasının teşvik edilmesini politika olarak benimsemiş gözükmektedir.

Üye ülkeler arasında çocuk pornografisi, terörizm, ırkçılık ve telif hakları gibi içerik türlerine karşı önlem alınması ve mücadele edilmesi ve suç oluşturan içeriğe erişimin engellenmesi konusunda ortak bir görüş bulunsa da, suç oluşturan içeriklerin kriterleri, kimin hangi hukuki esasa göre ve ne ölçüde sorumlu tutulacağı hususlarına ilişkin yaklaşım, hukuki düzenleme ve uygulama farklılıkları bulunmaktadır. Diğer yandan, uygulamada yasadışı ve zararlı içerikle mücadelenin sektördeki şirketlerce “zorunlu gönüllü” olarak STK'lar ve güvenlik güçleri ile işbirliği içerisinde yürütüldüğü de görülmektedir.

AB içerik düzenlemesi uygulamalarında göze çarpan bu “zorunlu gönüllülük” gerçeği, AB'nin konuya ilişkin genel yönetsel yaklaşımının öz düzenleme yönünde olduğu şeklindeki görüşü zayıflatmaktadır. Belki şekilsel olarak öz düzenlemeye uygun bir yapı var gibi gözükse de, arka planda kamu kurumlarının doğrudan veya dolaylı olarak etki ve yönlendirmede bulundukları, hatta ince yollu tehditlerle istikamet belirledikleri bu tür yapıların öz düzenleme ilkelerine ve öz düzenleme yaklaşımının ruhuna uygun düşmeyeceğini söylemek mümkündür. İçerik düzenlemeleriyle ilgili temel yönetsel yaklaşımların özellikleriyle AB

uygulamaları karşılaştırıldığında, iddia edilenin aksine, AB'nin yaklaşımının “öz düzenleme”den çok “birlikte düzenleme” yaklaşımına yakın olduğu görülmektedir.

Nitekim, uygulamalarda örnekleri görüldüğü gibi, AB içerik düzenlemelerinde sektördeki şirketlerle birlikte STK ve özellikle güvenlik güçleri arasında yakın bir işbirliği söz konusudur. Genel çerçevenin belirlenmesi ve yönlendirme anlamında AB ve üye devletlerin ciddi etkileri bulunmaktadır. Dolayısıyla böyle bir yapıda öz düzenlemeden çok birlikte düzenleme yaklaşımından bahsedilmelidir. Buradan hareketle AB'nin içerik düzenlemesiyle ilgili genel yaklaşımının bilgi toplumunun popüler yönetim modeli olan “yönetişim” merkezli olduğu söylenebilir. İnternet içerik düzenlemesi konusunun tarafları ve paydaşları olan tüm aktörlerin devlet ile birlikte konunun yönetiminde ve uygulamalarında söz sahibi olmaları, AB'nin ve üye ülkelerin önem verdikleri bir tercih olarak görülebilir.

2.5.2 Devletler

İnternet içeriğinin düzenlenmesi konusunda ülke uygulamaları büyük bir çeşitlilik ortaya koymaktadır. Yasadışı ve zararlı içerikle mücadele etme konusunda içeriğin türleri, kapsamı, yöntemi, yönetimi, kriterleri gibi hususlarda farklı yaklaşımlar ve uygulamalar göze çarpmaktadır.

2.5.2.1 Amerika Birleşik Devletleri

İnterneti icat eden, geliştiren, yöneten ve dünyaya yayılmasına öncülük eden ABD, %78'lik kullanım oranı ve 245 milyon kullanıcı ile dünyanın en büyük İnternet aktörüdür (internetworldstats, 2012d). ABD için İnternet bugün de ulusal güvenliğinin önemli bir parçası olmaya devam etmektedir. Bu nedenle İnterneti geliştiren ülke olarak ICANN ve IANA gibi kurumların üzerindeki etkisini koruyarak İnternet politikalarının belirlenmesinde söz sahibi olmayı sürdürmektedir (Kaya, 2010: 48). Diğer yandan, içerik düzenlenmesi konusundaki kendine özgü uygulamalarıyla dikkat çekmektedir.

2.5.2.1.1 Yasal Çerçeve

ABD, İnternetin mucidi olduğu için; doğal olarak en uzun süredir kullanan ve bu nedenle İnternet suçlarının ilk ortaya çıktığı ve bu suçların düzenlenmesine de ilk olarak ihtiyaç duyan ve bunu ilk gerçekleştiren ülke olmuştur (Dülger, 2004: 91). Nitekim, tarihsel süreç içerisinde, ABD’de, eyaletlerde Anayasal sınırlar içinde farklı düzenlemelere rastlanıldığı gibi, ülke düzeyinde bir İnternet politikası belirlemek ve İnternet içeriğini kontrol etmek için genel düzenlemeler de yapılmıştır.

2.5.2.1.1.1 Müstehcen İçerikle Mücadele Yasaları

Ülkede İnternet içeriğine müdahale konusunun odak noktasını müstehcen içerik oluşturmaktadır. Görsel ve işitsel araçların yaygınlaşmaya başladığı 1960’lı yıllardan itibaren müstehcen materyallerin sınırlanması sorunu ABD’de önemli bir tartışma konusu olmuştur. Fakat 1996 yılına kadar ülkede müstehcen içeriğe müdahale edilmesine ilişkin yasal bir düzenleme yapılmamış ve yargı içtihatları ile ihtilaflar giderilmeye çalışılmıştır (Kaya, 2010: 48).

ABD’de müstehcenliğe ilişkin temel içtihadı, Amerikan Yüksek Temyiz Mahkemesi (The US Supreme Court)’nin 1973 yılında verdiği Miller v. California isimli karar oluşturmaktadır.⁴⁵ Yargılamada, müstehcen içerikli ürünlerin iletimi ifade hürriyeti kapsamında tartışılmış ve Mahkeme müstehcenliğin ölçütlerine dair içtihatla bulunmuştur. Buna göre, müstehcenliğin tespit edilebilmesi için üç aşamalı bir testin yapılması öngörülmüştür (Kaya, 2010: 48). İlk olarak, ortalama çağdaş ahlak anlayışına sahip sıradan bir kişinin o içeriğe karşı bütünsel olarak şehvi ilgi duyup duymadığı tespit edilecektir. İkinci olarak, içeriğin yürürlükteki kanunlarda tanımlanan cinsel hareketleri açıkça saldırgan ve/veya iğrenç bir şekilde tanımlayıp tanımlamadığı veya tasvir edip etmediği tespit edilecektir. Son olarak ise, içeriğin bir bütün olarak edebi, sanatsal, siyasi veya bilimsel bir değerinin olup olmadığına karar verilecektir. Bu aşamalardan herhangi birini geçemeyen içerik müstehcen kabul

⁴⁵ Miller’in, toplu elektronik posta göndererek cinsel içerikli ürünlerin tanıtımını yapması, müstehcen içeriğin yayılmasını yasaklayan Kaliforniya kanunlarına aykırılık teşkil ettiği gerekçesiyle aleyhine ceza davası açılmasına neden olmuştur. (Findlaw, 2011).

edilerek ifade hürriyeti kapsamında görülmeyecek ve korunmayacaktır. Mahkemenin bu içtihadına rağmen tartışmalar ilerleyen zamanlarda da devam etmiştir.⁴⁶

2.5.2.1.1.1.1 İletişim Ahlakı Yasası

1990'lı yılların başlarından itibaren İnternet kullanımının büyük bir hızla yaygınlaşmasıyla İnternet üzerindeki yasadışı ve zararlı içeriğe sahip yayınlarda ve özellikle müstehcen nitelikteki site ve haber gruplarında da büyük bir artış yaşanmıştır. Bu tür içeriklerin çocukların da içinde bulunduğu her yaştan insan için kolayca erişilebilir olması ve daha da önemlisi, içerisinde küçük çocukların kullanıldığı resim, fotoğraf, videoklip vb. materyallerin bulunduğu pedofili sitelerin İnternet üzerinde faaliyet göstermeye başlamaları, ABD kamuoyunda infiale neden olmuştur. Bu infialin sonucunda, diğer kitle iletişim araçlarında yasak olan bu tip faaliyetlerin, İnternet üzerinde de yasaklanması amacıyla, siyasi otorite üzerinde büyük bir baskı oluşturulmuştur (Sınar, 2001: 92).

Bunun üzerine Hükümet, hem müstehcenliğe ilişkin sınırlamaları yasal bir zemine kavuşturmak hem de özellikle çocukların müstehcen içerikten etkin bir şekilde korumasını sağlamak amacıyla 1996 yılında CDA (İletişim Ahlakı Yasası) isimli yasayı çıkarmıştır (GPO, 1996). Bu Yasa, dünya üzerinde İnternetin ortaya çıkardığı sorunların çözümüne yönelik yapılan ilk hukuki düzenlemelerden birisidir ve getirmiş olduğu hükümler bakımından tarihi bir öneme sahiptir(Sınar, 2001:92-93).

CDA, İnternet üzerinden müstehcenlik ve şiddet içeren materyallerin yayınlanması ve iletilmesini suç olarak düzenlenmekte ve yayını sunan süjelere 2 yıla kadar hapis ile 250.000 \$'a kadar para cezası öngörmektedir (Sınar, 2001: 93). Yasa'nın 223. maddesi, müstehcen veya açık bir şekilde zararlı kabul edilen içeriğin 18 yaşından küçüklere iletilmesini veya bilinçli olarak bu tür içeriğin çocuklar tarafından erişilebilir şekilde sunulmasını yasaklamaktadır. Yasa bu çerçevede İnternet aktörlerine bir takım sorumluluklar yüklemiş ve kredi kartları veya benzeri

⁴⁶ Amerika Yüksek Mahkemesi Yargıcı Potter Stewart müstehcenliğe ilişkin vermiş olduğu bir kararda müstehcenliğin ne kadar göreceli ve yoruma açık olduğunu "onu tanımlayamam, fakat gördüğüm zaman tanıyabilirim" şeklinde tarifiyle anlatmaya çalışmıştır. (UMKC, 2011)

teknolojiler kullanılarak yaş doğrulamasının yapılmasını ve içerik sağlayıcıların çocukları bu tür içeriklerden korumak için gerekli tüm tedbirleri almalarını zorunlu kılmıştır. Düzenlemenin 230. maddesine göre ise, yayınlanan içerikten içerik sağlayıcılar sorumlu tutulmuş ve İSS'lara gereken özeni göstermeleri şartıyla yayınladıkları içerikten sorumluluk yüklenmemiştir (Kaya, 2010: 49). Ayrıca, Yasa'nın uygulanabilmesi için yetkili mercilere, İnternet kullanıcılarının elektronik posta mesajlarının okunabilmesi ve haber gruplarındaki tartışmalar ile yapılan sohbetlerin izlenebilmesi olanağı da sağlanmıştır (Sınar, 2001: 93).

Ancak bu düzenleme yürürlüğe girdikten sonra içerdiği hükümler bakımından kamuoyunda büyük tartışmalara sebep olmuş ve aleyhinde birçok STK kampanyalar düzenlenmiştir. Sonuçta ACLU (Amerikan Temel Özgürlükler Birliği) önderliğindeki STK'lar Yasa'nın ifade özgürlüğünü kısıtladığı iddiasıyla dava açmıştır (Dülger, 2004: 92). Davanın sonunda CDA, yürürlüğe girmesinden bir yıl sonra, Yüksek Temyiz Mahkemesi tarafından Anayasal güvence altında bulunan ifade hürriyetini ihlal ettiği gerekçesiyle iptal edilmiştir.⁴⁷ Kararın gerekçesinde demokratik bir toplumda özgür fikir alışverişinin sağlayacağı toplumsal yararın, İnternette sansürün sağlayabileceği toplumsal yararlarla karşılaştırılamayacak kadar önemli olduğu savunulmuş ve yasadışı içerikli yayınlarla mücadele edebilme çabasının, iletişim ve ifade özgürlüğünün ihlal edilmesinin gerekçesi olamayacağına vurgu yapılmıştır (Sınar, 2001: 93).

Mahkeme, CDA ile yasaklanan müstehcenlik fiilinin tanımını muğlak bulduğu gibi, sakıncalı içeriğin çocuklar tarafından erişilebilir şekilde sunulmasının yasaklamasını kanunun uygulama alanını belirsiz hale getirdiğine hükmetmiştir. Kararın gerekçesinde, İnternetin teknik olarak bu tür denetime imkan vermediğine; bir web sitesini ziyaret eden İnternet kullanıcısının gerçek yaşını kesin olarak tespit etmenin mümkün olmayacağına, yaş doğrulaması gibi sistemlerin yanlış bilgiler verilmek

⁴⁷ Karar için bkz. <http://www.law.cornell.edu/supct/html/96-511.ZS.html>; CDA'nın iptaliyle ilgili tartışmalar için bkz. **The Battle for the Communications Decency Act 1996 is over**, <http://www.cyber-rights.org/battle.htm>; **Internet Censorship: Law & policy around the world**, <http://www.efa.org.au/Issues/Censor/cens3.html> (21.11.2011)

suretiyle kolayca aşılabildiğine dikkat çekilmiştir. Bu nedenle, yetişkinler için hizmet veren bir web sitesine sadece bir çocuğun erişmesiyle tüm içeriğin yasadışı hale geleceği belirtilerek, düzenlemenin hukuka aykırılığına hükmedilmiştir (Kaya, 2010: 50-51).

Ayrıca, kararın gerekçesinden, hakimlerin kararlarını İnternetin yakınlık-uzaklık kavramlarını ortadan kaldıran kendine özgü niteliğini gözönünde bulundurarak verdikleri anlaşılmaktadır. Hakimler, müstehcen yayın yapan sinemaların ancak yerleşim yerlerinin uzağında yayın yapmalarına izin verilmesini öngören düzenlemelerden esinlenerek oluşturulan Yasa'daki bir hükmün, mevcut teknolojik düzey sebebiyle İnternet ortamında birebir uygulanamayacağına karar vermiş ve İnternetin yetişkinler için özel bir alan yaratmaya elverişli olmadığı belirtilmiştir (Kaya, 2010: 50).

2.5.2.1.1.1.2 Çocukların Online Yayınlardan Korunması Yasası

CDA'den sonra İnternet üzerindeki çocuk pornografisinin önlenmesine özgülenmiş bir yasa olan 1998 tarihli COPA (Çocukların Online Yayınlardan Korunması Yasası) yürürlüğe girmiştir (GPO, 1998). Yasa özellikle İnternet üzerindeki çocuk pornografisi ticaretinin önüne geçmeyi amaçlamıştır (Sınar, 2001: 95). 22 Haziran 2000 tarihinde Yüksek Temyiz Mahkemesi, ACLU ve 17 STK'nın açtığı bir davada, yapmış olduğu inceleme sonucunda COPA'nın CDA'ya göre daha makul bir sınırlama getirdiği gerekçesiyle kanunu iptal etmemiştir (Vill, 2000).

COPA, çocukların kullanıldığı pornografik materyalleri bulunduran ve teşhir eden ticari seks siteleri açan kişilere 2 yıla kadar hapis ve 150 bin \$'a kadar para cezası getirmiştir (Sınar, 2001: 95). Yasa'nın 103. maddesiyle, çocukların müstehcenlik gibi zararlı İnternet içeriğinden korunması amacıyla, İnternete yoğunlukla erişim sağlanan kütüphaneler ve devlet okullarında filtreleme yazılımlarını kullanma zorunluluğu getirilmiştir. COPA, müstehcenlik konusunda Miller kararındaki ölçütlerin esas alınmasını benimsemiştir. Ayrıca, 231. madde ile içerik sağlayıcılara, çocuklara zararlı içeriği sağlamaktan dolayı sorumlu tutulmamaları için kredi kartı,

kimlik kartı veya mevcut teknolojilere göre kullanılması makul kabul edilebilecek herhangi bir tekniği kullanmasını zorunlu kılmıştır (Kaya, 2010: 50-52).

Yüksek Temyiz Mahkemesi'nin 2000 yılındaki kararına rağmen COPA'nın ifade hürriyetini ihlal ettiğine yönelik tartışmalar devam etmiş ve konu 2009 yılında tekrar Temyiz Mahkemesi'nin önüne getirilmiştir. Mahkeme yürürlük dönemindeki uygulamalarını da göz önüne alarak, ifade hürriyetini ihlal ettiği gerekçesiyle COPA'yı Anayasaya aykırı bularak iptaline hükmetmiştir (Kaya, 2010: 52).

2.5.2.1.1.3 Çocukları İnternette Koruma Kanunu

COPA sonrasında zararlı İnternet içeriğinden çocukların korunması amacıyla 2001'de yürürlüğe konulan CIPA (Çocukları İnternette Koruma Kanunu) (FCC, 2001), daha “yumuşak” bir düzenlemeyi içermektedir Çağlar, ö2011: 116). Diğer iki yasanın aksine CIPA, çocukların korunması amacıyla kütüphaneler ve devlet okullarının filtreleme yazılımlarını kullanmalarını zorunlu tutma ve çocukların İnterneti bilinçli kullanmaları için gerekli bilgilendirmelerin yapılmasını talep etme ile sınırlı bir uygulama alanını düzenlemiştir. Kütüphaneler ve devlet okullarının filtreleme yazılımını kullanmamalarının yaptırımı ise, sadece federal yardımlarından kesintiye gidilmesi olarak belirlenmiştir. ABD Kütüphaneler Birliği, CIPA'yı Anayasa'nın 1. maddesine aykırılık iddiasıyla Yüksek Mahkeme'ye götürmüş fakat Mahkeme bu iddiayı 23.06.2003 tarihli kararı ile reddederek Yasa'yı desteklemiştir (Wikipedia, 2011b). Tüm eleştirilere rağmen CIPA yürürlüğünü sürdürmektedir.

Çocukların korunması amacıyla İnternet içeriğine müdahale etmek için dayanak oluşturan diğer bir düzenleme ise, ABD Ceza ve Ceza Usul Kanunu'nun çocukların istismarının önlenmesine ilişkin 2256 Nolu maddesidir (Oneckle, 2011). Bu hükme dayanılarak, içerik sağlayıcıların en azından müstehcen içeriğe ilişkin yaş doğrulaması gibi sistemleri kullanması zorunlu kılınmaktadır (Kaya, 2010: 52).

2.5.2.1.1.2 Çocuk Pornografisi ve İstismarına İlişkin Yasalar

ABD'nin İnternet içeriğine müdahale konusundaki bir diğer gerekçesini ise çocuk pornografisi oluşturmaktadır. ABD, BM Çocuk Haklarına Dair Sözleşme gibi çocukların istismarının önlenmesine ilişkin temel uluslararası sözleşmelere taraftır. ABD'de birçok eyalette çocukların seks amaçlı görüntülerinin oluşturulması, bulundurulması veya dağıtılması yasaktır.

Bu kapsamda, 1977 yılında yürürlüğe giren Çocukların Cinsel İstismarı Yasası (Sexual Exploitation of Children), pornografik görüntülerde çocuk kullanımını, çocukların pornografik fotoğraflarının alınmasını, çocuk pornosunun reklamını yapan materyallerin üretimini ve dağıtımını yasaklamaktadır (Goldenessays, 2011). 1984 tarihli Çocuk Koruma Yasası (Child Protection Act), 18 yaşından küçükleri çocuk olarak tanımlamakta ve bu nedenle 17 yaş veya altında olan bir kişinin seks amaçlı belirgin fotoğrafları çocuk pornografisi olarak kabul edilmektedir (Goldenessays, 2011). 18 Kasım 1988'de yürürlüğe giren Çocuk Koruma ve Müstehcenliği Uygulama Kanunu (Child Protection and Obscenity Enforcement Act) ise, çocuk pornografisinde kullanılmak üzere çocuğun transferi, satışı ve satın alınması yanında, çocuk pornografisi materyallerinin eyaletler arası elektronik posta ya da bilgisayarla taşınması ve ticaretini de yasaklamıştır (Goldenessays, 2011).

30.09.1996 tarihli Çocuk Pornografisinin Önlenmesi Yasası ile ABD Temel Yasası'nda değişiklik yaparak çocukların görüntülediği pornoğrafik yayın ve materyallerin elde bulundurulması, İnternet üzerinden ticaretinin yapılması veya İnternette yayınlanması yasaklanmıştır. Yasa'da aynı yıl yapılan bir değişiklikle "bilgisayar yoluyla oluşturulan çocuk pornografisi görüntüleri" de suç kapsamına alınmıştır. Bu şekilde, çocuk pornografisiyle ilgili materyali bulunduran veya ticaretini yapanların elindeki görüntülerin gerçek olmadığı iddiasıyla yaptırımından kurtulmasının önüne geçilmek istenmiştir (USDOJ, 2011; Dülger, 2004: 93).

Ancak ABD'de çocuk pornografisine ilişkin temel tartışmayı nüdizm konusu oluşturmaktadır. "Kişilerin vücutlarından utanmadan rahatlıkla sosyal olarak çıplak

bir şekilde bir arada ve doğa ile bütünleşik bulunabilmeleri hali” olarak tanımlanan Nüdzizm’in ABD’ndeki taraftarları böyle dolaşmanın farklı bir ifade şekli olduğunu ve bunun için ifade hürriyeti kapsamında korunması gerektiğini iddia etmektedir (Wikipedia, 2011c). Bu iddia, cinsellik içermeyen salt çıplaklığın bir ifade biçimi olarak korunması gerektiğine ilişkin S. Book Co. v. Summerfield isimli Yüksek Temyiz Mahkemesi kararıyla desteklenmektedir (Altlaw, 2012). Bu karara dayanarak nüdzizm savunucuları, çocukların salt çıplak görüntülerinin çocuk pornografisi kabul edilmemesi gerektiğini savunmaktadır. Görüldüğü gibi, çocuk pornografisi konusundaki ABD uygulaması, görsel içeriğin sunuş şeklinin her somut olayda değişmesi sebebiyle yeknesaklık göstermemektedir (Kaya, 2010: 53).

2.5.2.1.1.3 Terörizmle Mücadele Yasaları

Müstehcenlik ve çocuk pornografisi dışında İnternet içeriğine müdahale konusunda ABD’nin önem verdiği diğer bir husus uluslararası terörizmle mücadeledir. 11 Eylül saldırılarından sonra ABD terörle mücadele amacıyla İnternet politikasını radikal bir şekilde değiştirmiştir. 26 Ekim 2001’de yürürlüğe konulan anti-terör kanunu olan Patriot Act, İSS’lara abonelerinin üye bilgilerini soruşturma makamlarına verme konusunda daha ağır yükümlülükler getirmiş, ulusal güvenliğin gerektirdiği hallerde hakim kararı olmaksızın haberleşmenin denetlenebileceğini ve istihbarat örgütleri arasında bu yollardan elde edilen bilgilerin paylaşılabileceğini hükme bağlamıştır (Cybercrime, 2011: Yıldız, 2007: 117).

Ayrıca, Yasa bazı güvenlik hizmeti veren kamu kurumlarının bilişim sistemlerine hukuka aykırı erişimler ve bu sistemlerde bulunan verilere yönelik saldırıları “siber terörizm suçu” olarak tanımlayarak yeni bir suç kategorisi oluştururken, siber suçun kapsamını da genişletmiştir. Yasa’dan önce ABD makamlarının uluslararası bir siber suçu izlemesi ve kovuşturma yapabilmesi için ülke sınırları içerisinde bulunan bilgisayara veya network’e saldırıda bulunulması ve zarar verilmesi gerekmekteydi. Yeni Yasayla saldırının ABD’de bulunan network sistemlerinden geçmesi yeterli sayılmıştır. Buna göre, başka bir ülkede gerçekleşse dahi, herhangi bir şüpheli eylemde bulunulduğunda eğer bu eylem ABD’de bulunan network’lerden birisi

üzerinden data paketi olarak geçmişse, FBI işe karışabilecektir. Dünya İnternet trafiğinin %70'inin ABD networkleri üzerinden geçmesinin bu düzenlemenin nedeni olduğu dile getirilmektedir (Yıldız, 2007: 117-118).

Patriot Act, ABD vatandaşlarının temel hak ve özgürlüklerine getirdiği kısıtlamalar yanında, genel olarak veri iletişimi üzerinde oluşturduğu ağır ve kısıtlayıcı düzenlemeler ve uluslararası hukuku ilgilendiren iletişimin tespiti, izlenmesi ve siber suçların kovuşturulmasıyla ilgili hükümleri nedeniyle hem ülke içinde, hem de dünyada yoğun eleştirilere maruz kalmaktadır (Yıldız, 2007: 118; Dülger, 2004: 96).

Benzer şekilde, 2003 yılında yürürlüğe koyulan “Information Operations Roadmap” isimli⁴⁸ düzenleme ile başta İnternet olmak üzere tüm iletişim araçlarının askeri amaçlarla kullanılması, düşman ağların çökertilmesi ve her türlü mecrada propagandalara karşı mücadele edilmesi amaçlanmaktadır (GWU, 2011; Berber ve Kaya, 01.12.2010:15). Bu düzenleme, İnternet içeriğine keyfi olarak müdahale etmenin önünü açtığı ve ABD'nin İnternet yönetimi konusundaki yetkilerini kötüye kullandığı gerekçesiyle yoğun eleştirilere muhatap olmaktadır (Kaya, 2010: 54).

2.5.2.1.1.4 Telif Hakkı İhlallerine İlişkin Yasalar

AB ve ABD'nin İnternet aktörlerinin sorumlulukları ile ilgili yapmış oldukları düzenlemeler 1996 tarihli WIPO Fikir Hakları Andlaşması gereğince yapıldığı için birbirine benzemektedir (Özbey, 2011: 51). ABD'de İSS'ların sorumlulukları 1998 tarihli DMCA (Dijital Milenyum Telif Hakları Kanunu) ile belirlenmiştir (U.S. Copyright Office, 1998). DMCA dünyada ilk defa İSS'lara sorumluluk getiren düzenleme olması açısından önem taşımaktadır (Oktay and Wrenn, 1999). Yasa'da İSS kavramı erişim, yer ve içerik sağlayıcıların tümüne eşdeğer tutulmuş olup verilen hizmete göre farklı sorumluluklar belirlenmiştir (Özbey, 2011: 51; Oğuz, 2008).

⁴⁸ **Information Operations Roadmap,**
http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB177/info_ops_roadmap.pdf (14.12.2011)

İSS'lara telif haklarına aykırı yayınlarla mücadele amacıyla uyar-kaldır sistemini işletme zorunluluğu getirilmiştir. Hak sahiplerinin uyarıları iletilebileceği etkin bir kurumsal yapı-ajans kurmaları ve ajansla ilgili bilgileri web sitelerinden yayınlamaları gerekmektedir. Keza, İSS'ları usulüne uygun olarak kendilerine iletilen uyarılar üzerine hak ihlali yapan içeriği yayından kaldırmak veya erişimi engellemek zorundadırlar (Oğuz, 2008). ABD'de telif hakkı ihlaline ilişkin uyarıları alan ve değerlendiren Telif Hakkı Ofisi bulunmaktadır. Yer sağlayıcıların telif hakkı ihlallerinden haberdar olabilmeleri için Ofis'in web sitesine başvuruda bulunmaları gerekmektedir (U.S. Copyright Office, 2012).

ABD'de USC (United States Code)'da da İSS'ların sorumluluklarına ilişkin hükümler bulunmaktadır. Buna göre, İSS müşterileri ile yapacakları sözleşmelerde çocukların korunmasına yönelik hükümlere yer vermek zorundadırlar. USC'ye göre kasıtlı ve ticari amaçlı olarak küçüklere ve gençlere zararlı materyalleri İnternete veren herkes cezalandırılır. Bu durum bütün İnternet aktörlerini kapsadığı gibi, tüm aktörler buna ilişkin tedbirleri aldıklarını ispat etmek durumundadırlar (Gpoaccess, 2011).

2.5.2.1.1.5 İnternette Kumarın Yasaklanması Yasası

İçerik düzenlemesine ilişkin olarak getirilen diğer bir federal yasa, 23 Temmuz 1997 tarihli İnternette Kumarın Yasaklanması Yasası'dır. Buna göre, ABD'de Las Vegas ve Atlantic City gibi belirli alanların dışında yasaklanmış bulunan kumar ve şans oyunlarının, İnternet üzerinden oynanması yasaklanarak, şans oyunu oynayanların, suç ve istismardan korunmasına yönelik adım atılmıştır (Köse ve Özen, 2010). Bu yasa ile İnternet üzerinden kumar oynatanlara 2 yıla kadar hapis ile 10.000 \$'a kadar para cezası getirilmiştir (LOC, 1997). Daha sonra UIGEA (Yasa Dışı İnternet Kumar Uygulama Yasası) yürürlüğe girmiştir (Firstamendment, 2011).

ABD bir federal devlet olduğu için her federe devlet kendi sınırları içerisinde Anayasada öngörülen sınırlamalara bağlı kalmak şartıyla farklı düzenlemeler yapabilmektedir. Örneğin, Michigan Eyaleti'nde 1993 yılında Eyalet Ceza

Yasası'nda yapılan bir deęişiklik ile, e-posta ve dięer elektronik iletiřim sistemleri ile gerekleřtirilen taciz eylemlerine özgü bir düzenleme yapılmıřtır. Michigan Eyaleti'nde bařlayan bu düzenleme ardından Arizona, Alaska, Connecticut, New York Oklahoma ve Wyoming eyaletlerinde de gerekleřtirilmiřtir (Sınar, 2001: 84). Keza, 2010 yılında Massachusetts Eyaleti'nde, müstehcenlik yasasında yapılan bir deęişiklikle ocuklara zararlı kabul edilen pornografik ierikli web sitelerinin yasaklanması yönünde bir karar alınmıřtır (Shein, 2010).

Bazen eyaletlerce yapılan düzenlemelerin Anayasa'ya aykırılık nedeniyle iptal edildiklerine de rastlanılmaktadır. Örneęin, New York, New Mexico, Michigan ve Virginia eyaletlerinde ocukların İnternetteki sakıncalı ierikten korunması amacıyla hazırladıkları düzenlemeler Temyiz Mahkemesi tarafından Anayasa'ya aykırı oldukları gerekesiyle iptal edilmiřtir (EFA, 2011).

2.5.2.1.2 İerik Düzenleme Politikası

ABD'de bilgi ve iletiřim teknolojileri konusu Ticaret Bakanlığı'nın görev alanına girmektedir. Bakanlıęa baęlı Ulusal Bilgi ve Telekomünikasyon İdaresi (NTIA)'nin sorumlu olduęu konular arasında İnternet politikası (gizlilik, telif hakları), İnternet alan adları, spektrum yönetimi ve geniřband hizmetleri de bulunmaktadır (NTIA, 2011).

Bunun yanında, ABD'de elektronik haberleřme ve yayıncılık sektörünü düzenleyen özerk kurum, 1934 tarihli İletiřim Kanunu ile kurulan Federal İletiřim Komisyonu (FCC)'dur. FCC, ulusal ve uluslararası alanda telli, telsiz, televizyon, kablo ve uydu hizmetlerini düzenlemekle görevlendirilmiřtir. Kurum, elektronik haberleřme hizmetlerine yönelik düzenleme ve denetleme fonksiyonları yanında, bünyesinde bulunan medya bürosu, kablo televizyon, televizyon ve radyo yayınlarını da ieren elektronik medya sektörünü yönetmektedir. Bu çerevede, söz konusu hizmetlerle ilgili programların lisanslandırılması ve politikaların belirlenmesi iin hükümete tavsiyelerde bulunmaktadır (FCC, 2011).

ABD'nin kendine has demokrasisi ve özgürlük anlayışı içinde zararlı görülen İnternet içerikleriyle mücadele için ya da İnternet suçlarının önlenmesi için yapılan her türlü hukuki düzenleme tepkiyle karşılanmaktadır. Her yapılan yeni düzenlemenin ve yeni suç tipleri oluşturulmasının gerek anayasal, gerekse evrensel hukuk temelinde bazı özgürlüklerin özüne dokunması tehlikesinden endişe duyulmaktadır. Bu nedenle yapılan her bir düzenleme karşı bir sivil toplum hareketi de doğurmaktadır. Bu hareketler STK'lar tarafından yönlendirilmekte, şartlar olgunlaştığında yine bu örgütler tarafından açılan davalarla bir kısım düzenlemeler bir süre sonra Yüksek Mahkeme tarafından iptal edilebilmektedir. Bu durum bazı eylemleri yaptırımsız bırakabilirken, zararlı İnternet içeriğiyle veya İnternette işlenen suçlarla yapılacak mücadelede hukuksal boşluklar ortaya çıkarabilmektedir (Dülger, 2004: 91). Diğer yandan ise, bu durumun gönüllülük esasının yer bulmasına neden olduğu ve İnternet sektörünün inisiyatif alması ve öz düzenleme mekanizmalarının harekete geçmesi beklentisi oluşturduğuna dair iyimser bir yaklaşım da vardır (OpenNet, 2006-2007a).

Ayrıca, çocuk pornosu hariç içerik düzenlemesi ile ilgili genel temayül, içeriği tümüyle bloklamaktan ziyade istenmeyen kısımlara erişimin engellenmesi yönündedir. Bunun için de servis, yer ve içerik sağlayıcıların bu konuda teknik imkanlarını kullanacaklarına ve uyar-kaldır benzeri yöntemlere olumlu katkı sağlayacaklarına güvenilmektedir. Nitekim, ABD uyar-kaldır sistemini yasal düzenlemeye kavuşturmuş ilk ülkedir (OpenNet, 2006-2007a).

Benzer şekilde, ABD'de de dijital oyun sektörünün öz düzenleme uygulamaları geliştirdiği görülmektedir. ESRB (Eğlence Yazılımı Değerlendirme Kurulu) bunlardan en meşhur olanıdır. ESRB, ABD oyun pazarında önemli bir paya sahibi olan oyun ve eğlence yazılım şirketleri tarafından 1994 yılında kurulmuştur. Kar amacı gütmeyen, bir öz düzenleme kuruluşu niteliğindedir (ESRB, 2010).

ESRB, oyunları içeriklerine göre sınıflandırmaktadır. Kuruluşun görevleri arasında ebeveynleri, yaş derecelendirmeleri ve içerik tanımlayıcıları sayesinde aileleri için alacakları interaktif oyun ürünleri konusunda bilgilendirmek ve bilinçlendirmek, bilgisayar ve dijital oyun sektörünü sorumlu pazarlama uygulamaları açısından hesap

verebilir hale getirmek bulunmaktadır. ESRB'nin uygunsuz durumlarda müdahale yetkisi vardır. Ürün ile müşterinin sağlıklı bir piyasada buluşması amacını gerçekleştirmeye çalışmaktadır (ESRB, 2010).

ESRB tarafından gerçekleştirilen yaş derecelendirme işlemi zorunlu olmamakla beraber, neredeyse bütün oyunlar ESRB tarafından derecelendirilmektedir. Hatta bazı oyun satan mağaza zincirleri ve marketler sadece ESRB logolu ürünleri satışa sunmayı tercih etmektedirler. Bu öz düzenleme uygulamasının olumlu sonuçlar verdiğine dair bir rapor Federal Ticaret Komisyonu tarafında 2009 yılında yayınlanmıştır. Rapora göre, dijital oyunlar endüstrisinin, pazardaki ürünlerde çocuklar için uygun olan derecelendirme içinde şiddet içeriğini kısıtlayıcı tedbirler almakta oldukça önemli gelişmeler kaydettiği belirtilmektedir (Güneş, 2011: 58).

ABD'de İnternet kullanıcılarının, özellikle de çocukların ve gençlerin zararlı içerikten korunmaları için bilinçlendirme faaliyetlerine önem verilmektedir. Bu kapsamda 1998 yılında kurulan ve kar amacı gütmeyen i-SAFE Vakfı, İnternet güvenliği alanındaki eğitimleriyle sadece ABD'nde değil dünyada da önemli bir yere sahiptir. Vakıf, medya okur-yazarlığı ve dijital vatandaşlık eğitim materyalleri ve yazılımlarının da önemli isimlerinden birisidir (ISFE, 2011).

İ-SAFE'in "NetSmartz Workshop" programı 5-17 yaş arasındaki çocukların çevrimiçi ve çevrimdışı güvenliği hakkında yaş gruplarına uygun kaynaklar kullanarak interaktif eğitim vermektedir. Bu program, Ulusal Kayıp ve İstismara Uğramış Çocuklar Merkezi (NCMEC)'nin de interaktif eğitim kaynağıdır (Bayzan, 2011: 150). NetSmartz Workshop, kamu-özel ortak girişimi ile meydana gelmiştir. Özel firmalardan alınan sponsorluk, NetSmartz Workshop ve yenilikçi içeriğinin çocuklarla, ebeveynlerle, velilerle, eğitimcilerle ve yasa uygulayıcılarıyla "www.netsmartz.org" sitesinden İngilizce ve İspanyolca dillerinde paylaşılmasını sağlamaktadır. Ayrıca, aynı adresten İngilizce ve İspanyolca yayın yapan, İnternetin güvenli kullanımı konularında ebeveynler ve eğitimcilerin her türlü soru ve problemlerine cevap veren bir yardım hattı da bulunmaktadır (Netsmartz, 2012).

ABD’de, önemli bir STK olan NCMEC tarafından kurulup işletilen, “www.missingkids.com” veya “www.ncmec.org” adreslerinden İngilizce ve İspanyolca yayın yapan, Cybertipline adında, INHOPE üyesi bir İnternet ihbar merkezi bulunmaktadır. Cybertipline, 1998’de kurulmuş olup, çocukların cinsel istismarı ve bunları içeren materyallerin dağıtımıyla mücadele etmekte ve FBI ile birçok resmi kurumla işbirliği içinde çalışmaktadır (Missingkids, 2012a).

Cybertipline çocukların cinsel istismarına ait içerikleri, çocukları İnternette cinsel amaçlı ayartma, çocuk fuhşu, çocuk seksi turizmi, çocukların cinsel tacizi, çocuklara istekleri dışında müstehcen yetişkin içeriklerinin gönderimi, yanıltıcı alan adları kullanımı yolu ile ve aldatıcı kelimeler ve dijital fotoğrafların kullanımı yolu ile çocukları zararlı içeriklere yönlendirme suçları ile ilgili ihbarları kabul etmektedir. İhbarlar çevrimiçi form ve telefon ile alınmaktadır. İSS’ların ihbarı için web sitesinde ayrı bir bölüm oluşturulmuştur. Merkez, 2012 Aralık ayına kadar yarısı halktan yarısı da İSS’lerden 1,7 milyondan fazla ihbar almıştır (Missingkids, 2012b).

İhbarla ilgili ilk değerlendirme ihbar merkezi operatörleri tarafından yapılmaktadır. Daha sonra NCMEC’in sömürülen çocuklar bölümü tüm delilleri incelemekte ve gerekli yeni araştırmaları yapmaktadır. Sonrasında elde edilen bilgiler FBI, Göç ve Gümrük Kuvveti (ICE), yerel adli merciler ve Birleşik Devletler Posta İzleme Servisi (USPIS)’ne güvenli bir ağ bağlantısı üzerinden iletilmektedir. Bu bilgiler ayrıca Çocuklara Karşı İnternet Suçları Görev Güçleri (ICAC) bürolarına ve gerekli ise İSS’lara gönderilmektedir (Missingkids, 2012b).

Temel amacı kaybolmuş veya cinsel istismara uğramış çocuklar konusunda adli merciler, aileler ve çocuklara yardım etmek ve bu konuda uzmanlık hizmeti sunmak olan NCMEC, 1984’te Kongre tarafından çıkarılan bir yasa ile kurulmuştur. NCMEC, 7 ofisi ile faaliyet göstermekte ve ABD hükümeti ve işbirliği yapan kişiler ve kurumların bağışları ile finanse edilmektedir. Herhangi bir ücret almadan gönüllü olarak çalışmak isteyenlere faaliyetlerinde görev vermektedir. 2010 yılındaki 52 milyon dolarlık toplam gelirinin 37 milyon doları federal bütçeden, kalan kısmı ise bağışlar ve diğer gelirlerden oluşmuştur (Missingkids, 2012b, 2012c).

NCMEC, CVIP (Mağdur Çocuk Tanıma Programı) adlı uygulama yazılımı ile çocuk kurbanların kimliklerini teşhis etmeye çalışmakta ve bu yolla adli soruşturmalara ve kayıp çocukların bulunmasına yardım etmektedir. 2007 yılında her fotoğrafın tekil parmak izi olarak tarif edebileceğimiz hash değeri üzerinden fotoğraf eşleştirmesi yapmaya başlayan program, Microsoft'un teknik desteği ile 2009 yılında Photo DNA denilen ve hata oranının on milyarda bir olduğu ifade edilen yeni bir teknolojiye geçmiştir. NCMEC'in çocuk kurbanı teşhis programı 2012 Kasım'ına kadar 77 milyona yakın çocuğun cinsel istismarına ait fotoğraf ve videoyu incelemiştir. Bu programın elde ettiği tüm hash değerleri İSS'lar ile paylaşmakta ve sunucularında bulunabilen bu içeriklerin tespit edilip İnternet ortamından uzaklaştırılmasında kullanılmaktadır. NCMEC 1984'den 2012 Aralık'ına kadar 183 binden fazla çocuğun kurtarılmasında FBI'a yardımcı olmuştur. Bu çocukların içinde henüz iki haftalık bebekler bulunmaktadır (Missingkids, 2012c, 2012d, 2012e).

NCMEC, 2007 yılından bu yana ABD'deki İSS'ların %74'üne karşılık gelen 67 İSS ve 6 uluslararası polis teşkilatı ile ortaklaşa bir bağlantı adresi kara liste projesi yürütmektedir. Proje kapsamında, Cybertipline'a gelen ihbarlar NCMEC analistleri tarafından değerlendirilmekte ve açıkça çocukların cinsel istismarını içeren görüntüler polise ve adli mercilere rapor edilmektedir. Sunulan rapordan sonra NCMEC içeriğin kaldırılıp kaldırılmadığını sürekli kontrol etmekte ve 7 gün içinde kaldırılmaz ise içeriğin bağlantı adresi kara listeye eklenmektedir. Bu liste her gün güncellenmekte ve anlaşmalı İSS'lara gönderilmektedir (Missingkids, 2012f).

ABD'de çocukların cinsel istismarına ait içeriklerin satış ve pazarlama cirosunun multi milyar dolarlar seviyesine geldiği ve İnternette en hızlı gelişen sektör olduğu görülmektedir. Bu nedenle 2006 yılında FCACP (Çocuk Pornografisine Karşı Finansal Koalisyon) adında, çocukların cinsel istismarına ait içeriklerin ticaretinin engellenmesi amacıyla birçok banka, kredi kartı şirketi, üçüncü kişi ödeme şirketleri ve İnternet şirketlerini bir araya getiren gönüllü bir organizasyon kurulmuştur. ABD'deki ödeme endüstrisinin %90'ından fazlasını oluşturan organizasyonun üyeleri, çocuk pornografisi sektörüne ait ödemeleri ve parayı takip etmekte, finansal

bağı keserek bu paraların yasal finans sistemine dahil olmasını engellemeye çalışmaktadır (ICMEC, 2012a).

FCACP, ICMEC (Uluslararası Kayıp ve İstismara Uğramış Çocuklar Merkezi) ve NCMEC tarafından yönetilmekte ve organizasyon üyeleri kendi arasında bilgi ve tecrübe paylaşımı yapmaktadır. FCACP'ın faaliyete girmesinden bu yana ticari olarak çocukların cinsel istismarına ait içerikleri pazarlayan web siteleri ile ilgili Cybertipline'a yapılan şikayetler %50 oranında azalırken, diğer yandan, içeriklerin fiyatlarında ciddi artışların meydana geldiği görülmüştür. 2006 yılında çocukların cinsel istismarına ait içerikleri pazarlayan web sitelerinin üyelik ücretleri genel olarak 30 dolar civarında iken, bugün bu rakamın yer yer 1200 doların üzerine çıktığına rastlanılmaktadır. Tüm bunlar FCACP'ın çalışmalarının bu tür sitelerin faaliyetlerini ne kadar zorlaştırdığını göstermektedir (ICMEC, 2012a).

NCMEC'in uluslararası alanda işlevini yerine getirmesi için 1998 yılında ICMEC kurulmuştur (ICMEC, 2012b). ICMEC desteği ile FCACP organizasyonu, faaliyet alanını ABD dışına da taşımaktadır. Bu amaçla, Avrupa'da bölgesel ağlar oluşturmak için 2009 yılında Avrupa Finansal Koalisyonu kurulmuştur (Missing Children Europe, 2012). İsviçre'deki tüm bankalar ve İsviçre Bankacılar Birliği de bu projeye destek vermektedir. Yine bu bağlamda Asya Pasifik Finansal Koalisyonu kurulmuştur. Diğer yandan Brezilya'nın en büyük yerel bankası olan Banco Bradesco'nun da FCACP'a katılmasıyla benzer bir çalışmanın Latin Amerika'da yapılabilmesi için ilk adım atılmıştır. FCACP'ın arkasındaki örgüt olarak ICMEC'in Brüksel, Singapur ve Atina'da üç ofisi bulunmaktadır. Şimdi de Latin Amerika'ya hitap edecek bir ofisin Brezilya'da açılması planlanmaktadır (ICMEC, 2012c).

Diğer yandan, yasadışı ve zararlı içerikle mücadele konusunda tüm dünyada yeni bir trend olarak ortaya çıkan sektörde yer alan şirketlerle özel çalışma ve anlaşma yapma uygulamaları ABD'de de görülmektedir. Daha önce New York Adalet Bakanlığı'nın, ABD'nin üç büyük İSS'sı ile yapmış olduğu bir anlaşmadan bahsetmiştik.⁴⁹ Harvard

⁴⁹ Bkz. "Özel anlaşmalar Yapma" maddesi.

Üniversitesi Berkman İnternet ve Toplum Merkezi'nin direktörlüğünde, İnternetin güvenli kullanımı ve gençler üzerine etkileri gibi konularda çalışmalar yapmak üzere ABD'nin önde gelen sektör firmaları, düşünce ve araştırma kuruluşları ile STK'larının bir araya gelmesiyle oluşturulan "İnternet Güvenliği Teknik Görev Kolu" çalışması da bu örneklerden bir diğeridir (Berkmen Center, 2008).⁵⁰

Bu grup bir yıllık bir çalışma sonunda yayınladığı "İnternet Teknolojileri ve Çocuk Güvenliğini Geliştirme" başlıklı raporda, İnternet toplumu üyelerinin, çocuk güvenliği uzmanları, teknoloji uzmanları, kamu idareleri, sosyal hizmetler görevlileri ve kanun koyucular ile iş birliği yaparak, çocukları İnternetin zararlarından korumak için teknoloji geliştirilmesinin, bilgi paylaşımı ve teknoloji kullanımına standartlar getirilmesinin ve yapılacak bu çalışmaların yaygınlaştırılması için çaba sarf edilmesinin gerekliliği ortaya konulmuştur (Berkmen Center, 2008).

Diğer yandan, ABD telif hakkı ihlallerine ilişkin olarak yoğun bir şekilde İnternet içeriğine müdahale etmektedir (Deibert vd., 2008): 9). Bu konuda bireysel engellemelerin yanında, etkin bir mücadele yürütmek amacıyla İnternet ortamı da dahil olmak üzere, her türlü ortamda telif hakkı ihlalleri için ağır cezalar getirmiştir. Böylece, bireyler üzerinde psikolojik baskı oluşturmak suretiyle bir sosyal engelleme tekniği de kullanmış olmaktadır (Kaya, 2010: 54). Bunun yanı sıra, telif hakkı ihlalleri için, Digital Milenium Act ile uyar-kaldır modeli de getirilmiştir.

ABD'nin, diğer konulardaki içeriklere karşı doğrudan önlem almayı hala tartışırken, ulusal güvenlikle birlikte telif hakkı ihlalleri ve online kumar konusunda tartışmasız olarak önlem alması oldukça dikkat çekicidir. Bu konulardan ulusal güvenlikle ilgili olan düzenlemeler terörizmle mücadele gerekçesine dayandırılırken, telif hakkı ihlalleri ve online kumar içerikleriyle ilgili düzenlemelerin temel gerekçesini

⁵⁰ Çalışma grubunun üyeleri, AOL/Bebo, Aristotle, AT&T, Center for Democracy & Technology, Comcast, Community Connect Inc., ConnectSafely.org, Enough Is Enough, Facebook, Family Online Safety Institute, Google Inc., IAC, İkeepsafe, IDology, Inc., Institute for Policy Innovation, Linden Lab, Loopt, Microsoft Corp, MTV Networks/Viacom, MySpace and Fox Interactive Media, National Center for Missing & Exploited Children, The Progress & Freedom Foundation, Sentinel Tech Holding Corp., Symantec, Verizon Communications Inc., Xanga, Yahoo! Inc., Wiresafety.org'tur. (Berkmen Center, 2008)

üreticilerin ve rekabetçi piyasanın korunması oluşturmaktadır. Doğrudan önlem alınmasıyla ilgili tartışmaların sürdüğü diğer konuların genel gerekçesini kullanıcıların güvenliği ve korunması düşüncesinin oluşturduğu dikkate alınırsa, çarpıcı bir sonuçla karşılaşmış olunmaktadır.

Yani, ABD, ulusal güvenlik ve ekonomik gerekçelerle İnternet içeriğinin düzenlenmesi konularını, kullanıcıların güvenliği ve korunması gerekçesinden daha önemli kabul etmekte ve bu konularda daha katı bir tutum sergilemektedir. Diğer bir deyişle, devletin kendisini koruma refleksleri ile telif hakkı ihlallerinden ve online kumardan olumsuz etkilenen sektörlerin menfaatleri kullanıcı vatandaşların güvenliğinden ve korunmasından daha öncelikli görülmekte ve içerik politikalarını daha çok etkilemektedir.

Keza, dünyadaki porno piyasasının üretim, tüketim ve dağıtım boyutu ile en önemli aktörü olan ABD porno sektörünün, ABD içerik politikalarının oluşumunda etkili olarak İnternette yer alan bu tür içeriklere karşı doğrudan önlem alınmasına engel olduğu da iddia edilebilir. Dolayısıyla, ulusal güvenlik konusunu bir kenarda tutacak olursak, küresel kapitalist sistemin kalbi durumundaki ABD'nin içerik politikalarını büyük oranda ilgili piyasa oyuncularının belirlediğini söyleyebiliriz.

Diğer yandan, piyasanın ve dolayısıyla paranın hemen her konuda etkili olduğu bu siyasal ve sosyal yapı içerisinde, ABD'de çocuk istismarı ve pornografisi ile mücadele eden en önemli ve etkili örgüt olan NCMEC'in 2010 yılı bütçesinin 52 milyon dolar olduğu düşünülürse, on milyar dolarların döndüğü bu devasa sektörle yeterli mücadelenin yapıldığını veya yapılabildiğini söylemek gerçekçi olmayacaktır. Nitekim, NCMEC gibi iyi niyetli girişim ve çabalara rağmen, çocuk pornografisi sektörünün her geçen yıl hızla büyümesi bunun bir göstergesidir.

Sonuç olarak, ABD'de teknik olarak genel bir İnternet filtrelemesi olmamakla birlikte, okullarda ve kütüphanelerde çocukların müstehcenlik gibi zararlı içeriklerden korunmasına yönelik filtreleme programlarının kullanılmasını zorunlu kılan düşük düzeyli yasal bir düzenleme vardır. Ülkede tartışmalar sürekli canlılığını

sürdürse de, çocukların cinsel istismardan korunması, ulusal güvenliğin sağlanması, telif hakkı ihlallerinin ve online kumar oynanmasının önlenmesi konularında yasal düzenlemelere dayalı olarak mücadele yürütülmektedir (OpenNet, 2006-2007a).

Bunun yanında, ABD’de İnternette yer alan çocukların cinsel istismarı gibi belirli suçlara yönelik önleyici tedbirler alınması amacıyla, farklı adlarla da olsa sektördeki aktörlerin (firmalar, STK, araştırma kuruluşları vb.) öz düzenleme yaklaşımıyla oluşturdukları yapılar teşvik edilmektedir. Bu çerçevede, bilinçlendirme faaliyetleri, ihbar ve yardım merkezleri kurulması, özel anlaşmalar yapılması ve çalışma gruplarının oluşturulması gibi uygulamalar gerçekleştirilmektedir. Bu yapılar, genelde bağımsız gözükseler de, gerçekte dolaylı olarak hükümetlere bağlı olarak faaliyet yapmaktadır (Çağlar,2011: 115). Dikkatle incelendiğinde neredeyse her bir öz düzenleme uygulamasında, doğrudan veya dolaylı olarak hükümetlerin etkisi görülmektedir. Bu etki bazen bir kamu kurumu ile işbirliği, bazen ilgili bakanlıkların veya kurumların yönlendirmesi ya da zorlaması şeklinde tezahür edebilmektedir.

Bu durumda, ABD uygulamalarının niteliği göz önünde bulundurulduğunda, içerik düzenlemesinin yönetsel boyutu bakımından benimsenen yaklaşımın, öz düzenleme yaklaşımından daha ziyade birlikte düzenleme yaklaşımına daha yakın olduğu görülmektedir. ABD içerik düzenlemesi uygulamaları, ülkede her ne kadar sivil toplum ve İnternet sektörü güçlü olsa da devletin de işleyen sistem üzerinde hatırı sayılır bir ağırlığının olduğunu ortaya koymaktadır. Bu tablo aynı zamanda, içerik düzenlemesine ilişkin kamu yönetimi politikaları açısından ABD örneğinin, genel yaklaşım olarak “yönetişim” modeline uygun düştüğünü de göstermektedir. Dolayısıyla, konunun tüm taraflarının ve paydaşlarının devlet ile birlikte yönetimde söz sahibi olmasını esas alan “yönetişim” yaklaşımının izlerine, ABD içerik düzenlemesine ilişkin örneklerde sıkça rastlanmaktadır.

2.5.2.2 Avustralya

24 milyon İnternet kullanıcısına sahip Avustralya’da İnternet kullanım oranı %67’dir (internetworldstats, 2012b). Avustralya demokratik batılı ülkeler içerisinde, İnternet

içeriğine fazlaca müdahale etmesi ve engelleyici İnternet politikaları nedeniyle eleştirilen bir ülke (Deibert vd., 2008: 166) olmakla birlikte, aynı zamanda, İnternet içeriği konusunda düzenleme ve uygulamalarıyla önemli ilerlemeler kaydeden en özgün İnternet politikalarına sahip demokratik ülkelerden birisidir.

2.5.2.2.1 Yasal Çerçeve

Avustralya, İnternet içeriğine özel hukuki düzenlemeleri bulunan az sayıdaki demokratik ülkeden birisidir.

2.5.2.2.1.1 Yayın Hizmetleri Yasası

Avustralya’da İnternet içeriğinin düzenlenmesine özgü temel yasa, 1992 tarihli Yayın Hizmetleri Yasası’dır. Bu Yasa’ya, 1 Ocak 2000’de online yayıncılık konuları da eklenmiştir. Başlangıç bölümünde de belirtildiği gibi Yasa’nın konusu, etkin rekabet ve izleyici ihtiyaçlarına cevap verecek bir yayın endüstrisinin gelişimini kolaylaştıracak düzenleyici ortam sağlamaktır. Bunun için Yasa ile, tüm yayın hizmetlerinin etkili bir kontrol ve denetimle yürütülmesi hedeflenirken, hizmet çeşitliliği yanında gelişmekte olan Avustralya kimlik, karakter ve kültürel çeşitliliğini de yansıtan yayın hizmetleri teşvik edilmektedir (Comlaw, 2012a).

Bu çerçevede Yasa, yayın hizmetleri ile ilgili şikayetleri ele alacak araçların geliştirilmesi ve zararlı yayınlardan çocukların korunmasına öncelik verilmesi prensibinden hareketle; belirli İnternet içeriği ile ilgili şikayetleri değerlendirecek mekanizmaların kurulmasını, makul bir yetişkin için suç nedeni olabilecek belli İnternet içeriğine erişimin kısıtlanmasını ve çocukların yasadışı ve zararlı İnternet içeriğine maruz kalmalarının önüne geçilmesini konu edinmiştir (Comlaw, 2012a).

Yasa’nın başlangıç kısmında bu alandaki düzenleyici politikaların temelini kamu yararının oluşturduğunun; içerik düzenlemesine ilişkin kurallar belirlenirken içerik, yer ve servis sağlayıcılara gereksiz mali ve idari yükümlülükler getirilmemesinin, bu alandaki teknolojik gelişim ve değişimin teşvik edilmesinin ve toplumun sosyal,

endüstriyel ve ticari ihtiyaçlarını karşılayacak performans standartlarıyla İnternet hizmetlerinin yürütülmesinin temin edilmesinin altı çizilmektedir (Comlaw, 2012a).

Bu Yasa bir bütün olarak, İnternet içeriğinin sınıflandırılması, yasadışı içerikle mücadele, İSS'lar ve içerik sağlayıcıların sorumlulukları, şikayetler ve soruşturmalar, cezai yaptırımlar, sektörel kuralların, standartların, yayıncılık ilkelerinin ve kıstaslarının belirlenmesi gibi online yayıncılığın düzenlenmesi ve denetlenmesi ile ilgili alanları kapsayıcı hükümler öngörmekte ve bunlarla sorumlu idari otorite olarak Avustralya Yayın Kurumu (ABA)'nu oluşturmaktaydı (Comlaw, 2012a).

Buna göre ABA'ya, ilgili endüstri, tüketici grupları ve devlet kurumları ile işişare içinde İnternet içeriğini izleme, kamuoyunu eğitime, bilinçlendirme ve danışmanlık yapma; yasadışı ve zararlı içeriklerle ilgili ihbar ve şikayetleri alma ve değerlendirme ile yasadışı ve zararlı içeriklerin uyar-kaldır yöntemi ile yayından kaldırılmasını sağlama; Sınıflandırma Kurulu'nunun kararlarına göre içeriklerin hostinglerce veya İSS'larınca filtrelenme ve erişim kontrol sistemlerinin uygulamasını sağlama; İnternet içeriği ve İnternet taşıma hizmetleri ile ilgili konularda araştırmalar yapma ve komisyonlar kurma; İnternet sektörünün düzenlenmesi ve geliştirilmesi için birlikte çalışma prensibiyle ilgili yurtdışı kurumlarla yardımlaşmanın zeminini oluşturma görevleri verilmekteydi (Comlaw, 2012a).

Fakat, bütün dünyada olduğu gibi, sayısal teknolojilerin gelişimi ile Avustralya'da da elektronik haberleşme, basın-yayın ve bilgi teknolojileri arasındaki sınırlar belirsizleşmeye başlamıştır. Bu yakınsamadan kaynaklanan sorunlar üzerine Hükümet çareyi Avustralya Telekomünikasyon Otoritesi ile Yayıncılık Otoritelerini birleştirmekte bulmuştur. Böylece, 6.4.2005 tarihinde çıkartılan Avustralya İletişim ve Medya Kurumu Yasası ile ABA ve Avustralya İletişim Kurumu (ACA)'nın⁵¹ yerine ülkede İnternet içeriğinin düzenlenmesiyle ilgili özerk yetkili kuruluş, diğer

⁵¹ ACA, Australian Communications Authority Act (Avustralya Telekomünikasyon Yasası - 1997) ile kurulmuş telekomünikasyon ve spektrum yönetimi ile ilgili özerk kurumdur. Bu Yasa'nın tam metni için bkz. <http://www.comlaw.gov.au/Details/C2004A05150> (25.02.2012)

medya içeriklerinde olduğu gibi Avustralya İletişim ve Medya Kurumu (Australian Communications and Media Authority-ACMA) olmuştur (Comlaw, 2012b).

2.5.2.2.1.2 Sınıflandırma Yasası

Avustralya’da İnternet içeriğini ilgilendiren ikinci önemli düzenleme, 1995 tarihli olmakla birlikte 2010 Temmuzunda bazı değişikliklere uğrayan Sınıflandırma (Yayınlar, Filmler ve Bilgisayar Oyunları) Yasası’dır. Bu Yasa ve Yasa’ya dayalı olarak çıkarılan Filmlerin ve Bilgisayar Oyunlarının Sınıflandırılması İçin Yönerge ile ülkedeki film, bilgisayar oyunları ve içerisinde İnternet yayınlarının da yer aldığı diğer yayınların sınıflandırılmasına ilişkin usuller, kıstaslar ve yetkili organlar belirlenmiştir. Buna göre söz konusu materyalleri sınıflandırmak üzere Avustralya Sınıflandırma Kurulu oluşturulmuştur (Comlaw, 2012c).

Bu Yasa ile yayınlar, filmler ve bilgisayar oyunlarının sınıflandırılması amaçlanmaktadır. Özerk bir yapı olarak kurulan Sınıflandırma Kurulu söz konusu yazılı, sesli ve görsel materyalleri sınıflandırarak, sertifika ve ulusal sınıflandırma kodu vermektedir. Burada metin şeklindeki görüntülerle birlikte, gerçek ve bilgisayar tarafından oluşturulan görsel imajlar, tasvirler ve ses kayıtları da bu kapsamda değerlendirilmektedir. Sınıflandırma Kurulu’nun kararlarına karşı ilgili Bakan, eser sahibi, yayıncı, kararla haksızlığa uğradığı düşünülen kişi ve kuruluşlar itirazda bulunabilirler. İtirazlar Sınıflandırma Değerlendirme Kurulu tarafından görüşülerek nihai karara bağlanmaktadır (Comlaw, 2012c).

Yasa’ya göre filmler, “G” Genel, “PG” Ebeveyn Rehberlik, “M” Olgun, “MA 15+” Olgun Eşliğinde, “R 18+” Kısıtlı, “X 18+” Kısıtlı, “RC” Sınıflandırma reddi; bilgisayar oyunları, “G” Genel, “PG” Ebeveyn Rehberlik, “M” Olgun, “MA 15+” Olgun Eşliğinde, “RC” Sınıflandırma reddi olarak artan sırayla sınıflandırılmakta ve kodlamaya tabi tutulmaktadır (Comlaw, 2012c).

Sınıflandırma talebi reddedilen materyaller “RC” kodu ile işlem görmektedir. “RC” kodu, sınıflama kuralları dikkate alındığında diğer hiçbir kodun özelliklerine uygun olmayan ve bu nedenle sınıflandırılmayan/sınıflandırma dışı materyal anlamına

gelmektedir. Bu materyallerin makul bir yetişkin için genel olarak sakıncalı ve suç teşkil eden veya çocukların görmesine ve okumasına uygun olmayan içeriklere sahip olduğu kabul edilmektedir. Yasa'ya göre, Ceza Kanunu kapsamı içinde doğrudan veya dolaylı olarak terör eylemi çağrısı yapan, talimat veren veya terör eylemini tarif eden, terör eylemlerini savunan veya öven yayınlar, filmler ve bilgisayar oyunları “RC” kodu ile işlem görmektedir (Comlaw, 2012c).

Ayrıca Sınıflandırma Kurulu, sınıflandırılması istenilen materyale ilişkin şu durumları tespit ederse sınıflandırmayı reddetmektedir (Comlaw, 2012c):

- Bağımlılık oluşturan zararlı madde kullanımı, suç, zulüm, şiddet veya makul yetişkinler tarafından genel olarak kabul edilemeyecek düzeyde ahlak, terbiye ve görgü standartlarına aykırı ve rahatsız edecek bir şekilde iğrenç ya menfur olayların gösterilmesi, tasvir ve teşvik edilmesi, talimat verilmesi,
- Makul yetişkinler tarafından genel olarak sakıncalı ve suç kabul edilebilecek bir şekilde yetişkin veya 18 yaşın altındaki çocuklara ilişkin cinsel aktivitelerin tasvir veya anlatımı.

Yasa bir yayının, filmin veya bilgisayar oyununun sınıflandırılmasında göz önünde bulundurulması gereken kriterleri şu şekilde belirtmektedir (Comlaw, 2012c):

- Makul yetişkinler tarafından genel olarak kabul edilen ahlak, terbiye ve görgü standartları,
- Edebi, sanatsal veya eğitimsel niteliğe haiz olup olmadığı,
- Genel karakterinin tıbbi, yasal ya da bilimsel nitelikte olup olmadığı,
- İçeriğin nerede yayımlandığı, kimlere yönelik olduğu ve ne amaçladığı.

Yasa, ticari veya mesleki promosyon, bilimsel ve eğitsel nitelikli yayın; güncel konular, olaylar, haber, bilgi ve analizlerine ilişkin yayınlar; spor, hobi, sosyal aktivite, canlı sanatsal performans, müzikal sunum, kültürel ve dini etkinlikler benzeri içeriklere sahip film ve yayınları sınıflandırmadan muaf tutmuş ve bu tür materyaller için başvuruları gerekli görmemiştir.

2.5.2.2.1.3 Sınıflandırma Yönergesi

Sınıflandırma Yasası'na dayalı olarak çıkartılan ve ilk olarak 2005 yılında yayınlanan fakat 2008 yılında revize edilen söz konusu içeriklerin sınıflandırmasına ilişkin Yönerge, sınıflandırma kategorilerini, bu kategorilerin kapsamını ve materyallerin her kategori için sınırlarını detaylı olarak belirlemektedir. Buna göre sınıflandırma kararları Sınıflandırma Kurulu tarafından verilmekte, bu kararlara yapılan itirazlar Sınıflandırma Değerlendirme Kurulu tarafından incelenmektedir. Söz konusu Kurullara Avustralya Hükümeti Başsavcılık Dairesi tarafından destek sağlanmaktadır (Comlaw, 2012d).

Yönerge bir yayını, filmi veya bilgisayar oyununu sınıflandırırken Yasa'da geçen kriterleri aynen sayarken bu kriterlere göre değerlendirilen içeriklerin kodlanmasında aşağıdaki ilkelerin dikkate alınmasını öngörmektedir (Comlaw, 2012d):

- Yetişkinler ile çocuklara uygun içeriklerin belirlenmesi ve küçüklerin zarar verecek veya rahatsız edebilecek materyallerden korunması,
- Toplumun saldırganlık içeren istenmeyen içerikten korunması,
- Toplumun kaygılarını dikkate alarak, genel olarak şiddete ve özellikle cinsel şiddete göz yuman ya da teşvik eden tasvirler ile kişileri alçaltıcı nitelikteki içerik ve tasvirlerin engellenmesi.

Yönerge, bu ölçüt ve ilkelere göre içerikleri genel bağlam ve tema, şiddet, seks, argo ve kaba dil, çıplaklık ile uyuşturucu kullanımı unsurları açısından Yasa'da bahsi geçen hiyerarşiye göre kodlanmaktadır. Yönergeye göre, "R 18+" ve "X 18+" film kategorilerinin daha üzerinde yer alan içeriklere sahip materyaller ile "MA 15+" kategorisini aşan içeriklere sahip bilgisayar oyunlarının sınıflandırma talepleri reddedilmektedir ve yasaklı içerik olarak kabul edilmektedir (Comlaw, 2012d).

Yasa ve Yönerge çok detaylı ve anlaşılır bir sınıflandırma sistemi öngörmektedir. Bu sınıflandırmaya dayalı olarak ülkede "Sınırlandırılmış Giriş Sistemi" (Restricted Access System) oluşturulmuştur. Bu sistem, adından da anlaşılacağı gibi, İnternet

kullanımında yaşa dayanan bazı sınırlandırmalar getirmektedir. Sistem; ilgili kamu kurumları, yayıncılık endüstrisi ve üniversitelerin ortak çalışması sonucunda meydana getirilmiştir. Televizyondaki programların kategorize edildiği gibi İnternetteki web sitelerinin de kategorize edilmesi mantığına dayanmaktadır. Sınırlandırılmış Giriş Sisteminde İnternet yayınları için de geçerli olan üç farklı kategori bulunmaktadır. Bu kategoriler şunlardır (ACMA, 2007; ACMA, 2012a):

1. RC veya X18+ Kategorileri: Çocukların cinsel istismarı, hayvan pornosu, enstet ilişkiler, fetişler, saldırgan ya da tiksindirici benzeri gerçek ve fantezi ekstrem pornografi barındıran içerikler yanında, suçun, şiddetin ve uyuşturucu kullanımının detaylı anlatıldığı içerikler ile şiddeti, uyuşturucu kullanımını veya terörizmi savunan içerikleri kapsar. Bu içerikler Avustralya'da tamamen yasaktır.

2. R18+ Kategorisi: RC ve X18+ kategorilerindeki içeriklerle birlikte cinsel aktivite tasvirlerinin taklitleri, sert ve gerçek şiddet barındıran içerikler ve diğer yoğun bir biçimde yetişkinlere hitap eden içerikler de bu kategoride yasaktır. Bu içerikler söz konusu sistem gereği çocukların girişinden korunmalıdır.

3. MA15+ Kategorisi: RC, X18+ ve R18+ kategorilerinde bahsi geçen içerikler yanında çıplaklığın vurgulu tasviri, cinsel aktivite iması, uyuşturucu kullanımı, şiddet, sık kullanılan kaba dil bu kategoride yasaktır. Bu kategori de sınırlandırılmış giriş sistemine tabidir.

Sınıflandırma Kurulu'ndan R18+ veya MA15+ ticari sertifikası almak isteyen web siteleri asgari şu şartları sağlamalıdır: Siteye giriş için başvuru şart olmalıdır, giriş sayfasında içerikle ilgili uyarılar bulunmalıdır, bakıcılar ve ebeveynlere yönelik koruyucu bilgiler içermelidir, şifre ile giriş sınırlandırılmalıdır, 2 yıl boyunca yaş doğrulama bilgilerini tutup sonra imha etmelidir. Ayrıca, R18+ sertifikası için söz konusu web sitesi, kullanıcının 18 yaşından büyük olduğunu doğrulayan, MA15+ sertifikası için de 15 yaşından büyük olduğunu ıspatlayan bir mekanizmaya sahip olması gerekmektedir (ACMA, 2007; ACMA, 2012a).

Böylece, Sınırlandırılmış Giriş Sistemi ile bir tür çevrimiçi filtreleme sistemi kurulmuştur. Dolayısıyla R18+ sertifikası olan bir sitenin erotik içerikten dolayı ihbar edilmesi gereksizdir. Ama bu sertifikaya sahip olmayan bir web sitesi bu tür bir içeriği barındıramamakta ve barındırır ise şikayete konu olmaktadır (ACMA, 2007; ACMA, 2012a).

2.5.2.2 İçerik Düzenleme Politikası

Avustralya’da bilgi teknolojileri ve iletişim konularıyla ilgili olarak İnternet, telefon, televizyon, radyo ve posta hizmetlerinden sorumlu ve yetkili müstakil bir bakanlık olarak “Geniş Bant, İletişim ve Dijital Ekonomi Bakanlığı” kurulmuştur. Bakanlık, İnternet ile ilgili en üst düzey sorumlu kamu idaresi olarak İnternet hizmetleri ile İnternet içeriği, siber güvenlik ve gizliliğin sağlanması, İnternet üzerindeki bahis oyunlarının düzenlenmesi ve istenmeyen elektronik postalarla ilgili hususlarda yetkilidir (DBCDE, 2012).

Bu Bakanlığa bağlı olarak 2005 tarihli Avustralya İletişim ve Medya Kurumu Yasası ile kurulan ACMA, ülkede radyo, televizyon, İnternet ve cep telefonu dahil olmak üzere her türlü yayın ve iletişim aracına ait içeriğin düzenlenmesinden sorumlu özerk kamu kurumudur. Kurum, bahsi geçen araçların lisans koşulları, uymaları gereken kurallar ve standartlar ile endüstriyel uyumluluğu sağlamaya çalışırken, öz-düzenleme uygulamalarının geliştirilmesi için sektörel oyuncularla da aktif işbirliği yapmaktadır. Ayrıca, onların toplumun ihtiyaçlarına duyarlı olmalarını sağlamak için düzenlemeler yaparken, mevcut uygulamaların etkisini de izlemeye çalışmaktadır (ACMA, 2012b). Bu kapsamda İnternet içeriği ile de ilgilenmekte, içeriklerle ilgili şikayetleri değerlendirmekte ve sektördeki İSS’lar ve içerik sağlayıcıları düzenlemekte ve izlemekte; güvenli İnternet kullanımı konusunda toplumu bilgilendirmek ve bilinçlendirmek için faaliyetler yürütmektedir (ACMA, 2012c).

ACMA, bu görevlerini yerine getirirken sanayi, tüketici, devlet ve akademi temsilcileri ile yoğun bir işbirliği içinde çalışmaktadır. Politikalar, mevzuat, ürün ve hizmetlerle ilgili sektördeki tüm paydaşları bilgilendirmek için konferanslar ve diğer

etkinlikler ile eğitim programları yapmaktadır (ACMA, 2012b). Kurum, büyük çoğunluğu sektörden gelen profesyonel yöneticiler ve akademisyenlerden seçilmiş ACMA Başkanı, Başkan Yardımcısı, bir tam zamanlı üye ve beş yarı zamanlı üyeden oluşan bir tepe yönetimi tarafından idare edilmektedir (ACMA, 2012b).

ACMA, içerik ve yer sağlayıcılarını düzenleyebilme ve yasaklı ve şüpheli kabul edilen içerik ile mücadele etme konusunda yetkilendirilmiştir. Buna göre, Sınıflandırma Kurulu'nca yasak kapsamına alınan içerik ile daha önce bu Kurul'ca değerlendirilmemiş fakat ACMA tarafından yasak olmasına ilişkin kuvvetli şüphe oluşan içeriklerle mücadele etmektedir. Bu çerçevede, söz konusu içeriğin Avustralya bağlantılı olmasına veya içeriğin yurtdışında barındırılmasına göre ACMA'nın müdahale yöntemi değişmektedir (ACMA, 2012e).

ACMA, bir şikayet aldığı anda veya kendi inisiyatifi ile belirlediği herhangi bir şüpheli İnternet içeriğiyle ilgili olarak içeriğin Avustralya bağlantısı var ise;

a) İçerik, Sınıflandırma Kurulu tarafından “yasaklı içerik” olarak tasnif edilmiş ise, kaldırılması ile ilgili olarak yer sağlayıcıya “uyar-kaldır”, canlı içerik servisi sağlayıcısına “servis durdurma”, link servisi sağlayıcısına da “link silme” kesin bildirimi göndermektedir.

b) İçerik, Sınıflandırma Kurulu tarafından tasnif edilmemiş ancak ACMA'ya göre şüpheli ise; ilgili yer, içerik ve servis sağlayıcıya geçici bildirimde bulunmakta ve Sınıflandırma Kurulu'ndan içeriğin derecelendirilmesini talep etmektedir. Sınıflandırma Kurulu'ndan gelen cevaba göre geçici bildirim ya kesin bildirim dönüşmekte veya iptal edilmektedir (Deibert vd., 2008: 166-167).

Bunlara ilaveten ACMA, kanuni yaptırım gerektiren içeriğe ilişkin Avustralya Polis Teşkilatı'na bildirimde bulunmak zorundadır. Bu durumda, soruşturmayı olumsuz yönde etkilememesi için, yer, içerik veya servis sağlayıcıya gönderilen geçici veya kesin bildirim ertelenebilir veya uygulanmayabilir (Deibert vd., 2008: 167).

Avustralya dışında barındırılan içerikle ilgili olarak ise ACMA'nın Sınıflandırma Kurulu'ndan görüş almasına gerek görülmemiştir. Dolayısıyla ülke dışında barındırılan bir içerik için içeriğin yasal olup olmadığına ACMA karar vermektedir. ACMA tarafından yasaklı veya şüpheli olarak belirlenen içeriğin web bağlantı adresi ACMA'nın Famil Friendly Filters bölümüne yönlendirilip ulusal filtre listesine alınması sağlanmaktadır. Bu şekilde oluşturulan kara liste bu listeyi bloke etme konusunda yükümlülük alan, içerik filtreleme üreticilerine iletilmektedir. Ayrıca bu güncel kara listelerin yer aldığı veri tabanı Avustralya Polisi ve Gümrük Muhafaza Birimine gönderilmekte ve bu kurumların, içeriklerin barındırıldığı ülkelerin yetkili kurumları ile iletişime geçmeleri sağlanmaktadır (Deibert vd., 2008: 168-169).

Veri tabanındaki siteler genellikle, çocukların cinsel istismarı, hayvanlarla cinsel ilişki, aşırı şiddet ve tecavüz, uyuşturucu kullanımını özendirme ve terör içeriği sunan web siteleridir. Bu yasaklı sitelerin listeleri gizli tutulmaktadır. Ülkedeki İnternet kullanıcıları gönüllü olarak kabul ettikleri, ülke dışında barındırılan istenmeyen içerikleri bloklayan filtreleme programlarını desteklemekte ve finanse etmektedir. İSS bu filtre programlarını tüm müşterilerine sunmak zorundadır (Deibert vd., 2008: 168-169).

Sınıflandırma Yasası ve Yönergesi'nde İnternet içeriği için seçilen sınıflandırma sistemi, filmler için kullanılan sistemden daha sert bir sistemdir. Çevrim dışı müsaade edilen bir içeriğe çevrim içi müsaade edilmemektedir. Zira, filmler için öngörülen ve yasal kabul edilen X 18+ film kategorisine giren İnternet içerikleri ülke içinde bir yer sağlayıcı tarafından barındırılıyorsa ACMA'nın bildir-kaldır mekanizmasına konu edilmektedir (Deibert vd., 2008: 171-172).

Diğer yandan bildir-kaldır mekanizması işletilmeye başlanması ve içerik/yer/servis sağlayıcıya bildirimde bulunmasından sonra, yasal olmadığı bildirilen bir içerik kaldırılmamış ise ACMA yasal yollara başvurulabilmektedir. Bildirimde bulunulmasından sonraki iş günü sonuna kadar yasal olmadığı bildirilen içeriği yayından kaldırma uyarısına uymazsa, işletmelere veya gerçek kişilere ağır mali cezalar verilebilmektedir. Kaldırma uyarısına uymayan şirketler 27.500 \$ günlük

para cezası ödemekle yükümlüyken, gerçek kişiler 5.500 \$ günlük para cezasına çarptırılmaktadır (ISOC, 2012).

Avustralya’da ACMA’ya ait bir İnternet ihbar merkezi bulunmaktadır. “www.acma.gov.au” adresinden yayın yapan bu merkez, İnternette yer alan saldırganlık ve şiddet ile çocukların cinsel istismarı içerikleri, yetişkin pornografisi, uyuşturucunun imalinin tarifi veya teşvik edilmesi, suçun detaylı tarifi ve teşviki, terörizmin savunulması, çevrimiçi kumar gibi konularda toplumun endişe ve şikayetlerini ulusal bir düzenleyici program çerçevesinde incelemekte ve bunlara cevap vermektedir. Bu ihbar merkezi resmi bir devlet kuruluşudur ve kurulduğu 1999 yılından bu yana INHOPE’a üyedir (ACMA, 2012f).

ACMA yasadışı kumar içeriği ile ilgili şikayetleri de kabul etmektedir. Telefon bahisçiliği, izin alınmış at yarışları bahisleri, diğer müsabakaların müsabakadan önce oynanan bahisleri, reklam ve malların tanıtımı amaçlı promosyon çekilişleri ve çekiliş hizmetlerini şirket hukukuna uygun ve izin alınmış bir şekilde yapan bahis şirketlerinin durumu yasalıdır. Bunların dışındakilerin tümü yasal olmayan kumar içeriği tanımına girmekte ve şikayete konu olabilmektedir (ACMA, 2012f).

Merkez sadece yer ve içerik sağlayıcılar ve link servislerini ilgilendiren ihbar ve şikayetleri araştırmaktadır. İletişim bilgisi verilmesi durumunda şikayetin sonucu şikayetçiye iletilmektedir. Ayrıca herhangi bir zamanda, şikayetin neticesi ile ilgili e-posta yolu ile sorgulama yapılmasına olanak sağlanmaktadır (ACMA, 2012f).

İhbar merkezi sanal ortamdaki dolandırıcılık, telif hakları ihlalleri, iftira ve hakaret, mahramiyetin ihlali ve genel anlamda spam mesajlar ile ilgili ihbarları kabul etmemektedir. Ama bu konularda nereye başvurulacağı, neler yapılması gerektiği en ince ayrıntısına tarif edilmektedir (ACMA, 2012f). ACMA ihbar merkezi, 2011’de 6.043 ihbar almış ve bunların 2.123’ü hakkında işlem yapmıştır (ACMA, 2012g).

ACMA ülkede, İnternetin güvenli kullanımına ilişkin bilinçlendirme, eğitim, yardım ve destek sağlama çalışmalarında etkin bir kuruluştur. Bu çerçevede çocuklar ve gençler için İnternet güvenliğinin teşvik edilmesine ilişkin olarak Cybersmart ve

Cybersafety Outreach gibi programlar ACMA tarafından geliştirilmiştir. Keza, ACMA'nın geliştirdiği bir diğer destek hizmeti de kütüphane personeli eğitmek ve kütüphane kullanıcılarının güvenli ve olumlu çevrimiçi deneyimlere sahip olmalarını sağlamak amacıyla risk yönetimini içeren bir dizi kaynaktır. Avustralya Kütüphane ve Bilgi Derneği (ALIA) ve Avustralya halk kütüphaneleri ile birlikte geliştirilen bu kaynaklar, kütüphanelerdeki mevcut politikaları desteklemek ve kütüphane personeli için ek kaynak ve destek sağlamak amacıyla geliştirilmiştir (Cybersmart, 2012).

Bir diğer uygulama ise, çocukların ve ailelerin güvenli İnternet kullanımını sağlamak amacıyla tasarlanan “Cybersafety yardım düğmesi”dir. Burası, çocuklara ve gençlere sanal güvenlik konularında yardımcı olmak ve bilgi vermek için 7/24 çevrimiçi hizmet sunan bir merkezdir. Ücretsiz olan uygulama yüklendikten sonra bu siteye doğrudan bağlantı sağlanabilmektedir. Örneğin, uygulamada yer alan konuşma fonksiyonu “Çocuklar Yardım Hattı”na bir bağlantı vermektedir. Sanal zorbalık veya hakaret/uygunsuz sayılabilecek çevrimiçi davranış veya içerik ile ilgili endişe duyan kullanıcılar, bu menü aracılığıyla profesyonel bir danışman ile online sohbet edebilmekte veya telefon görüşmesi yapabilmektedir (DBCDE, 2012).

Avustralya’da uygulanan bir diğer güvenlik uygulaması da ihbar fonksiyonudur. Facebook, MySpace ve Twitter gibi sitelerin sayfalarına, siteye özgü sanal güvenlik bilgisi içeren ve doğrudan bağlantılar sunan bu özellik sayesinde dolandırıcılık, sahtecilik, uygunsuz web siteleri, uygunsuz davranışları ihbar etmek ve Avustralya Polis Teşkilatı ile irtibat sağlamak mümkün olmaktadır (Bayzan, 2011: 83).

Cybersmart programına verilen desteğin yanı sıra Avustralya Hükümeti sektörden Google, Facebook, Yahoo!, Telstra, Microsoft ve Alannah-Madeline Vakfı, “Childwise” ve “Bravehearts” gibi STK’ların temsilcilerinden oluşan Sanal Güvenlik Danışma Grubu’nu oluşturmuştur. Bu çerçevede sanal-güvenlik hususlarının gençlerin bakış açısından incelenebilmesi için de Danışma Grubu’na ve Hükümet’e sanal güvenlik konularında öneriler sağlamak üzere 8-17 yaşları arasındaki gençlerden oluşan Genç Danışma Grubu’nu kurmuştur (Bayzan, 2011: 81).

Görüldüğü gibi Avustralya, İnternet içeriğinin düzenlenmesi konusunda yasal tedbirleri ve uygulamalarıyla müdahaleci ve mücadeleci özelliği ile ön plana çıkan ülkelerden birisidir. İnternet içeriğine özgü yasal düzenlemeleri yanında çok boyutlu ve çok yönlü içerik politikaları ile ülkede İnternet içeriğiyle etkili bir mücadele yürütülmeye çalışılmaktadır. Bu çerçevede saldırganlık ve şiddet, çocukların cinsel istismarı içerikleri, makul sınırlar dışındaki yetişkin pornografisi, uyuşturucunun imalinin tarifi veya teşvik edilmesi, suçun detaylı tarifi ve teşviki, terörizmin savunulması, yasadışı kumar gibi yasadışı ve şüpheli kabul edilen İnternet içeriği ile ACMA isimli özerk düzenleyici kamu kurumunun kontrol ve denetiminde mücadele edilmektedir. Buna göre, kategorizasyonun esas alındığı bir sistemle ülkede barındırılan yasadışı ve şüpheli içeriğe uyar-kaldır yöntemi, ülke dışında barındırılan bu tür içeriklere de filtreleme yöntemi uygulanmaktadır.

ACMA, bu mücadelede Sınıflandırma Kurulu ve polis teşkilatı gibi diğer kamu kurumları yanında, sektörde yer alan yer, içerik ve servis sağlayıcılar ile tüketici ve akademi temsilcileri ve STK'larla işbirliği yapmaktadır. ACMA, bu çerçevede öz düzenleme uygulamalarını teşvik etmekle birlikte ihbar merkezinin işletilmesini ve bilinçlendirme faaliyetlerinin büyük bir kısmını kendi uhdesinde yürütmektedir. Dolayısıyla içerik politikalarının oluşturulmasında ve uygulanmasında kamu otoritelerinin merkezde yer aldığı yönetsel bir yöntemi tercih etmiş gözükmektedir. Bunu yaparken de yönetim yaklaşımı ile hareket etmeye ve demokratik değerlere özen göstermeye çalışmaktadır. Özellikle sınıflandırma konusunda getirilmiş olan sistem ile yasadışı içeriğe ilişkin açık, şeffaf ve sınırları mümkün olduğunca belirlenmiş bir düzenleme ve mücadele zemini oluşturulmaya çalışılmıştır. Dolayısıyla ortaya koyduğu yaklaşım ve uygulamaları ile Avustralya örneği, demokratik değerleri zedelemeyen yasadışı ve zararlı İnternet içeriği ile mücadele etmeye önem veren diğer ülkelere ilham olabilecek niteliklere sahiptir.

2.5.2.3 İngiltere

52 milyon İnternet kullanıcısına sahip İngiltere'de İnternet kullanım oranı %83 gibi yüksek bir rakama ulaşmıştır (internetworldstats, 2012e). Bu kadar yoğun kullanılan

İnternetin içerik düzenlemesiyle ilgili olarak İngiltere, dünyada öncü uygulamalar geliştirmektedir. İngiltere, büyük oranda genel çerçevesini AB'nin belirlemiş olduğu temel ilkelere bağlı kalmakla birlikte, bu ilkeleri de zorlayan kendine özel bazı uygulamalara da gitmektedir. Örneğin, çocuk pornografisi ve ırkçılığa ilişkin içeriğin dışında aşırı pornografik içeriği yasa dışı kabul edip mücadele kapsamına alması ve yakın zamanda Türkiye'deki "Güvenli İnternet Hizmeti"ne benzer bir uygulamayla İnternette yer alan pornografik içeriğe merkezi filtre uygulmasına geçeceğini açıklaması oldukça dikkat çekicidir.

2.5.2.3.1 Yasal Çerçeve

İngiltere'de, gerçek hayatta suç olan İnternette de suç olarak görüldüğünden mahkemeler, Ceza Kanunu'nda yer alan bütün suçlar için suç unsuru teşkil eden içeriklere ilişkin erişim engelleme kararları uygulayabilmektedir (Çağlar, 2011: 125). Bunun dışında, İngiltere'de sakıncalı İnternet içeriğiyle mücadele kapsamında birçok hukuki düzenleme yapılmıştır.

Bu düzenlemelerin önemli bir kısmı pornografi ve çocuk pornografisi alanına yöneliktir. Bunların başlıcaları; 1959 ve 1964 tarihli Müstehcen Yayınlar Kanunu, Çocukların Korunması Kanunu, Kamu Düzeni Kanunu, Cinsel Suçlar Kanunu, ve Ceza Adaleti Göçmen Kanunu dur (IWF, 2011a; OPSI, 2003,2008). Bu yasaların dışında ayrıca 1984 tarihli Telekomünikasyon Kanunu'nda yapılan değişikliklerle, "yayınlama" teriminin kapsamına bilişim sisteminde bulunan veriler de dahil edilmiş ve sanal alanda yapılan pornografik yayınlar da düzenlenme altına alınmıştır (Dülger, 2004: 97).

İngiltere'de, 1978 tarihli Çocukların Korunması Kanunu'nda yer alan fotoğraf tanımı, 1994 tarihli Ceza Adaleti ve Kamu Düzeni Kanunu ile sanal alanda sayısal formda veri halinde bulunan resimleri de kapsayacak şekilde değiştirilerek İnternette veri halinde bulunan çocuk pornografisi resimleri ve bunların montajla yapılmış şekillerini bulundurmak suç sayılmıştır (Dülger, 2004: 97-98).

2009'da yürürlüğe giren Ceza Adaleti Göçmen Yasası o zamana kadar suç olmayan extreme (aşırı, uç) yetişkin pornografisi bulundurmaya suç kabul ederek yaptırımlara bağlamıştır. Yasa'nın 62. ve devam eden maddeleri, extreme porno görüntülerinin bulundurulmasını iki yıla kadar hapis cezası veya para cezası ya da her ikisi ile birlikte cezalandırılmayı öngörmektedir. Yasa extreme pornografik görüntüleri; kişi yaşamını tehdit eden, cinsel organlarda veya vücutta ciddi yaralanma sonucu doğuran davranışlar, ölüye cinsel dokunuş içeren davranışlar ve ölü veya canlı hayvanla cinsel ilişki görüntüleri olarak açıklamaktadır (Cyberlaw, 2008).

İngiltere İnternet aktörlerinin sorumluluğu açısından AB'nin e-Ticaret Direktifi'ndeki ilkeleri aynen uygulamaktadır. Direktif, İngiltere'de 21 Ağustos 2002'de yürürlüğe girmiş ve e-Ticaret Direktifi'nin uygulanması için "İSS'ların Sorumluluğu İçin Uygulanabilir Direktif" adlı belge hazırlamıştır (Çağlar, 2011:122).

İSS'lerin sorumluluklarına, 1996 tarihli Birleşik Krallık İftira Yasası (Defamation Act)'nda da yer verilmiştir. Yasa'ya göre, İSS'lar içeriğin yazarı, editörü veya yayıncısı değilse, içerik açısından makul tedbirler almışlarsa ve doğuracağı sonuçlardan haberleri yoksa, içerikten sorumlu değildirler. Fakat, yasadışı içerik kendilerine bildirilmesine rağmen, bu içeriği engellemek hususunda yeterli ve gerekli girişimlerde bulunmazlar ve kusur işlerlerse bu durumdan sorumlu olurlar. Benzer şekilde sadece yer sağlama hizmeti veren İSS'lar içerik nedeniyle sorumlu olmazlar, fakat yetkililerin yasalara uygun olarak aldıkları kararlar çerçevesinde sunucuya müdahale olanağı sağlamakla yükümlüdürler (Akgün vd., 2002).⁵²

Diğer yandan, İngiltere'de İnternet içeriğinin düzenlenmesi konusunda tartışmalara neden olan başka bir yasal düzenleme de Dijital Ekonomi Yasası'dır. Telif hakları

⁵² Akgün vd., **a.g.e.**; İngiltere'de İSS'ların sorumluluğunun tartışıldığı ve yargılamaya konu ilk dava "Demon Davası"dır. Dava konusu olayda, 13 Ocak 1997'de haber ve tartışma sayfalarından birisine Dr. Godfrey hakkında gerçek dışı beyanlar ve hakaret içeren ifadelerin yer aldığı bir mesaj atılmıştır. Dr. Godfrey, faks çekerek İSS'yı uyarmış ve mesajın ilgili sayfadan çıkartılmasını istemiştir. Ancak Demon Şirketi hiçbir girişimde bulunmamış ve mesaj 15 günlük faal sürenin ardından kendiliğinden silinmiştir. Bunun üzerine Dr. Godfrey, kişilik haklarına saldırıdan doğan zararların tazmini için Demon Şirketi'ne dava açmıştır. Mahkeme dava sonucunda, 1996 tarihli İftira Yasası'nı dayanak göstererek, uyarıya rağmen hiçbir sebebi olmadan hukuka aykırı içeriğin web sitesinden kaldırılmasını temin etmediği için davalı İSS'nin sorumluluğuna hükmetmiştir (Soysal, 2005: 304-339).

ihlalleri, İnternet alan adları yönetimi, radyo ve televizyon hizmetleri, spektrum gibi konuları düzenleyen ve haberleşme sektörünün düzenleyici otoritesi olan Ofcom’a bir takım yetkiler tanıyan Yasa 7 Nisan 2010’da kabul edilmiştir (Legislation, 2010).

Özellikle, “İnternet bağlantısını geçici olarak durdurma” ve “erişimin engellenmesi” tedbirleri nedeniyle yoğun tartışmalara neden olan Yasa, Fransa’da başlayan ve daha sonra Avrupa’ya yayılan telif hakkı ihlallerinde “Three Strikes” modelini benimsemiştir. Bu modele göre, abone ilk ihlalde e-posta ile uyarılır, ikincisinde mektup gönderilir ve son olarak üçüncü kez yakalanırsa bir yıla kadar İnternet hesabı kesilebilir. Yasa’ya göre, İSS’ler telif hakkı ihlali yapan abonenin erişimini engellemekle yükümlüdür (Wikipedia, 2012d). Diğer yandan, İngiltere’de Facebook gibi sosyal ağ sitelerinin izlenerek kullanıcıların bağlantı detaylarının tutulması amacıyla düzenleme yapılması için de adımlar atılmaktadır (BBC, 25.03.2009).

2.5.2.3.2 İçerik Düzenleme Politikası

İngiltere’de İnternetle ilgili genel sorumlu kurum Kültür, Medya ve Spor Bakanlığı’dır. Bakanlığın görev alanları arasında “Telekomünikasyon Hizmetleri ve İnternet”, “Yayıncılık” ve “Medya Sahipliği ve Medya Birleşmeleri” de yer almaktadır (Culture, 2012a). “Telekomünikasyon Hizmetleri ve İnternet” başlığı altında belirtilen görevlerin bazıları şunlardır; İnternet politikası ve yönetimini (İnternet tarafsızlığı, güvenli İnternet ve telif haklarının korunması dahil) belirlemek ve uygulamak, dijital içerik (dijital oyunlar da dahil) sektörünü desteklemek, haberleşme sektörünün düzenleyici otoritesi olan Ofcom’u desteklemek (Culture, 2012b).

İngiltere’de bilgi ve iletişim teknolojilerinin bütün öğeleri tek bir bakanlık altında toplanmış; elektronik haberleşme ve yayıncılık hizmetleri, İnternet politikası, İnternet üzerinde telif haklarının korunması ve e-ticaret ile bilgi teknolojilerine ilişkin tüm hizmetler Kültür, Medya ve Spor Bakanlığı’nın görev alanı içinde yer almıştır. Ülkemizin aksine, İngiltere Ulaştırma Bakanlığı’nın sadece deniz, hava ve kara ulaşımına ilişkin yetkileri bulunmaktadır (DFT, 2012).

Aynı yaklaşımla İngiltere’de, bilgi ve iletişim hizmetlerindeki yakınsama nedeniyle hangi altyapının hangi hizmetlere ait olduğunun belirlenmesi ve işletmecilerin hangi hizmetleri sunabileceği konusunda problemler yaşanması üzerine, elektronik haberleşme ve medya alanlarını düzenlemek üzere tek bir kamu otoritesi olarak Ofcom 2002 yılında kurulmuş ve 2003’de İletişim Yasası yürürlüğe girmiştir. Bu kanun ile yayıncılık ve elektronik haberleşme düzenlemeleri tekrar tanımlanmış ve bu görevler Ofcom’a verilmiştir (Ofcom, 2012).

İngiltere’nin İnternet içeriğine müdahale konularını çocuk pornografisi, müstehcenlik ve ırkçılık söylemi oluşturmaktadır (Kaya, 2010: 60). Ülkede bu mücadele büyük oranda IWF (İnternet İzleme Kurumu) adındaki STK eli ile yürütülmektedir. Aynı zamanda bir ihbar merkezi de olan IWF, 1996’da, başlangıçta çocuk pornografisi, daha sonra ise ırkçılık ve extreme porno olmak üzere İnternette yasa dışı içerikle mücadele etmek amacıyla, İSS’ler, telekomünikasyon firmaları, GSM operatörleri, yazılım firmaları, polis teşkilatı, hükümet, adli merciler ve kamu ile ortak çalışmalar yapmak üzere İngiliz Hükümeti’nin desteğiyle kurulmuştur (IWF, 2012).

1999’da INHOPE’u kuran 8 üyeden birisi olan IWF, her ne kadar İngiltere’de yerleşik bir kurum gibi görünse de, aslında uluslararası bir kuruluş olarak faaliyet göstermektedir. Tüm dünyadaki İSS’ler, arama motorları, ve İnternet sektöründeki şirketlerin üyelik taleplerini kabul etmekte ve üye olmalarını teşvik etmektedir. Bu nedenle birçok uluslararası şirket IWF üyesidir. IWF resmi olarak üyelere aidat alırken, kurumlar ve kişilerden bağış toplamaktadır. Aidatlarının toplamı yıllık yaklaşık 1 milyon Euro’yu bulmaktadır. Ayrıca ihbar merkezine AB Safer Internet Plus Program tarafından da finansal destek sağlanmaktadır (IWF, 2012).

Üst düzey yöneticileri emekli polis teşkilatı mensuplarından oluşan ve bünyesinde hukukçu barındırmayan; içeriğin suç olup olmadığına hukukçu olmayan analistlerin karar verdiği IWF, Cinsel Suçlar Kanunu’na göre İngiltere’deki 52 polis teşkilatı ile imzalamış olduğu mutabakat zaptıyla, çocukların cinsel istismarına yönelik yayınları inceleyip işlem sürecini tetikleyebilmektedir. Bu mutabakat zaptı, İngiltere’de çocuk pornosuyla mücadele konusunda ayrıcalıklı bir yere sahiptir (OPSI, 2003; TİB, 2008).

IWF'nin bünyesinde hiçbir hukukçu bulunmamasına rağmen, çocuk pornografisi yanında ırkçılıkla ve extreme pornografik içerikle mücadele etmek amacıyla oluşturduğu kara listeler, İngiltere'deki tüm İSS'lere, mobil operatörlere, arama motorlarına gönderilmekte ve bunlar tarafından "gönüllü" olarak kullanılmakta ve erişimleri engellenmektedir. Bununla birlikte, hukuki alanda sorun yaşanırsa Adalet Bakanlığı'ndan hukuki destek alınmaktadır (TİB, 2008; Şen, 2009).

Nitekim, gönüllü olarak İnternet filtreleme uygulaması Avrupa'da ilk defa İngiltere'de başlamıştır. İngiltere'nin en büyük İSS'si olan British Telecom, İçişleri Bakanlığı'nın telkini ile 2004 yılı Haziran ayından itibaren "Cleanfeed" projesini uygulamaya koymuştur. Projeye göre, 1978 tarihli Çocukların Korunması Kanunu'na dayanarak, IWF tarafından resmi ve sivil İnternet aktörleri ile kolluk güçlerinin katkısıyla sürekli güncellenen bir kara liste oluşturulmuştur. British Telecom, bu kara liste ile dünyanın herhangi bir yerindeki çocukların cinsel istismarına yönelik içeriğe erişimi engellemektedir. İngiltere'de barındırılan içeriğin ise uyar-kaldır yöntemi ile kaldırılması sağlanmaktadır (OpenNet, 2006-2007b). Erişimin engellenmesi, kara liste ve içerik engellemesi mekanizmalarının ikisinin birlikte kullandığı iki aşamalı çalışan melez bir filtreleme sistemiyle gerçekleştirilmektedir (Clayton, 2012). Söz konusu sistemde, İnternet kullanıcılarına, bloke edilen içeriğe ilişkin herhangi bir bilgilendirilmede bulunulmamakta, bloke edilen sayfada sistem, "sayfa bulunamadı" (hata kodu 404) uyarısını vermektedir (Guardian, 07.02.2006).

Gönüllülük esasına göre işlediği söylenmesine rağmen ilerleyen zamanlarda, bu proje kapsamında uygulanan sistemin veya benzerlerinin diğer tüm İSS'lerce de uygulaması istenmiştir (OpenNet, 2006-2007b). Sonrasında bu filtreleme sistemi aşamalı olarak tüm İSS'ler tarafından uygulanmaya başlamıştır (Theregister, 18.05.2006).

"Cleanfeed" benzeri filtreme sistemlerinin diğer İSS'lar tarafından da "gönüllü" olarak kullanılmaya başlamasında İngiliz Hükümeti'nin ciddi baskıları olmuştur. Nitekim, British Telecom'un "Cleanfeed" sistemini servise vermesini müteakip, 2006 yılında, İçişleri Bakanı Vernon Coaker, tüm İSS'lardan, 2007 yılının sonuna

kadar “Cleanfeed” benzeri network seviyesinde içerik bloke platformu kurmalarını beklediklerini belirtmiş ve eğer hedeflerine İSS’larla işbirliği yaparak ulaşamazlarsa, IWF listesindeki web sitelerine erişimi engellemek için farklı seçenekleri değerlendireceklerini ifade ederek, İSS’ları üstü kapalı bir şekilde tehdit etmiştir (Theregister, 18.05.2006; LINX Public Affairs, 2006). Dolayısıyla, İSS’ların “gönüllülük”ü, “zorunlu gönüllülük”tür.

İngiltere’de, çocukların müstehcenlik ve online kumardan korunması amacıyla bu tür içeriklere erişim için yaş doğrulama sistemlerinin kullanılması zorunluluğu vardır. En yaygın yaş doğrulama yöntemi olarak ise, yüz-yüze doğrulama yöntemi çevrim dışı olarak uygulanmaktadır (OECD, 2011: 55).

Diğer yandan İngiltere’de, yapılan bilimsel çalışmaların sonucunda online pornografinin yaygınlığı ve toplum için oluşturduğu riskler nedeniyle bu içerikleri engelleyecek merkezi bir filtrenin uygulamaya konulacağı 2013 yılı Temmuz ayında Başbakan Cameron tarafından duyurulmuştur. Bu kapsamda, ülke çapındaki tüm İSS’lardan söz konusu filtreleme sistemini uygulayabilecek teknik altyapılarını Ekim ayına kadar hazırlamaları istenilmiştir. Bu yeni uygulama ile birlikte İngiltere’de artık yetişkinlere yönelik cinsel içerikli materyallerin İnternet üzerinden erişimi merkezi filtreleme ile tamamen engellenmiş olacaktır (Webrazzi, Bianet, 23.07.2013).

Mevcut aboneleri isteğe bağlı olarak, 2014 yılından itibaren yeni abone olan herkesi mecburi olarak filtre programına dahil etmeyi öngören bu uygulama, ülkemizde tamamen isteğe bağlı kılınan “Güvenli İnternet Hizmeti”nden daha ileri bir sistemi hayata geçirmiş olacaktır. Yani, bizdeki uygulamanın aksine, 2014 yılından itibaren yeni aboneler için filtreli sistem asıl, filtrenin dışında kalmak başvuruyla mümkün hale gelecektir. Fakat her halükarda “aşırı pornografi” olarak nitelendirilen içerikteki sitelere yine de erişim olmayacaktır (Webrazzi, Bianet, 23.07.2013).

Cameron, yeni uygulamayı açıkladığı konuşmasında, “Değişen şudur ki, uzun zamandır İnternet hakkında bir şey yapılamayacağını, belli bir yöneteni olmadığı için elimizden bir şey gelmeyeceğini düşünüyorduk.” diyerek bu politikanın geride

kaldığını belirtmiş ve “Resimleri yayımlayan insanları engellemeliyiz, bunlara erişenleri engellemeliyiz ve İnternet şirketlerinden bunları engellemek için ellerinden gelenin en iyisini yapmalarını istemeliyiz” ifadeleriyle zararlı İnternet içerikleriyle ilgili değişen yeni politikalarının ipuçlarını vermiştir (Bianet, 23.07.2013).

Bunun yanında IWF, içerik ve yer sağlayıcısının ülke içinde veya dışında olmasına bakmaksızın çocuk pornografisine yönelik her türlü içeriği engellemektedir. Hatta, ülkedeki İnternet kullanıcılarına, ihbar etmek için dahi çocuk pornografisi resimlerinin araştırılmasının mahkemeler tarafından geçerli bir savunma olarak kabul edilmediği uyarısında bulunmaktadır (IWF, 2011b). Ancak IWF, suç oluşturan extreme pornografi ile ırkçılığa ait içeriklerin engellenmesi için yer veya servis sağlayıcının İngiltere’de bulunması şartını aramaktadır. Bu içeriğin İSS’sı INHOPE üyesi başka bir ülkede ise, bu durum INHOPE kanalı ile ilgili ihbar merkezine iletilmektedir(Kaya, 2010: 60;TİB, 2008). Uygulamadaki bu farklılığın nedeni olarak, çocukların istismarının önlenmesinin uluslararası düzeyde kabul edilmiş standartlara sahip olmasına rağmen müstehcenlik ve ırkçılık söylemi için aynı ortak duyarlılığın ve standartların olmaması gösterilmektedir (Kaya, 2010: 60; Çamlı, 2010c).

IWF, ihbarlarda yasa dışı içerikle karşılaştığında İngiltere kaynaklı sitelerle ilgili olarak, içerisinde sadece site ekran görüntüsü ve İSS’sı gibi bilgilerin yer aldığı basit bir rapor hazırlanmakta ve içeriğin engellenmesi için ilgili İSS’sına ve polis teşkilatına bildirmektedir. Sektördeki şirketlerle kurulan özel bir alarm sistemi mekanizması sayesinde İngiltere’de barındırılan çocukların cinsel istismarı içerikleri uyar-kaldır metodu ile birkaç saat içinde kaldırılmaktadır. Uygulanan bu sistem ile mahkemelerin yükünü hafifletici bir ara oluşum gerçekleştirilmiştir (IWF, 2012).

IWF tarafından aynı zamanda çocukların cinsel istismarı ile ilgili alan adlarının alan adı kayıt kuruluşlarınca iptali sağlanmakta ve bu içeriklerin arama motorlarında bulunması engellenmektedir. Ayrıca, bir web sitesindeki birkaç yasadışı içerik için alan adından erişim engellemesi yapılmamakta, sadece içeriğin bulunduğu web bağlantı adresi, yani URL’si engellenmektedir. Sadece web sitesinin ağırlıklı içeriği yasadışı ise alan adından engelleme yoluna başvurulmaktadır (IWF, 2012).

IWF, İngiltere menşeli İSS'lar dışında sektördeki global aktörlerle de işbirliği yapmaktadır. Örneğin, Avrupa'nın en büyük, dünyanın 5. büyük IP trafik taşıyıcısı Teliasonera International Firması'yla, çocuk pornografisiyle mücadele amacıyla oluşturduğu kara listelerin bu firma tarafından kullanılması konusunda işbirliğine gitmiştir. Buna göre, 2008 yılından itibaren Teliasonera, müşterilerine (ISP'ler, mobil operatörler v.b.) kendi networkleri üzerinden bu kara listelerde yer alan siteleri engelleyecek ücretsiz bir çözüm sunmaya başlamıştır (IWF, 2012).

IWF, İnternet ortamında herkesin ulaşabildiği içeriklerle ilgilenmektedir. Herkesin ulaşamayacağı sohbet servisleri, P2P paylaşım ağları vb. çevrimiçi ortamlarda istismara maruz kalan çocuklar için IWF'e değil de CEOP (Çocuk İstismarı ve Çevrimiçi Koruma Merkezi)'e ulaşılması gerekmektedir. CEOP, İngiltere'de yerleşik, tüm adli merciler, İSS'ler, yer sağlayıcılar ve İnternet endüstrisi aktörleri ile sıkı bir işbirliği içinde çocukların çevrimiçi ortamda korunması konusunda faaliyet gösteren uzmanlaşmış bir kolluk kuruluşudur (CEOP, 2012).

İngiltere'de, yasadışı ve zararlı İnternet içeriği ile mücadelede etkin rol oynayan İSS'lar, Birleşik Krallık İnternet Servis Sağlayıcılar Derneği (ISPA-UK) adlı örgüt çatısı altında bir araya gelerek öz düzenleme çalışmalarını yürütmektedir. İSS'lar, sektörün daha iyi hizmet sunması, sorunlarına çözüm bulunması yanında İnternet aktörlerinin cezai sorumlulukları ile tabi olacakları hukuki rejimin ana ilkelerinin belirlenmesi konularında da çalışmalar yapmakta ve kendi koymuş oldukları kuralların sağlıklı bir şekilde işleyip işlemediğini yine kendi oluşturdukları bir kontrol mekanizması ile denetlemektedir (Akdeniz, 1996).

World Wide Web Consortium tarafından oluşturulan ve İnternet derecelendirme sistemi konusunda en bilinen öz düzenleme kuruluşu olan PICS, İngiltere'de oluşturulmuştur. PICS, İngiltere'de de kullanılmakta ve hükümetler ve İnternet aktörlerince desteklenmektedir (w3.org, 2011).

Dijital oyunlar konusunda Avrupa'nın en geniş, dünyanın ise ABD ve Japonya'dan sonra üçüncü büyük pazarı olan İngiltere'de (UIKE, 2011), dijital oyunlarla ilgili

olarak ise biri resmi diğeri STK iki düzenleyici kurum bulunmaktadır. Bir devlet kuruluşu olarak 1912 yılında filmleri sınıflandırmak için kurulmuş olan İngiltere Film Sınıflandırma Dairesi (BBFC), 1984 yılından bu yana dijital oyunları da sınıflandırmaktadır. BBFC, sinema filmlerini, video filmlerini ve dijital oyunları gençlerin ve toplumun ruh sağlığı ve ahlak yapısını korumak için incelemekte, denetlemekte ve sınıflandırmaktadır. Kurum, her üç kategoride de film yapımcıları, hukukçular, pedagoglar, psikiyatristler ve sosyologlardan oluşan kurullara başvurur. Kurum'un kararlarına itiraz hakkı mevcuttur. BBFC'nin oyunlarla ilgili sınıflamalar için içerikte dikkat ettiği hususlar, uyuşturucu, şiddet, korku ve cinselliktir (BBFC, 2011).

Dijital oyunlarla ilgili ikinci düzenleme kurumu, sektördeki yayıncılar tarafından, 2010 yılında kurulan Birleşik Krallık İnteraktif Eğlence Ortaklığı (UKIE)'dir. Dijital oyun sektörünün gelişimine katkı sağlamak için kurulan UKIE, geniş ölçüde PEGI modeli ile uyumlu bir dereceleme kriteri benimsenmiştir (UIKE, 2011).

Yine öz düzenleme yaklaşımı içinde AB'nin Güvenli İnternet Plus Programı çerçevesinde İngiltere'de güvenli İnternet konusunda bilinçlendirme çalışmalarını Birleşik Krallık Güvenli İnternet Merkezi (UKSIC) yürütmektedir. Merkez, IWF dışında Childnet International⁵³ ve South West Grid for Learning⁵⁴ adındaki iki STK ortaklığı ile oluşturulmuştur (UKSIC, 2012). Ülkede bilinçlendirme faaliyetleri yürüten başka bir STK da UK Council For Child Internet Safety'dir.⁵⁵

⁵³ 1995 de kurulan çocuklara yönelik bir yardım kuruluşu olup, İnternetin çocuklar için güzel ve güvenli bir yer haline getirilmesini kendisine misyon edinmiştir. Bu alanda politika geliştirmeye yönelik çalışmalar da yapan Kuruluş, Facebook'un Güvenlik Danışma Kurulu'nda da yer almakta ve eğitim alanında faaliyet de göstermektedir. Bu kurum, her yaştan çocukla görüşmek için okul ziyaretlerinde bulunmanın yanı sıra, çocuklar, ebeveynler ve öğretmenler için İnternetin güvenli ve sorumluluk alınarak kullanılmasına ilişkin yardım sağlayan bir dizi ödüllü web sitesi de geliştirmiştir. (Bkz. Childnet International, <http://www.childnet.com/> (14.05.2012))

⁵⁴ İngiltere'nin kuzeybatısındaki 15 yerel yetkili kurum tarafından finanse edilen SWGfL, bölgesinde bulunan devlet okullarına ve birçok diğerk eğitim kurumlarına güvenli geniş bant İnternet bağlantısı ve geniş bant öğrenme kaynakları sunmanın dışında, İngiltere'nin diğerk bölgelerinde profesyonellere, ebeveynlere ve çocuklara İnternetin güvenli olarak kullanılması ile ilgili öneriler, kaynaklar ve destek hizmetleri sağlamaktadır. (Bkz. South West Grid for Learning, <http://www.swgfl.org.uk/> (15.05.2012))

⁵⁵ Konsey, Hükümet, sektör firmaları, kolluk, akademi ve yardım kurumlarından 180 örgütün ve ebeveynler ve çocukları temsil eden grupların biraraya gelmesiyle oluşturulan ve amacı çocukların ve

İngiltere’de kimi olaylar üzerinden İnternet içerik düzenlemesine ilişkin konularda bazı tartışmalar yaşanmaktadır. 2008 yılında online ansiklopedi Wikipedia’nın erişiminin engellenmesi bunlardan birisidir. Scorpions müzik grubunun “Virgin Killer” adlı albümünün kapağında çıplak bir kız çocuğunun resmini kullanması ve bu albümün Wikipedia’nın sayfasında yayınlanmasından sonra bu içerik sebebiyle IWF’nun, 5 Aralık 2008 tarihinde Wikipedia’nın ilgili sayfasını URL engellemesi tekniği kullanarak engellemesiyle, İngiltere’de İnternet içeriğine yönelik gerçekleştirilen müdahalelerle ilgili yoğun tartışmalar yaşanmıştır (Wikipedia, 2011d). IWF, söz konusu resmin sanatsal amaçlarla kullanıldığı ve engellenmenin ifade hürriyetine aykırılık teşkil ettiğine yönelik yoğun tepkiler ve itirazlar gelmesi üzerine, Wikipedia üzerindeki erişim engelleme kararını kaldırmıştır. Bu kararın alınmasına ise, bu içeriğin potansiyel bir ihlal içermesine rağmen resmin uzun süredir ve yaygın olarak İnternette yer almasını gerekçe göstermiştir (IWF, 2011c).

Bir diğer olay ise, Birmingham Şehir Meclisi’nin kullandığı filtreleme yazılımının büyü, ateizm ve satanizm ile ilgili içerikleri engellemesiyle ortaya çıkmıştır (BBC, 29.06.2008). Bu yazılımın sadece meclisin kendi ağında kullanılmasına rağmen, düzenlemeyle çalışanlar arasında dinsel ayrımcılık yapıldığı gerekçesiyle eleştirilere neden olmuş ve hukuka aykırılığı iddia edilmiştir (Kaya, 2009: 66).

Sonuç olarak İngiltere’de, İnternet yayınlarına yönelik özel düzenleme bulunmayıp, gerçek hayatta suç olan İnternette de suç olarak görülmektedir. Bunun yanında, değişik yasal düzenlemelerle çocuk istismarı, ırkçılık, aşırı pornografi türlerine ait içerikler konusunda ve bu çerçevede İnternet aktörlerinin sorumluluklarına ve telif haklarına ilişkin mevzuat oluşturulmuştur.

İngiltere’de yasadışı ve zararlı görülen çocuk istismarı, ırkçılık ve aşırı pornografi türlerine ait içeriklerle mücadele büyük oranda bir STK olan IWF tarafından yapılmaktadır. Bir ihbar merkezi de olan IWF bu mücadeleyi, bir kısmı aynı

gençlerin İnternet ortamında güvenliklerini sağlamak için işbirliği içinde çalışmak olan bir kuruluştur. UKCCIS’in üyeleri arasında, bazı üniversiteler, medya kuruluşları, Childnet International gibi yardım kuruluşları, Adalet, Eğitim gibi bazı bakanlıklar, Cisco, Apple, Sony, Vodafone, Yahoo!, Google, Facebook, Myspace, Microsoft gibi şirketler bulunmaktadır. (Education, 2012).

zamanda üyeleri de olan İSS'ler, telekomünikasyon firmaları, GSM operatörleri, yazılım firmaları, polis, hükümet ve kamu ile ortak çalışmalarla gerçekleştirmektedir. Söz konusu içeriklerle mücadelede İSS'ların daha çok “zorunlu gönüllü” oldukları bir sistem uygulanırken; uygulamalarda daha ziyade uyar-kaldır sistemi tercih edilmekte fakat bunun yanında, IWF'nin hazırladığı kara listeye göre filtreme de yapılmaktadır. Ayrıca, diğer öz düzenleme araçları olan bilinçlendirme faaliyetlerine ve içerik derecelendirme çalışmalarına önem verilmekte ve teşvik edilmektedir.

Son tahlilde İngiltere uygulamasında içerik düzenlemesine ilişkin kamu politikalarındaki popüler söylemin öz düzenleme yaklaşımının benimsendiği yönünde olsa da, dikkatlice incelendiğinde, sistem içinde devlet ile sektör aktörlerinin ve STK'ların ortak düzenleme yaklaşımı içinde hareket ettiklerine şahit olmaktadır. Dolayısıyla, İnternet içerik düzenlemesi konusunda İngiltere uygulaması yeni bir “birlikte düzenleme” ve “yönetişim” örneği olarak karşımıza çıkmaktadır.

2.5.2.4 Fransa

Fransa 52 milyon İnternet kullanıcısı ile %80'e yaklaşan İnternet kullanımı oranına sahiptir (internetworldstats, 2012e). Fransa'nın, yasadışı ve zararlı içerikle mücadele konusunda temel ilkeler bağlamında AB normlarına uyum sağlamakla birlikte, ulusal ölçekte uyguladığı politikalar açısından kendisine özgü özellikleri de bulunmaktadır.

2.5.2.4.1 Yasal Çerçeve

Fransa'da, İnternetle ilgili ceza hukuku alanında özel bir yasa bulunmamaktadır. Fransız yasa koyucular İnternetle ilgili özel bir Kanun hazırlamak yerine ceza mevzuatını İnterneti de kapsayacak şekilde geniş olarak ele almayı tercih etmişlerdir (Kangal, 2001: 228). Örneğin, İnternetin ortaya çıkardığı hukuki sorunlara ilişkin olarak 1994 tarihli Yeni Fransız Ceza Yasası'na bakıldığında, bu yasada öngörülen bazı suç tiplerinin, İnternet aracılığıyla işlenmeleri olasılığı da göz önüne alınmak suretiyle hazırlandığı sonucuna varılabilmektedir (Sınar, 2001: 98).

Nitekim, söz konusu Yasası'nın 227/24. maddesi, şiddet ve pornografi içeren ya da insan onurunu ağır bir şekilde rencide eden bir içeriğin, hangi araçla olursa olsun çocuklar tarafından erişilebilir kılınmasını 3 yıl hapis ve 500 bin Frank para cezası öngörmüştür. 227/23. maddesi ise, çocuk pornografisini ele alarak; çocukların kullanıldığı pornografik materyallerin üretimi ve yayılmasını suç olarak düzenlemiş ve çocuk pornografisi içerikli bir resim, video, çizim, imaj vb. temsili çocuk görüntülerinin yayılması amacıyla muhafaza edilmesi, kayıt altında tutulması veya nakledilmesini cezai müeyyideye bağlamıştır. Suça konu eylemin teşebbüs aşamasında kalması durumunda da aynı cezai müeyyide öngörülmüştür. Buna göre suçun cezası, görüntülerin 15 yaşından küçük çocuklara ait olması durumunda 3 yıl hapis 500.000 Frank para cezası, 15 yaşından büyük çocuklara ait olması durumunda ise 1 yıl hapis ve 300.000 Frank para cezası olarak belirlenmiştir (Legifrance, 1994).

Bunun yanında, Fransız Ceza Yasası'nda, pornografik içerikten ne anlaşılması gerektiğine yönelik herhangi bir tanıma yer vermediği de görülmektedir. Fransa Anayasa Konseyi (Conseil Constitutionnel de France) ise açık bir pornografi tanımı yapmasa da verdiği bazı kararlarda pornografiyi belirleme yoluna gitmiştir. Buna göre, Mahkeme sapkın, cinsel şiddet içerikli, hayvanların kullanıldığı, sado-mazoşist nitelikli, ikiden fazla kişinin birbirleriyle aynı anda giriştikleri cinsel ilişki temsillerinin pornografik olduğunu kabul etmiştir (Özbek, 2009: 34).

Fransa'da İnternet içeriğine ilişkin ikinci temel müdahale nedeni telif haklarına yönelik ihlallerdir. Ülkede telif haklarının ihlallerine ilişkin ilk düzenleme 2006'da DADVSI (Bilgi Toplumunda Telif Hakları Ve Benzer Haklar Hakkında Yasa)'dır (Legifrance, 2006). Sarkozy Hükümetinin İnternette içerik indirmeye karşı hapis ve ağır para cezası getiren hükümler eklediği Yasa, Fransa Anayasa Konseyi tarafından hukuki eşitlik ilkesini ihlal ettiği gerekçesiyle iptal edilmiştir (Uçkan, 2009).

Daha sonra uzun süren tartışmaların ardından 13 Haziran 2009'da müzik endüstrisinin baskısıyla takma ismi HADOPI olan "İnternet Üzerinde Fikri Eserlerin Dağılımı Ve Korunmasını Teşvik Kanunu" yasalaşmıştır. Yasa ile İnternet ortamında fikir ve sanat eserlerinin korunması amaçlanmış ve İnternette yapılan

yasadışı müzik, video ve programların paylaşımının önüne geçilmeye çalışılmıştır. Bunun için Yasa ile fikri mülkiyet ihlallerinin cezalandırılmasına ilişkin erişimin engellenmesi ve para cezası gibi hükümler getirilmiştir (Legifrance, 2009a).

Yasa “Three strikes” sistemini benimsemiştir. Buna göre yasadışı içerik indiren aboneler bu uygulama için özel olarak kurulan HADOPI tarafından ilk olarak mail ile, 6 ay içinde indirme işlemi yine gerçekleşirse ikinci olarak mektup gönderilerek uyarılacaktır. Buna rağmen kullanıcının indirme işlemi devam ederse müşterinin İnternet erişimi bir yıla kadar askıya alınabilecektir. Yine sonuç alınamazsa konu yargıya taşınacaktır (FRANCE24, 10.06.2009).

Ancak, Yasa Anayasa Konseyi tarafından idari bir otoriteye cezai yaptırım yetkisinin devrinden dolayı Anayasası’nın “güçler ayrılığı” ilkesiyle çelişmekte olduğu ve anayasal bir hak olan ifade ve iletişim özgürlüğünün ihlaline neden olduğu gerekçesiyle 10 Haziran 2009’da iptal edilmiştir. Anayasa Konseyi’nin, gerekçede belirttiği “kamu haberleşme servislerine online ücretsiz giriş insan hakkıdır ve bireylerin bu hakkı sadece hakim kararıyla engellenebilir” görüşü üzerine Hükümet, Yasa’da yaptığı değişiklik ile HADOPI’ye verilen İnternet aboneliğini askıya alma yetkisini sadece hakimlerin tasarrufuna bırakmıştır. Bu değişiklik ile Yasa 22 Ekim 2009 tarihinde Anayasa Konseyi’nin onayından çıkmıştır (FRANCE24, 10.06.2009). Buna rağmen HADOPI Yasası ve beraberinde getirdiği uygulamalar Fransa’da yoğun tartışmaların ve eleştirilerin odağı olmaya devam etmiştir (Uçkan, 2009).

Fransa’da İnternetle ilgili diğer bir düzenleme ise, Sarkozy’nin İçişleri Bakanlığı döneminde Loppsi 2 (İç Güvenlik Performansı İçin Kılavuzlar Ve Programlama İle İlgili Kanun) ismini almış 15 Mart 2011 tarihli yasadır (Legifrance, 2011a). Yasa, hazırlık aşamasında siber suçlarla ilgili “özel bir mesele için bir istisna” olarak sunulmuştur (Silicon (2009). Yasa’nın 4. maddesiyle, Fransız Ceza Kanunu madde 227-23’de yer alan çocuklara ait pornografik resim veya temsillerin yayılmasıyla mücadele hükmü çerçevesinde İSS’lara, idari makamların konuyla ilgili bildirimde bulunmaları durumunda içeriği derhal kaldırma yükümlülüğü getirilmiştir (Legifrance, 2011). Böylece kamu idaresine İSS’lar üzerinden çocukların

korunmasına yönelik olarak herhangi bir yargı kontrolü olmaksızın İnternet sitelerine erişimi engelleyebilme yetkisi verilmiştir. Yasa, hem çocuk pornografisiyle mücadelede çözüm olmayacağı, hem de yargısal kontrolü devredışı bıraktığı için Anayasa'ya aykırılık gerekçesiyle eleştirilmiştir. Ayrıca Yasa, diğer maddelerinde yer alan ve güvenlik gerekçesiyle emniyet güçlerine verdiği geniş yetkilerle elektronik gözetimi güçlendiren düzenlemeleri açısından da yoğun eleştirilere neden olmuştur (Antiloppsi2, 2012; Edri, 2011a; Zeropaid, 2009).

Loppsi 2, yürürlüğe girdikten sonra Anayasa'nın ifade ve iletişim özgürlüğünü düzenleyen maddelerine aykırı olduğu gerekçesiyle Anayasa Konseyi'ne iptal davası açılmıştır. Yüksek Mahkeme, 10 Mart 2011 tarihinde Yasa'nın Anayasaya aykırı olmadığına ilişkin kararını açıklamıştır. Kararın gerekçesinde, Yasa ile kamu idaresine verilen yetkinin kamu düzenini sağlamakla ilgili görevlerine yönelik olduğu ve bu durumun ifade ve iletişim özgürlüğünün anayasal hedefleri ile arasında orantısızlık oluşturmadığı ifade edilmiştir (Edri, 2012; Legifrance, 2011b).

Fransa da Almanya gibi ırkçı İnternet içeriğine müdahalede bulunmaktadır. Bunun en bilindik örneklerinden birisi Yahudi Öğrenciler Birliği ve ırkçılık karşıtı LICRA adlı örgütün 2000'de Yahoo'ya karşı açtığı davadır (EFF, 2004). Bu iki kuruluşun Yahoo'ya dava açma sebebi, Yahoo'nun online açık arttırma sitesinde Nazi hatıraları koleksiyonu satmasıdır. Davacılar bunun her türlü Nazi eşyasının Fransa'da satışını yasaklayan yasalara aykırı olduğunu iddia etmişlerdir (BBC, 23.05.2000). Yahoo yetkilileri, Fransız mahkemesinin yetkisine itiraz ederken İnternete devletlerin müdahalesiyle ilgili çok temel bir soruna değinmiş ve şu savunmayı yapmıştır: Eğer Fransız hukuku Amerika'daki bir web sitesine uygulanabiliyorsa, aynı şekilde Alman, Japon, Suudi ve Çin hukuku da uygulanabilir. Bu durumda şirketler tüm zamanlarını uygulanacak hukuku tespit etmekle geçirecekler ve ticaret yapamaz hale geleceklerdir (Goldsmith ve Wu, 2006; 2).

Ancak Mahkeme, Yahoo'nun Fransız ziyaretçilerin Nazi ürünlerini görüntülemesini engellemekle yükümlü olduğuna hükmetmiştir. Mahkeme, Yahoo'nun IP analizi yaparak Fransa'dan bağlanan kullanıcıların %90'ını tespit edebileceğine, dolayısıyla

bu yükümlülüğü yerine getirebilecek kabiliyette olduğu sonucuna varmış ve bu yükümlülüğü yerine getirmek için tedbir almaması halinde cezai müeyyide uygulanmasına ve Fransa'daki Yahoo ofisinin gelirlerine el konulmasına karar vermiştir (BBC, 23.05.2000). Yahoo, Fransız mahkemesini yetkisiz kabul etse de Fransa'daki yatırımlarını riske atmamak için, kullanıcılarının IP adreslerine bakarak ve kullanıcılardan da bulundukları ülkeyi doğrulamalarını isteyerek Fransız ziyaretçilerinin söz konusu içeriklere erişimini zorlaştırmıştır (Kaya, 2010: 38).

Bu olayın ardından 2001 yılında ABD Kuzey Kaliforniya Bölge Mahkemesi Yahoo'nun başvurusu üzerine, söz konusu şirketin ırkçılıkla ilgili olarak Fransız kanunlarına uyması konusunda zorlanamayacağına; çünkü bu durumun ilgili şirketin ABD kanunlarındaki ifade özgürlüğüne yönelik düzenlemelerdeki haklarına aykırılık teşkil ettiğine karar vermiştir (Computerweekly, 2001).

Fransa'da, online kumarla ilgili bir yasal düzenleme de bulunmaktadır. Sektördeki rekabeti sağlama ve sektörü düzenleme amacıyla çıkarılan 13.05.2010 tarihli Kumar ve Online Kumar Yasası, online oyunları düzenleme otoritesi olarak kurulan ARJEL'e yasadışı kumar sitelerine karşı önlem alma yetkisi vermiştir (Legifrance, 2010). Bu çerçevede ARJEL, İSS'lara başvurmakta ve mahkeme kararına ihtiyaç olmaksızın bu sitelere erişimin engellenmesini talep etmektedir (ARJEL, 2012).

Fransa, terörizm ile mücadele gerekçesiyle çıkarttığı 24.11.2006 tarihli anti-terör yasası ile İSS'lar, İnternet kafeler, yer sağlayıcıları ve cep telefonu operatörlerine trafik verilerini bir yıl süreyle saklama ve bu verilerin paylaşımı konusunda emniyet güçleriyle işbirliği yapma zorunluluğu getirmiştir. Hükümetin terörist eylemleri önlemek için gerekli gördüğü bu düzenleme, Fransa kamuoyunda yoğun tartışmalara ve insan hakları örgütlerinin eleştirilerine neden olmuştur (Edri, 2006).

Fransa'da, AB e-Ticaret Direktifi'ne uyum sağlamak için 2004'te Dijital Ekonomide Güven Yasası (LCEN) çıkartılarak İnternet aktörlerinin yükümlülük ve sorumlulukları belirlenmiştir. Yasa'ya göre, içerik sağlayıcılar suç teşkil eden yayınlardan dolayı genel kurallara göre sorumlu olurken, yasadışı içeriğin yayına

hazırlanmasında veya konulmasında katkısı bulunan kişiler de suça iştirak kurallarına göre sorumlu tutulacaktır. Erişim sağlayıcılar ise sadece verileri taşıyan konumunda olmaları nedeniyle ceza sorumluluğu getirilmemiş, fakat bazı hizmetleri ayıklamaya yarayan teknik olanakları kullanıcılara bildirmekle yükümlülü kılınmışlardır (Legifrance, 2004a; Turan, 2006: 94).

Yasayla, metin, resim, ses ya da her türlü dijital veriyi depolayarak halkın erişimine sunan gerçek ve tüzel kişiler, bu işi ücretsiz dahi yapsalar yer sağlayıcı olarak kabul edilmiştir. Dolayısıyla içeriklerini incelemenden yayımlayan Youtube, Dailymotion, Facebook gibi bloglar, tartışma forumları, sosyal paylaşım siteleri bir siteyi barındırmaları dahi yer sağlayıcı sınıfına dahil olmuşlardır ve yöneticileri Yasayla gelen sorumluluklardan etkilenmektedirler (Ichay&Mullenex, 2004).

LCEN, uyar-kaldır yönteminin sağlıklı olarak işlemesini sağlamaya çalışmaktadır. Buna göre, gerçek veya tüzel kişi yasadışı bir faaliyetin veya bilginin farkına vardığında yer sağlayıcıya durumu bildirir; yer sağlayıcı içerik sağlayıcıyla irtibata geçtiğini ve içerik ile ilgili gerekenin yapılmasını istediğini veya içerik sağlayıcıya ulaşmaya çalışıp ulaşamadığını ispat edebilmelidir (Ichay&Mullenex, 2004).

Yasa'ya göre, yer sağlayıcıların, barındırdıkları içeriklerin yasal olup olmadıkları konusunda araştırma yapmak gibi bir sorumlulukları olmamakla birlikte; içerik sağlayıcıların kayıtlarını tutma, insanlık suçları, ırkçılığa teşvik ve çocuk pornosuyla mücadele etmek ve bu kapsamda kullanıcıları haberdar etmek için herkesin kolayca ulaşabileceği görülebilir bir bilgilendirme mekanizması oluşturma, kendisine gelen yasa dışı içerikle ilgili bildirimleri ilgili birimlere iletme ve yasadışı içeriklerle mücadelede ne tür araçlar kullandığını yayınlama görevleri bulunmaktadır (Ichay&Mullenex, 2004).

Yasa'ya göre yer sağlayıcı, içerik sağlayıcının veya herhangi bir içeriği oluşturanın kişisel bilgilerini tutmaması veya insanlık suçları, ırkçılığı teşvik, çocuk pornosuyla mücadele konusunda üzerine düşen yükümlülükleri yerine getirmemesi durumunda bir yıl hapis ve 75 bin €'luk para cezası ödemek zorundadır (Ichay&Mullenex, 2004).

Fransa’da yer sağlayıcılarla ilgili olarak 01.03.2011’de, video paylaşımı ve blog barındırma hizmetleri de dahil olmak üzere yer sağlayıcı şirketlerin, çevrimiçi içeriklerin bir yıl süre ile log kayıtlarının tutulmasına ilişkin bir kararname yayınlanmıştır. Buna göre içeriğin oluşturulması, değiştirilmesi, silinmesi, yapılan işlemler, bağlantı ve içerik transferlerinin tarih ve saatleri, kullanılan protokoller vb. trafik bilgilerinin bir yıl süre ile ilgili yer sağlayıcı tarafından kayıtlarının saklanması zorunluluğu getirilmiştir. Ayrıca, bir hesap silindikten sonra bir yıl süre ile bu hesaba ait kullanıcı adı, adresi, e-posta ve ilişkili adresleri, telefon numaraları, şifresi, rumuzu, abone hattı özellikleri gibi kişisel bilgilerin yanında, ücretli abonelerin ödeme yöntemine ilişkin veriler, ödenen miktar ve tarih ve işlem saati gibi bilgilerin de saklanması istenilmektedir (Legifrance, 2011c). Bu Kararname de İSS’lar ve yer sağlayıcılardan tepki görmüş ve haberleşmenin gizliliğine ve kişisel verilerin korunması ilkesine aykırı olduğuna ilişkin eleştirilere neden olmuştur (Edri, 2011b).

2.5.2.4.2 İçerik Düzenleme Politikası

Yasal düzenlemelerden de anlaşılacağı gibi Fransa’da çocuk pornografisi, ırkçılık, insanlığa karşı işlenen suçlar, telif hakları ihlalleri, yasadışı online kumar, terör aktiviteleri, şiddete özendirme gibi İnternet içerikleri ile mücadele yürütülmektedir. Fransa’da İnternetle ilgili değişik niteliklere sahip düzenleyici kurumlar, danışma kurulları, kolluk güçleri ve bazı öz düzenleme kuruluşları bulunmakla birlikte, genel olarak yasadışı içerikle mücadeleyi büyük oranda kamu kurumları yürütmektedir.

Ülkede yasadışı ve zararlı İnternet içeriğiyle mücadele konusunda özerk düzenleyici idari otorite olarak ön plana çıkan üç önemli kamu kurumu bulunmaktadır. Bunlardan ilki HADOPI Yasası’na dayanarak, İnternet ortamında fikir ve sanat eserlerinin korunması için çalışmalar yapmak üzere aynı yıl kurulan HADOPI’dir. HADOPI, Yasa’nın kendisine verdiği yetkiye dayanarak İnternet içeriğini telif hakkı boyutu ile izlemekte ve “Three strikes” sistemini uygulamaktadır (HADOPI, 2012).

Fransız İSS’lerinden Bouygues Telecom ve Numéricable, 2010’da şüpheli yasa dışı dosya paylaşımı yapan Fransa’daki abonelerine HADOPI otoritesi adına ilk uyarı e-

postalarını göndermiştir. Uyarı yazısında, İnternet bağlantısının suç işlemek amacıyla kullanıldığı bunun da kanunu ihlal anlamı taşıdığı ifade edilirken, korsanlığın ekonomi ve kültürel sektör için ciddi bir tehdit olduğu belirtilmiştir (Edri, 2010).

HADOPI'ye, kullanıcılar için yasal indirme sitelerini belirleyerek etiketleme yapma, telif hakları açısından bilinçlendirme ve eğitim faaliyetleri yürütme, göstergeleri izlenme, filtreleme teknolojileri ve içerik tanıma, teknik koruma önlemleriyle ilgili düzenleyici öneriler geliştirme görevleri de verilmiştir (Legifrance, 2009b).

HADOPI düzenlemesi ve uygulamaları Fransa'da yoğun tartışmalara ve eleştirilere neden olmuştur. İnsan hakları örgütleri Fransa'nın telif hakkı ihlallerini kamuflaj olarak kullandığını ve asıl amacın İnternet trafiğini istihbarat amaçlı denetlemek olduğunu iddia etmektedirler (Berber ve Kaya, 01.12.2010: 9).

Fransa'da yasadışı İnternet içeriğiyle mücadele konusunda ikinci önemli düzenleyici kurum ARJEL (Online Oyunları Düzenleme Otoritesi)'dir. Kumar ve Online Kumar Yasası'yla kurulan ARJEL'e, yasadışı online kumar sitelerine karşı önlem alma yetkisi verilmiştir. Buna göre, online oyun piyasasını düzenlemek için lisans vermek, yasal ve çevrimiçi operatörleri izlemek ve kontrol etmek ve İçişleri ve Adalet Bakanlıklarının ilgili birimleriyle işbirliği içinde yasadışı online kumar sitelerine karşı mücadele etmekle görevlidir. Keza, küçükleri koruma, dolandırıcılık, kara para aklama ve kumar bağımlılığıyla mücadele de görevleri arasındadır (ARJEL, 2012).

ARJEL, yasadışı online oyun siteleri için ilgili İSS'lara başvurmakta ve mahkeme kararına ihtiyaç olmaksızın bu sitelerin engellenmesini talep edebilmektedir. İlgili İSS kendisine iletilen bu talebi yerine getirmek için teknik imkanlarını yeterince kullanmaz ve erişimi engellemezse her gün için 100 bin € ceza verilebilmektedir. ARJEL'e verilen bu yetki İSS'lar tarafından eleştirilirken bu çerçevede İSS'lar ile Kurum arasındaki bazı anlaşmazlıklar taraflar arasında davalara konu olmaktadır (Edri, 2011c; Numerama, 2010).

Yasa'yı eleştiren bazı STK'lar bu uygulamanın başlangıçta kumar siteleri için düşünülse de daha sonra istenilmeyen diğer içerik türlerini de kapsayacak

engellemelere ve özgürlük sınırlamalarına kapı aralayacağı endişelerini dile getirmektedir. Öte yandan, söz konusu uygulamada IP engellemesi tekniği kullanıldığı için aynı IP'den İnternete çıkan diğer masum içeriklerin de engellenmesine neden olunduğuna dikkat çekilmektedir (Edri, 2009a).

Anti Terör Yasası, HADOPI, Loppsi 2 ve ARJEL uygulamaları Fransa'da İnternet içeriğine müdahalede bulunmayı sansür ile özdeş gören ve bu tür karar ve uygulamalara şiddetle karşı çıkan muhalif bir hareketin oluşmasına sebebiyet vermiştir. Bu muhalif hareketin iki önemli temsilcisi “La Quadrature du Net İnisyatifi” ve “Korsan Parti” dir. “La Quadrature du Net İnisyatifi” 2005'ten bu yana örgütlenerek HADOPI, Loppsi ve ARJEL karşıtı protestolarla güç kazanmıştır. Bu arada 2007'den günümüze İsveç'ten başlayarak büyük bir ivmeyle Avrupa genelinde örgütlenmeye başlayan Korsan Parti, HADOPI rüzgarını da arkasına alarak Fransa'da da kurulmuş ve büyümüştür (Uçkan, 2009). Bu muhalif hareket, Sarkozy'in başını çektiği Fransız Hükümetlerinin telif hakları ihlalleri, terörizm, çocuk pornografisi, yasadışı kumar bahaneleriyle tüm dijital iletişimi izleme ve dinlemeye ve İnternet sansürüne yasal kılıf oluşturduğunu ve bu durumun Fransız hukuk sistemi tarafından sindirildiğini ifade etmektedir (Uçkan, 2009).

Fransa'da İnternet düzenlemeleri konusunda ön plana çıkan üçüncü özerk düzenleme kurumu ise CNIL (Bilişim ve Özgürlükler Ulusal Komisyonu)'dir. 1978 tarihli Yasa ile doğan ve 2004'teki değişikliklerle yapısında ve görevlerinde önemli oranda revizyona uğrayan CNIL, bünyesinde kısmi olarak sektör temsilcilerine de yer vermektedir. “Bilgi teknolojilerinde insan kimliğine, insan hakları, mahremiyet ve özgürlüklere saygı” sloganını kullanan CNIL, kişisel verilerin gizliğinin sağlanması ve bireysel özgürlüklerin korunması için görev yapmaktadır (Legifrance, 2004b).

CNIL bu çerçevede, kişilerin bilgi teknolojilerini kullanırken hak ve özgürlükleri ile sorumluluklarının farkına varmalarını sağlamaya ve güvenlik açısından nelere dikkat etmeleri gerektiği konusunda bilgi sahibi olmalarına yönelik eğitim ve bilinçlendirme çalışmaları yaparken, sektörün de bu konulara ilişkin teknik ve idari tedbirler alması, kişilerin bu yöndeki taleplerini karşılaması için standartlar belirlemek, düzenlemeler

yapmak, kontrol ve denetimler gerçekleştirmek, yaptırımlar uygulamak ve etiketleme yapmak gibi faaliyetleri de yürütmektedir. Kurum, görev alanıyla ilgili olarak İçişleri ve Adalet Bakanlıkları yanında benzer uluslararası örgütlerle işbirliği yapmakta ve teknolojik gelişmeleri de takip ederek yeni politikalar oluşturulması hususunda teklif ve öneriler geliştirmektedir (CNIL, 2012a).

CNIL, ülkede faaliyet gösteren İnternet sektöründeki küresel ve yerel aktörlerin, sosyal ağların kişisel verilerin gizliliğinin sağlanması ve bireysel özgürlüklerin korunması açısından yapmış oldukları çalışmaları ve güvenlik politikalarını izlemekte ve denetlemektedir (CNIL, 2012b). Ayrıca web sitesinde, çevrimiçi şikayetlerin de değerlendirildiği, görev alanıyla ilgili şikayetleri aldığı ve bilgi ve destek hizmeti sunduğu bir de “alo CNIL” hattı bulunmaktadır (CNIL, 2012c).

Bu üç düzenleyici idari otoritenin dışında Fransa’da doğrudan İnternete yönelik olmasa bile genel olarak bilgi teknolojileri ve iletişim alanının düzenlenmesi ile ilgili başka özerk düzenleyici kurumlar da bulunmaktadır. Bunların en önemlileri ARCEP (Elektronik İletişim Ve Posta Hizmetleri İçin Düzenleme Kurumu) ve CSA (Yüksek Görsel-İşitsel Konsey)’dir. Görevleri itibarıyla ARCEP, Türkiye’deki, TİB hariç, Bilgi Teknolojileri ve İletişim Kurumu (BTK)’nun, CSA ise, Radyo Televizyon Üst Kurulu (RTÜK)’nun muadili sayılabilir (ARCEP, 2012; CSA, 2012).

Fransa’da yakın zamanda ARCEP ve CSA’nın merkezinde yer aldığı yeni bir içerik düzenlemesi tartışması yaşanmaktadır. Sarkozy’den sonra iktidara gelen hükümetin de İnternet üzerindeki kontrolü güçlendirecek yeni bir takım adımlar atmayı planladığı dile getirilmektedir. Başbakan Ayrault’ın İnternet içeriklerini bir tür medya yayını olarak kabul ederek bu çerçevede HADOPI’nin yetkilerinin CSA’ya aktarılmasını ve ikisinin birleştirilmesini planladığı ve yasadışı içerikle ilgili mücadelenin bir merkezi ağ kontrolü ile CSA ve ACREP üzerinden yürütülmesine ilişkin bir düzenleme üzerinde çalıştığından bahsedilmektedir. Ayrault, bu çalışmanın gerekçesinde bilgi ve iletişim teknolojileri arasında giderek artan yakınsama özelliğine vurgu yapmaktadır (Numerama, 2012).

“La Quadrature du Net İnisiyatifi” ise, İnternet üzerinde içerik yayınlamanın herkesin ifade ve demokratik katılım özgürlüğünün bir parçası olduğunu vurgulamakta ve İnterneti bir tür televizyon yayını olarak görmenin yanlış olduğunu, bu yaklaşımın Televizyon gibi İnternet için de yakın idari bir kontrol ve sansür düzenlemesi getireceğini ifade etmektedir (Laquadrature, 2012).

Yukarıda bahsi geçen kurumların dışında Fransa’da yasadışı İnternet içeriğiyle mücadele konusunda kolluk gücü olarak görev yapan iki önemli kamu kurumu daha vardır. Bunlardan birisi olan STRJD (Ulusal Jandarma Hukuki Araştırma ve Belgelendirme Teknik Servisi/Siber Suçlarla Mücadele Birimi) çocukların cinsel istismarını önleme konusunda uzmanlaşmıştır (Gendarmerie, 2012). Diğeri ise, siber suçlarla ilgili ve bu konuda uluslararası taleplerin iletişim noktası olan polis birimi OCLCTIC (Bilgi Teknolojileri ve İletişim Merkez Ofisi/Merkezi Adli Polis Bölümü)’dür (Police-Nationale, 2012).

Görüldüğü gibi Fransa’da İnternet içeriğinin düzenlenmesi ile ilgili bahsi geçen tüm idari otoriteler kamu kurumu niteliğindedir. CNIL’de kısmen yer almakla birlikte kurumsal yapılarında sektörel temsil söz konusu değildir. Birazda bu eksiklik görüldüğünden olsa gerek ülkede 29 Nisan 2011 tarihli Kararname ile hükümet ile sektör arasındaki diyalogu geliştirmek için CNN (Dijital Ulusal Konsey) isimli Dijital Ekonomi Bakanı’nın sorumluluğu altında çalışan bir danışma organı oluşturulmuştur (Legifrance, 2011c). Telekom oyuncuları, İnternet, yazılım, e-ticaret ve online reklam gibi dijital sektörden gelen 18 gönüllü üyeden oluşan CNN, bilgi toplumu alanı ile ilgili tüm konularda, mevzuat çalışmalarında hükümete görüş bildirmek ve kamuoyu tartışmalarına katılmak misyonu ile kurulmuştur (Cnnumerique, 2012). Bu çerçevede CNN’e içerik düzenlenmesi konuları da dahil, İnternetin geliştirilmesi, eğitim, sağlık, erişebilirlik gibi genel konular yanında vergi ve reklam gelirleri gibi ekonomik boyutlu konuları da içerecek şekilde çalışma grupları oluşturabilme imkanı verilmiştir (Wikipedia, 2012e).

İnternet’e müdahale edilmesine karşı mücadele yürüten “La Quadrature du Net İnisiyatifi” ve “Korsan Parti”nin başını çektiği Fransa’daki muhalif hareket, CNN’in

kurulmasını olumlu fakat yetersiz bir girişim olarak değerlendirmiştir. Önceki uygulamaların merkezinde olan Sarkozy'nin bu şekilde, İnternet sektörü ile uzlaşmaya çalıştığı ve geçmiş hatalarını gidermek için bir adım attığı ifade edilmiştir. Fakat bunun yanında Konsey'e, çoğu meşhur İnternet sitelerinin sahibi profesyonellerin seçilmesi ve sivil toplumun yani İnternet kullanıcılarının Konsey'de temsiline imkan verilmemesi eleştiri konusu olmuştur (Edri, 2011d; 01net, 2011).

Fransa'da CNN gibi yine bir tür danışmanlık görevi icra eden fakat kısmen uygulamaların da içine girmiş başka bir kuruluş da DUI (İnternet Kullanım Kurulu)'dir. DUI, 2003'de yayınlanan bir kararnameyle (Legifrance, 2003) bilgi toplumunun gelişmesini artırmak adına ülke genelinde izlenecek politikalar geliştirilmesi ve doğru uygulamaların yaygınlaştırılmasına ilişkin çalışmalar yaparak hükümete projeler ve öneriler sunmak için oluşturulmuş bir heyettir (Delegation Internet, 2012a).

Diğer yandan hem CNN'in hem de DUI'nin hükümet içinden Bakanlara bağlı olarak çalışmaları; CNN Başkanı her ne kadar üyeler arasından seçilse de, üyelerinin iki yıllıkına ve bir kez daha seçilebilme şartıyla Bakanlar Kurulu'nca belirlenip Cumhurbaşkanı tarafından atanması ve yine DUI'nin başkanının hükümetçe belirlenmesi (Delegation Internet, 2012b) gibi nedenler her iki kuruluşun da bir öz düzenleme kuruluşu olarak adlandırılmasını mümkün kılmamaktadır.

Fransa'da İnternetle ilgili en etkili bir öz düzenleme kuruluşu DYY (İnternet Hakları Formu)'dir. Devlet kurumları, STK'lar ve özel şirketlerden 70'e yakın üyesi ile DYY, kar amacı gütmeyen bir dernektir. Bu dernek, içerik ve kullanım açısından dijital toplumun gelişimi, İnternet ile ilgili kamu politikalarının oluşturulması düzleminde çok paydaşlı bir yapıda kamu, özel ve sivil toplumun geniş bir yelpazede bağımsız olarak buluşturulmasını amaçlamaktadır (Forum Internet, 2012a).

DYY, İnternet aktörleri arasında diyalog sağlamayı, İnternet konusunda halkı bilinçlendirmeyi, İnternet kullanımıyla ilgili sorunları arabuluculuk mekanizmasıyla çözmeyi ve İnternetle ilgili uluslararası işbirliğini kendisine misyon edinmiştir.

Resmi web sitesi üzerinde İnternete ait muhtelif konularda açmış olduğu tartışma formları oldukça ilgi görmektedir. Bu formlarda ortaya çıkan görüşlerle birlikte diyalog zemininde yürütülen çalışmaların sonuçları DYY tarafından öneriler, raporlar ve rehberler olarak yayınlanmakta ve ilgililere ve kamuoyuna sunulmaktadır (Forum Internet, 2012b).

Kuruluş, bilgilendirme ve bilinçlendirme faaliyetleri için web sitesinde kullanıcılara yönelik birçok içeriği yayınlamaktadır. Burada genel kullanıcılardan profesyonel kullanıcılara kadar her düzeye ve kesime uygun eğitici ve bilgilendirici materyaller yanında, akademik makaleler, mevzuat bilgileri, haberler ve “www.droitdunet.fr” adresinden kullanıcıların günlük kullanımda karşılaşılabilecekleri tüm hukuki konularda pratik cevaplar veren bir servis bulunmaktadır. Bu girişimi Wanadoo, Microsoft ve AFA (Servis Sağlayıcıları ve İnternet Hizmetleri Derneği) gibi sektördeki büyük şirketler desteklemektedir (Forum Internet, 2012a, 2012b).

DYY, 16 Eylül 2004 tarihinde başlattığı arabuluculuk hizmeti ile ülkede İnternet kullanımı alanında ortaya çıkan ulusal veya uluslararası uyuşmazlıkların çözüme kavuşturulmasına çalışmaktadır. İnternet kullanımı veya hizmetiyle ilgili olarak kişilerarası, kişiler ile şirketler ya da şirketler arası anlaşmazlıkları yargıya taşımadan çözmeyi hedefleyen, diyaloga dayalı ve esnek, tarafsız bir kişinin müdahalesine imkan tanıyan bir çalışmayı öngören bu uygulama büyük oranda başarılı olmuştur. Bu uygulamada sektördeki düzenleyici kurumlar yanında sektörde yer alan firmalarla işbirliği geliştirilerek sorunlar çözülmeye çalışılmaktadır. Bu bağlamda Fransa’da arabuluculuk hizmeti ilkelerine saygı gösterilmesini güvence altına alan mevzuat düzenlemesi de yapılmıştır (Forum Internet, 2012c).

DYY, Avrupa ve Avrupa dışında yer alan çeşitli uluslararası girişimlere katılmakta ve desteklemektedir. Özellikle AB’nde başlatılan EICN (Avrupa İnternet Ağı İşbirliği) çalışmalarına aktif destek vermektedir. Bu çerçevede, Avrupa’da İnternet hukuku konularında bilgi ve uzmanlığı olan bir ağ oluşturulması, bu ağ sayesinde üyelerin kendi deneyimlerini, uygulamalarını ve bilgilerini paylaşabilmelerini, içerik düzenlemesi ve İnternet kullanımı ile ilgili sorunların Avrupa düzeyindeki tüm

paydaşların (devlet temsilcileri, özel sektör ve sivil toplum) katıldığı bir platformda tartışılmasına imkan sağlanması ve Avrupa kurumlarına önerilerde bulunulması konularında çaba sarfetmektedir. Ayrıca Dünya Bilgi Toplumu Zirvesi'nin STK'lar düzeyindeki akredite temsilcilerinden biridir (Forum Internet, 2012d).

DYY tüm bu çalışmalarıyla Fransa'da hem öz düzenleme yaklaşımını hayata geçirmeye çalışan hem de bu yaklaşımın sektörde geliştirilmesi ve uygulamalarının artırılması yönünde faaliyet gösteren ülkedeki en güçlü ve başarılı kuruluştur.

Diğer yandan Fransa'da ihbar merkezi, güvenli İnternet bilinçlendirme çalışmaları ve özel anlaşmalar yapılması gibi bazı öz düzenleme araçlarının kullanıldığı da görülmektedir. Ülkede yasadışı ve zararlı İnternet içeriğiyle ilgili ihbarlar, sivil olan AFA ve polis birimi olan OCLCTIC tarafından alınmaktadır (TİB, 2009).

AFA tarafından 1998'de kurulan ve INHOPE'a üyesi olan Point de Contact İhbar Merkezi, İngilizce ve Fransızca dillerinde “www.pointdecontact.net” adresinden yayın yapmaktadır. Merkez, AFA üyeleri ve AB Safer Internet Plus Program'ca finanse edilmektedir. Point de Contact, çocukların cinsel istismarı ve çocukların erişimine açık pornografik içerikler, şiddet içeren ve saldırgan içerikler, ırkçı ve ayrımcı nefrete, kadınlara karşı şiddete, bomba yapmaya veya terörizme, savaş suçlarını övmeye veya insanlığa karşı işlenen suçlara ve intihara teşvik içerikleri ile spam/phishing içerikleri konularında ihbar kabul etmektedir. Point de Contact web sitesinde çocuklara, gençlere ve ebeveynlere İnternetin güvenli kullanımı konusunda kapsamlı bilgiler de sunulmaktadır (Pointdecontact, 2012a).

Merkezde, ihbar aldığı ilk olarak içeriğin yasadışı olup olmadığı incelenmektedir. İçerik yasadışı ve Fransa'da barındırılıyor ise polise iletilmektedir. Polis içeriği bir daha inceledikten sonra yasadışı olduğuna karar verirse kaldırılması için ilgili web sitesinin yer ya da servis sağlayıcısından gerekenin yapılmasını istemektedir. Polis adli soruşturma da yapabilmektedir. Eğer içerik Fransa dışında barındırılıyor ise, ilk olarak içerikteki suç türünün barındırıldığı ülkede de suç olup olmadığına bakılmakta, eğer suç oluşturuyor ise o ülkedeki INHOPE üyesi ihbar merkezine

durum bildirilmektedir. O ülkede INHOPE üyesi ihbar merkezi bulunmuyor ise, ihbar, Interpol aracılığı ile ilgili ülkedeki polis teşkilatına iletilmektedir. Bu süreçte çocukların cinsel istismarı ihbarlarında içeriğe Fransa'dan erişim engellenmektedir. İhbarın sonucu ile ilgili geri dönüş yapılmakta, ihbarın incelenme süreçleri ve incelemenin sonuçları ayrıntılı olarak anlatılmaktadır (Pointdecontact, 2012b).

Polis birimi olan OCLCTIC'da “internet-signalement.gouv.fr” adresinden aynı içeriklerle ilgili ihbarlar almakta ve aynı yöntemle değerlendirmektedir. Merkezin web sitesinde de İnternetin güvenli kullanımıyla ilgili eğitici ve bilgilendirme amaçlı yönlendirmeler ve dokümanlar bulunmaktadır (Internet-signalement, 2012).

Fransa Güvenli İnternet Merkezi, DUI'nun sorumluluğundadır. DUI'nun “Korkusuz İnternet Projesi”, Safer İnternet Plus Program tarafından finanse edilmektedir. Projenin resmi web sitesi olan “internetsanscrainte.fr”, İnternetin güvenli kullanımına yönelik referans site olarak çocuklar, ebeveynler, eğitimciler, kurumlar ve İnternet paydaşları için bir platform olarak ortaya çıkmıştır (Wikipedia, 2012f).

Ayrıca Fransa'da bir özel anlaşma uygulaması olarak Aile Bakanlığı ile varılan mutabakta dayalı olarak, 2005'de AFA üyesi İSS'lar çocukların İnternette güvenli bir biçimde gezinmelerini sağlamak amacı ile müşterilerinden ek bir ücret talep etmeden kullanıcı dostu ebeveyn kontrol ara yüzlerini hizmete sunmuşlardır (Edri, 2005). 2006 yılında da “İnternet Sürücü Belgesi” adında çocukları güvenli İnternet kullanımı konusunda eğitici bir oyun kullanıma sunulmuştur (Passe ton permis, 2012).

Sonuç olarak, Fransa'da çocuk pornografisi, yetişkin pornografisi içeriklerinin çocuklara erişimi, insanlığa karşı işlenen suçlar ve ırkçılığı övme, telif hakları ihlali, yasadışı online kumar, terör aktiviteleri ve şiddete özendirme konularındaki içerikler ile mücadele edildiği görülmektedir. Ülkede İnternetin düzenlenmesi konusunda arabuluculuk uygulamasını başarıyla hayata geçiren DYY gibi örnek bir öz düzenleme kuruluşu ile ihbar merkezi, bilinçlendirme faaliyetleri, özel anlaşmalar yapma gibi öz düzenleme araçlarının kullanıldığına rastlansa da yasadışı ve zararlı

içerikle mücadele konusunda muharrik unsurun kamu kurumları olduğu gözlemlenmektedir.

Bu çerçevede yasadışı içerikle ilgili olarak çıkarılan Anti Terör Yasası, HADOPI ve Loppsi 2 Yasaları yanında ARJEL benzeri özerk düzenleyici kurumların uygulamaları Fransa’da İnternetin sansüre uğradığı yönündeki endişeleri artırmış ve “La Quadrature du Net İnisiyatifi” ve “Korsan Parti”nin başını çektiği, bu tür karar ve uygulamalara şiddetle karşı çıkan muhalif bir hareketin oluşmasına neden olmuştur. Diğer yandan hükümet, bu mücadele ile birlikte İnternetle ilgili tüm konularda ve sorunlarda görüşü alınacak olan CNN adındaki gönüllü sektör temsilcilerinden oluşan bir danışma organını devreye sokarak hem eleştirileri bir nebze olsun azaltabilmek hem de bu alandaki çalışmaların eksenini biraz daha “birlikte yönetmek” yaklaşımına doğru kaydırmak istemektedir.

2.5.2.5 Almanya

Almanya 67 milyonu geçen İnternet kullanıcısı ve %83’lük İnternet kullanım oranı ile AB ülkeleri içinde İnternet açısından önemli bir ülkedir (internetworldstats, 2012e). Almanya, İnternet içerik düzenlemesiyle ilgili olarak AB’nin ilkesel normlarına bağlı kalmakla birlikte, çocuk pornografisi ve telif haklarıyla ilgili içerikler dışında ırkçılık ve her türlü pornografik içerikle en sıkı mücadele yürüten, geliştirdiği uygulamalar ile bu alanı en çok disipline eden ülkelerden birisidir.

2.5.2.5.1 Yasal Çerçeve

Genel olarak bilişim suçlarıyla ve İnternetle ilgili Kıta Avrupa’sındaki ilk düzenlemeler Almanya’da yapılmıştır. Bu ülkede yapılan düzenlemelerde suçla korunan hukuksal değer gözetilerek bilişim suçlarına ilgili oldukları bölümde yer verilmiştir (Dülger, 2004: 96). Keza Almanya, çocuk, genç ve yetişkin pornografisi, ırkçılık (Nazi propagandası) ve telif hakları ile ilgili içeriklerle mücadele konularında özel federal yasalar çıkarmak yerine, mevcut federal yasalarda değişikliğe giderek yasadışı ve zararlı olarak kabul ettiği içeriklere önlem alma yolunu tercih etmiştir. Bunlar dışında eyaletlerde de kimi düzenlemelere rastlanmaktadır.

Almanya İnternette yer alan çocuk, genç ve yetişkin pornografisine ait içeriklerle mücadelesini büyük oranda, 1871 tarihli federal bir düzenleme olan Alman Ceza Yasası (Strafgesetzbuch-StGB) ile yürütmektedir. Yasa, “yayın” kavramının işitsel ve görsel medya kayıtlarını, veri saklama (depolama) medya araçlarını, resim ve diğer fotoğraf, film, çizgi veya sair imajları kapsadığını belirttikten sonra, şiddet eylemi, çocukların cinsel istismarı ya da hayvanlarla cinsel ilişkide bulunmayı içeren pornografik yayınları “yasak yayın” kapsamında değerlendirilmiş ve yaptırıma bağlamıştır. Bu kapsamda, Yasa’nın “Pornografinin dağıtımı” başlıklı 184. maddesinde pornografinin yayımı ile ilgili aşağıdaki eylemler suç kabul edilmiş ve hapis cezası öngörülmüştür (Gesetze-im-internet.de, 2011):

- 1) Pornografik içerikli yayınları 18 yaşından küçüklere veren veya ulaşabileceği yer konusunda bilgilendirme gibi başka bir şekilde ulaşılabilir kılan,
- 2) Pornografik içerikli görüntüleri kamuya sunan, gönderen veya başka bir şekilde ulaşılabilir kılan,
- 3) Pornografik içerikli yayınları satış alanlarında sunan ya da e-posta siparişi aracılığıyla ticaretini yapan,
- 4) Pornografik yayınları umumi kamuya açık gösterim seanslarında gösteren, üreten, satın alan, depolayan ya da kiralayan, ihraç eden ya da yaymak için çoğaltan.

Yine Ceza Kanunu’nun 184b maddesinde; çocukların cinsel istismarını oluşturacak yayınların dağıtımı, gösterimi, üretimi, satın alınması, depolanması, ilan edilmesi kopyalanması yasaklanmış ve hapisle cezalandırılmıştır. Yasa’nın “Genç pornosunun yayılması, toplanması ve elde bulundurulması” başlıklı 184c maddesinde ise; 14 ile 18 yaş arasındaki genç insanların bulunduğu pornografik yayınların dağıtımı, gösterimi, üretimi, satın alınması, depolanması, ilan edilmesi, kopyalanması yasaklanmış ve hapis cezası öngörülmüştür (Gesetze-im-internet.de, 2011).

Keza Yasası’nın 86, 130 ve 131. maddeleri ise, ırksal, etnik, dinsel ayrımcılığı ve nefreti, insanlık dışı söylemleri ve şiddeti, insanlığa karşı yapılan Nazi soykırımını inkar eden medya içeriklerini yasaklamakta ve cezai müeyyide öngörmektedir (Gesetze-im-internet.de, 2011).

Müstehcenlik, ırkçılık, şiddet ve vahşet gibi İnternet içeriğiyle ilgili mücadelenin diğer bir dayanağını ise yine federal bir yasa olan 23 Temmuz 2002 tarihli Gençlik Koruma Yasası (JuSchG-Jugendschutzgesetz)'dır. 14-18 yaş arası gençlerin genel olarak korunmasına ve insan onurunun muhafazasına yönelik olarak çıkarılan bu Yasa, 31.10.2008'de önemli bir değişikliğe uğramıştır. Bu değişiklik ile elektronik medyada gençlerin ve insan onurunun korunmasını sağlamayı hedefleyen düzenlemeler yapılmıştır. Buna göre, çocuklar ve gençler için yasadışı ve zararlı görülen müstehcenlik, ırkçılık, şiddet ve vahşet içeren elektronik yayınlara önlem alınması, çocukların ve gençlerin bu tür yayınlardan korunmasına yönelik hükümler getirilmiştir. Video, film, dijital oyun vb. elektronik yayın materyallerinin içeriklerine göre yaş grupları gözetilerek kategorize edilmesi ve etiketlenmesi bu çerçevede Yasa'nın öngördüğü düzenlemelerden birisidir (Gesetze-im-internet.de, 2002).

Keza Almanya, çocukları ve gençleri, elektronik bilgi ve iletişim araçlarından kaynaklanacak, zararlı ya da tehlike oluşturabilecek içerikten koruyabilmek amacıyla, bütün eyaletler tarafından imzalanarak 2003'de yürürlüğe giren ve yasa gücünde olan Gençlik Medya Koruma Devlet Antlaşması (Jugendmedienschutz-Staatsvertrag-JMStV) isimli ortaklık belgesine istinaden İnternet içeriğiyle mücadele etmektedir (Kjm-online, 2002). Almanya'da müstehcenlik ve telif haklarına ilişkin içerikler yanında ırkçılıkla mücadele, insan onurunun ya da Alman Ceza Kanunu'nda yaptırıma bağlanmış olan hukuki değerlerin ihlal edilmesine karşı etkin önlemlerin alınmasında bu düzenlemenin önemi büyüktür (Edri, 2009b).

Elektronik yayın/medya ve iletişim ortamı için geçerli olan JMStV, halkın bir bölümüne karşı nefret veya ulusal ırksal kışkırtma ve dini, folklorik ve kültürel gruplara karşı tahrik ve şiddet, antisemitizm, insan onuruna hakaret, çocuk ve genç pornografisi ve istismarı ve aşırı yetişkin pornografinin yasak olduğunu ve cezai müeyyidelerinin bulunduğunu öngörmektedir. Bunların üretimi, sunumu, dağıtımı, ticari meta olarak kullanılması ceza gerektirmektedir.

JMStV, bu nevi yasadışı ve zararlı yayınların önlenmesi için ilgili sektörün öz düzenleme uygulamalarına gitmesini, bu çerçevede; çocuklar ve gençler için koruma

programlarının ve bilinçlendirme çalışmalarının yapılmasını, sözkonusu yayınlarla ilgili etiketleme ve işaretleme uygulamalarının hayata geçirilmesini, aynı zamanda eğitim, danışmanlık ve destek hizmetleri de verecek bir ihbar merkezinin kurulmasını, çocukların ve gençlerin zararlı içeriğe ulaşmasına engel olacak yaş sınırlama sistemlerinin kurulmasını öngörmektedir.

Almanya'da İnternet aktörlerinin sorumluluğunu düzenleyen federal nitelikteki temel yasa, 1997'de tarihli Teleservisler Yasası (Teledienstegesetz-TDG)'dir. Almanya, E-Ticaret Direktifi'ne uyum sağlamak amacıyla bu Yasa'da 2001 tarihinde yaptığı değişikliklerle İnternet aktörlerinin ceza sorumluluğuna yer vermiştir. Yasa, İnternet üzerindeki içeriklere ilişkin içerik, servis ve erişim sağlayıcı olmak üzere üç işlevi yürüten İnternet aktörlerini birbirinden ayırmış ve bu aktörlere yerine getirmiş oldukları işlevin özelliğine göre ceza sorumlulukları düzenlemiştir (Buzer, 2007).

Yasa'nın 5. maddesinde; içerik sağlayıcıların yayına koydukları içerik nedeniyle genel hükümlere göre sorumlu tutulacağı, İSS'ların, barındırdıkları verilerin sürekli değişmesi ve bunun takip edilmesinin olanaksız olmasından dolayı, kendi sistemlerinde barındırdıkları başkalarına ait yasal olmayan içeriklerin bu niteliğinden haberdar olmaları ve ayrıca bu bilgilerin İnternet üzerinden erişilebilir kılınmasını teknik olarak önleme olanağına sahip bulunmaları halinde bu bilgelere erişimi önlemezlerse sorumlu tutulacakları, sadece başkalarına ait verilere ulaşım imkanı sağlayan erişim sağlayıcıların ise içerik nedeniyle cezai sorumluluğunun bulunmadığı belirtilmiştir (Buzer, 2007).

Yasanın 6. maddesinde İSS'lara bilgilendirme yükümlülüğü getirilmiş, hizmet sunan kişinin ad ve adresi, grup veya tüzel kişilikse yetkili temsilcilerinin ad ve adreslerinin bildirilmesi zorunlu tutulmuştur. Ancak, İnternet servis sağlama hizmetleri serbest bırakılmış ve herhangi bir ruhsat ve izne tabi tutulmamıştır (Buzer, 2007).

Almanya'da, arama motorlarının erişim sağlayıcı olarak değerlendirilip değerlendirilmeyeceği, bu çerçevede üçüncü kişilere ait yasadışı içeriğe erişimi engelleme görevi bulunup bulunmadığı tartışılmaktadır. Alman hükümeti, "link"

kullanımının karışık bir işlem olması nedeniyle bu alanda bir düzenlemenin uygun olmayacağı, her olayın kendi şartları içerisinde mahkemelerce değerlendirilmesi gerektiği görüşündedir (Oğuz, 2008).

2.5.2.5.2 İçerik Düzenleme Politikası

Almanya diğer batılı ülkelere göre İnterneti düzenleme konusunda daha agresif davranmaktadır (Andrews, 1999). Almanya, İnternetin yoğun olarak kullanıldığı fakat aynı zamanda sıkı bir şekilde denetlendiği bir ülkedir. Bu denetim çocuk pornografisi, her türlü pornografik içerik ve tarihi sebeplerle ırkçı web siteleri ile özelde Nazi propagandası ve telif hakları ile ilgili konularda gerçekleştirilmektedir (Berber ve Kaya, 26.07.2010; Çamlı, 2010b). Hatta İnternet filtrelemelerine karşı olan bazı gruplar, bu özelliği nedeniyle Almanya’da İnternet’in “Germany.Net”e dönüştüğünü ifade etmektedirler (Lessig, 2003).

Almanya uygulamaları incelendiğinde bu iddiaların asılsız olmadığı görülmektedir. Gençleri Koruma Komisyonu (KJM), Gençlik Koruma Yasasıyla 2003’de kurulmuştur. Yasa, KJM’yi, gençleri koruma hususunda İSS ve yer sağlayıcılar üzerinden erişim engellenmesi konusunda yetkilendirmiştir. KJM ile İSS’lar arasında bir protokol yapılarak erişim engellemeler gerçekleştirilmektedir(Kjm-online,2012a).

KJM, çocukların, gençlerin ve insan onurunun her türlü medya yayınından korunmasından sorumlu bir kamu kurumu olarak, Gençlik Koruma Yasası ile Gençlik Medya Koruma Devlet Antlaşması’nda düzenlenen; halkın bir bölümüne karşı nefret veya ulusal ırksal kışkırtma ve dini, folkrolük ve kültürel gruplara karşı tahrik ve şiddet, antisemitizm, insan onuruna hakaret, çocuk ve genç pornografisi ve istismarı ve aşırı yetişkin pornografi gibi yasadışı ve zararlı her türlü medya içeriğiyle mücadele etmektedir. Ayrıca, video, film, online oyunlar ile online kumar ve bahis konularında da sorumludur (Kjm-online, 2012b).

Bu çerçevede İnternet yayını ve içeriği de dahil olmak üzere, sözlü, görüntülü ve elektronik olarak üretilen her nevi yayını ve içeriği değerlendirme, denetleme ve düzenleme yetkisine sahip olduğu gibi, yasal olarak eğitim ve destek hizmetleri de

yürütebilmekte ve sosyo-politik süreçleri başlatabilmektedir. Kurum, bu alanlarda yapılan çalışmalarda öz düzenleme prensibini esas almakta ve ilgili sektörlerin kendi kendisinin denetim ve kontrolünü yapmasını benimsemektedir. Bu bağlamda öz düzenleme uygulamalarını desteklemekte ve mevcut öz düzenleme kuruluşlarını akredite edip, yakın bir işbirliği içinde çalışmaktadır (Kjm-online, 2012c).

Dolayısıyla, bu kapsamda ilgili sektörün öz düzenleme uygulamalarına gitmesini; çocuklar ve gençler için koruma programlarının ve bilinçlendirme çalışmalarının yapılmasını, bu yayınlarla ilgili etiketleme ve işaretleme uygulamalarının hayata geçirilmesini, aynı zamanda eğitim, danışmanlık ve destek hizmetleri de verecek bir ihbar merkezinin kurulmasını, çocukların ve gençlerin zararlı içeriğe ulaşmasına engel olacak yaş doğrulama sistemlerinin yayını sunan şirketlerce kurulmasını sağlamaya çalışmakta, denetim ve düzenleme yapmaktadır (Kjm-online, 2012c).

KJM, ayrıca, çocukların ve gençlerin zararlı içeriklerden korunması ve içerik sorunlarını değerlendirme, koruyucu mekanizmaların kurulması, ülke ve Avrupa düzeyinde bu konularla ilgili uygulamaların, mahkemelere yansıyan davaların takibi, hukuki ve teknik boyutlarıyla ilgili uzman görüşlerinin alınması, eldeki verilerin analiz edilmesi, raporların hazırlanması faaliyetlerini yürütmektedir (Kjm-online, 2012d).

Keza, KJM bilinçlendirme programları yapmakta; bu amaçla dökümanlar hazırlamakta ve sunmaktadır. Örneğin KJM'nin gençlik komisyonu web sitesi olan www.kjm-online.de, Almanca ve İngilizce dillerinde yayın yapmaktadır. Web sitesi bilgi, donanım ve içerik bakımından dünyadaki örnekleri arasında mükemmele en yakın bilinçlendirme sitesidir. KJM çok aktif çalışmakta; Alman ulusal kanallarında bilinçlendirme ve bağış toplama programları da yapmaktadır (Bozkurt, 2012: 53).

KJM, çocukların ve gençlerin sakıncalı içerikle buluşmalarına engel olacak, yaş gruplarına göre farklılaşmış alternatifli filtre programlarının üretilmesi ve etkili bir şekilde kullanımının sağlanmasından da sorumludur. Bu çerçevede aileler, okullar, İnternet kafeler ya da gençlik merkezleri için koruma önlemi olarak sunulan filtre

programlarının kriterlerinin tespit edilmesi, kara listelerin oluşturulması ve bunların düzenli olarak güncellenmesi ve akredite edilmesi yanında ilgililerince ve İSS'lar nezdinde kullanılması gibi faaliyetleri yürütmektedir (Kjm-online, 2012e).

KJM, bahsedilen görevleri yerine getirirken kendisinin işlettiği Jugendschutz İnternet İhbar Merkezi, BpİM (Gençlik ve Medya Federal Dairesi) ve FSM (Multimedya Servis Sağlayıcıları Gönüllü Öz-Denetim Derneği) ile yakın bir işbirliği içinde çalışmaktadır. KJM, Jugendschutz İnternet İhbar Merkezi ile yasadışı ve zararlı içeriğin tespiti için aldığı ihbarları da değerlendirerek İnternet ortamının izlenmesi ve denetimi işlevini yerine getirmeye çalışmaktadır (Kjm-online, 2012f).

INHOPE üyesi Jugendschutz İhbar Merkezi 1997'da kurulmuş ve Almanca yayın yapmaktadır. Merkez, çocukların cinsel istismarı, genç pornosu, çocukların doğrudan erişebildiği yetişkin pornosu, ırkçılık ve nazi aktiviteleri, şiddet ve vahşet içeren oyunlar, cinsel şiddet, intihara yönlendirme ile ilgili ihbarları kabul etmektedir (Jugendschutzlandesstellen, 2012).

Jugendschutz bir ihbarı aldığı anda ilk olarak içerikte Alman yasalarına göre bir ihlalin bulunma durumunu incelemekte, eğer bir ihlal var ise içeriğin nerede barındırıldığını tespit etmektedir. İçerik Almanya'da barındırılıyor veya içerik sağlayıcısı ülke içinde ise uyar-kaldır yöntemiyle ilgili yer veya içerik sağlayıcı bilgilendirilmekte ve gerekenin yapılması sağlanmaktadır. Çocukların cinsel istismarı içerikleri ve cinayet gibi durumlarda ayrıca polise de ihbar iletilmektedir. Eğer içerik Almanya dışında barındırılıyor ise o ülkedeki INHOPE üyesi ihbar merkezine ihbar iletilmektedir. İşlemlerin sonunda, ihbarı yapan iletişim bilgisini vermiş ise ihbarın neticesi kendisine bildirilmektedir (Jugendschutz, 2012a).

Jugendschutz İhbar Merkezi INHOPE'un yanında INACH (The International Network Against CyberHate) ve YPRT (Youth Protection Roundtable) ile sıkı bir işbirliği içinde çalışmaktadır. INACH, merkezi Amsterdam'da olan 2002 yılında Hollanda'da kurulmuş bir vakıftır. İnternet ortamındaki ırkçılık ve sınıf ayrımcılığı ile uluslararası düzeyde mücadele etmek ve bu konuda dayanışma, bilgi ve deneyim

değişimini hedeflemektedir (INACH, 2012). YPRT ise bir AB projesi ile 2007 yılında kurulmuştur ve amacı İSS'ler ve filtre üreticilerini bir araya getirerek çocuk ve gençlerin korunmasına teknik çözümler bulmaktır. Jugendschutz, ayrıca bilinçlendirme faaliyetlerine katkı da sağlamaktadır (TPRT, 2012).

BpjM, KJM'nin İnternet içeriğinin endekslenmesi, kategorize edilmesi, derecelendirilmesi ve etiketlenmesi görevlerini yerine getirmesinde işbirliği yaptığı bir kamu kurumudur(Kjm-online, 2012g). Çocukları ve gençleri zararlı veya tehlikeli medya içeriğinden korumak amacıyla videoları, DVD'leri, dijital oyunları, ses kayıtları ve CD'ler ile yazılı basın ve İnternet sitelerini takip eden BpjM, söz konusu materyalleri değerlendirerek yaş grupları ve içerik türlerine göre yasadışı veya zararlı olup olmadığına karar vermekte, buna göre endekslemekte, kategorizasyon, derecelendirme ve işaretleme yapmaktadır (Bundespruefstelle, 2012a).

BpiM, Avrupa'nın en büyük ikinci oyun pazarı olan Almanya'da, oyunların sınıflandırması görevini yürütürken, USK (Eğlence Yazılımları Öz Denetimi) adlı kuruluşla işbirliği yapmaktadır (Bundespruefstelle, 2012b). USK, sektördeki oyun üreticilerinin katılımıyla oluşan ve bütçesi üye olan oyun üreticileri tarafından karşılanan bir öz düzenleme kuruluşudur. Bu kuruluş, BpiM'in oyun endeksleme kriterlerini baz alarak bir takım testlerden ve süreçlerden geçirerek oyunları yaş grupları ve içerik türlerine göre sınıflandırmakta ve etiketlemektedir. Bu işlem BpiM ve KJM'nin de onayından geçtikten sonra oyun piyasaya sunulmaktadır. Oyunların satışının yapılması ile ilgili de bir takım kurallar belirlenmiştir. Bu kurallara uymayan firmalara 50 bin € kadar para cezası verilebilmektedir (USK, 2012).

BpjM, ECO (Alman İnternet Sanayi Derneği) ve FSM gibi sektörün meslek örgütleriyle işbirliği yaparak filtrelemede kullanılmak üzere BpjM Modülü'nü geliştirmiştir. İçerisinde kara liste barındıran bu modül, bağımsız filtreleme yazılımlarına entegre edilebilir özelliktedir (Bundespruefstelle, 2012c). Keza, BpjM, çocuklara ve gençlere yönelik “medya eğitimi” kapsamında, İnternetin de yer aldığı tüm medya araçlarının, doğru ve güvenli kullanımıyla ilgili bilinçlendirme faaliyetleri yürütmektedir (Bundespruefstelle, 2012d).

FSM ise, öz düzenleme açısından Almanya’da örnek bir kuruluştur. Alman İnternet sektöründeki içerik sağlayan/üreten şirketlerin çoğu FSM üyesidir. Şirketler Derneği üye olurken yasadışı içerik sağlamayacaklarına/ üretmeyeceklerine ve Derneğin kurallarına uyacaklarına dair bir anlaşma imzalamaktadır. FSM, yarı yarıya AB Safer İnternet Plus Program’ı ve FSM üyelerinin aidat ve bağışları ile finanse edilmektedir. Üyelerden her biri yıllık geliri oranında oy hakkına sahiptir ve o oranda bağışta bulunmak zorundadır (FSM, 2012; Bozkurt, 2012: 50).

FSM web 2.0, sosyal ağlar, sohbet, mobil ve arama motoru servisleri işleten üyeleri için ayrı ayrı işletim kuralları belirlemekte ve anlaşmalar imzalayarak bunların uygulanmasını denetlemektedir. Örneğin çocukların sohbet ettiği servis hizmeti veren FSM üyelerine, çocukların yoğun giriş saatlerinde moderasyon hizmeti vermelerini zorunlu kılmaktadır. Benzer şekilde, arama motorlarına 16 yaş altı çocukların profillerinin bulundurulmaması kuralı getirilmiştir. Bir başka örnek, sosyal ağlarda alarm düğmesinin tüm sayfalarda belirgin ve kolayca görünür biçimde bulunmasının zorunluluğu kuralıdır. Ayrıca çocuklarla ilgili web siteleri için kalite kriterleri dokümanite edilmiş ve çok sıkı kurallar getirilmiştir. Bu siteler dokümandaki kurallara titizlikle uymak zorundadır (Bozkurt, 2012: 50).

FSM’nin bir de ihbar merkezi vardır. Gelen bir ihbardaki içeriğin yasadışı olduğuna karar verilirse FSM, ilgili içerik sağlayıcıdan gereğini yapmasını talep etmektedir. FSM bir içeriğin kaldırılmasını istediğinde kaldırmayan üye, uyarı cezasından başlayarak üyeliğin iptaline kadar giden yaptırımlara maruz kalabilmektedir. İçerik eğer FSM üyesi olmayan bir web sitesinde ise BpİM’ne başvurulup bu yolla içeriğin kaldırılmasına çalışılmaktadır. Yasadışı içerik, içeriği sağlayan tarafından kaldırılmazsa, içerik Almanya’da barındırılıyor ise son çare olarak yer sağlayıcıdan hizmeti sonlandırması istenmektedir (Bozkurt, 2012: 50).

Diğer yandan Almanya’da Jugendschutz ve FSM dışında INHOPE üyesi iki ihbar merkezi daha vardır. Bunlardan Beschwerdestelle İhbar Merkezi, ECO ve FSM tarafından 1997’de yasadışı ve zararlı İnternet içeriklerinin ihbar edilmesi için kurulmuş ve ortaklık biçiminde işletilmektedir. Bu iki kuruluş yıllarca sadece

“www.internet-beschwerdestelle.de” web sitesinden ihbarları kabul etmişler, daha sonra aldıkları bir kararla kendi web sitelerinden de ayrı ayrı ihbarları kabul etmeye başlamışlardır. Böylece, ECO “www.eco.de” web adresinden FSM ise, “www.fsm.de” web adresinden ihbar almaya başlamıştır. Aralarındaki işbölümüne göre web, mobil, sohbet ve yaş doğrulama servisleri ile ilgili ihbarlar FSM’ye; haber grupları, spam e-posta, forumlar, dosya paylaşım servisleri ve sitelerdeki kategori işaretleri ile ilgili ihbarlar ECO’ya iletilmektedir (Internet-signalement, 2012a).

Beschwerdestelle İhbar Merkezi, Almanca ve İngilizce yayın yapmaktadır. Merkez, çocukların cinsel istismarı içerikleri (14 yaş altı), genç pornosu (14-17 yaş arası olanlar), yetişkin pornosu ve diğer çocuklara zararlı içerikler ile ilgili ihbarları kabul etmektedir (Internet-signalement, 2012b). Beschwerdestelle, FSM ve ECO ihbar merkezleri Jugendschutz İhbar Merkezine benzer şekilde çalışmakta ve aldıkları ihbarları değerlendirmektedir.

Beschwerdestelle, web sitesinde İnternetin güvenli kullanımı ile ilgili bilinçlendirme amaçlı olarak, çocuklar ve gençlerin İnternet ortamındaki zararlı içerikten korunması için ebeveynler, gençler ve çocuklara hitab eden faydalı ve oldukça detaylı bilgilere ve linklere yer vermektedir (Internet-signalement, 2012c). Ayrıca, Almanya’dan Türkçe, Almanca ve İngilizce yayın yapan, son derece faydalı ve kapsamlı bir bilinçlendirme sitesi bulunan ve Avrupa Komisyonu’nun İnternet ve yeni medya kullanımı medya okuryazarlığını teşvik etmek ve bir farkındalık oluşturmak için desteklediği “klikSAFE.de” Projesi’nin ortaklarından (Internet-signalement, 2012d).

Diğer yandan, Federal Hükümetin Alman yasalarına göre suç teşkil eden ve Almanya dışında barındırılan siteleri engelleme girişimi konusunda tartışmalar devam etse de, söz konusu içeriğe müdahale edilebilmesi için içeriğin ülke içinde barındırılması koşulu aranmamakta, engellemelerin etkinliğini artırmak amacıyla İSS’ler ve bilişim şirketleri sıkı denetime tabi tutulmaktadır. İşbirliği gösterilmemesi durumunda ise katı bir tutum sergilenmektedir (Berber ve Kaya, 01.12.2010: 9).

Almanya’da genellikle hükümetlerin yönlendirmesiyle İSS’lar veya diğer bilişim şirketleri nezdinde filtreleme uygulamalarının gerçekleştirilmesine sıkça rastlanmaktadır. 2005 başlarında Alman hükümetinden gelen baskılar sonucunda, ülkede faaliyet gösteren Google Almanya, Lycos Avrupa, MSN Almanya, AOL Almanya, Yahoo ve T-Online, özdenetim uygulayacaklarını ilan ettiler ve hükümetin verdiği sınıflandırmaları ve kara listeleri temel alan aramaları filtreleyecek bir yapı oluşturdular (Çamlı, 2010b). Bu girişimin “gönüllü öz düzenleme” ye bir tepki olduğu ve AB düzeyinde yapılacak bir yasamanın önüne geçmeyi hedeflediği ileri sürülmüştür. Ancak sistemin şeffaf olmaması ve listede yer alan sitelerin halka açıklanmaması eleştirilmiştir (OpenNet, 2006-2007b). Alman makamları, arama motorlarının uyguladığı yöntemle ilave olarak DNS engellemesi yapmak suretiyle sitelere erişimi tamamen engelleyebilmektedir (Çamlı, 2010b).

Farklı yaptırımlarla karşılaşmak istemeyen bilişim şirketleri, Alman hükümeti ile işbirliği yapma eğilimi göstermektedir. Nitekim Youtube, siyasilerin ve Merkezi Yahudi Konseyi’nin isteği üzerine 2007’de Nazi içeriklerini engelleyeceğini duyurmuştur (Çamlı, 2010b). Keza, Jugendschutz ile Youtube, yasadışı Nazi videolarıyla ilgili bir anlaşma yapmış; anlaşma sonrası Youtube, Jugendschutz’un düzenli olarak bildirmiş olduğu Nazi videolarını kaldırmış veya Almanya’dan erişimi engellemiştir (Jugendschutz, 2012b).

İnternette yer alan zararlı içeriklerle mücadele konusunda, 17 Nisan 2009’da Federal Almanya Aile Bakanlığı aracılığıyla Federal Kriminal Polis Ofisi ile İnternet piyasasının %75’ine karşılık gelen İSS’lar arasında gönüllü olarak sözleşme yapılmıştır. Buna göre, Polis Ofisi’nin oluşturduğu kara listede bulunan porno içerikli, şiddet ve neo-Nazi aktivitelerine yönelik yasadışı İnternet sitelerine erişim engellenmektedir. Almanya’nın geçmişteki Nazi ve Doğu Almanya komünist rejimi tecrübeleri nedeniyle, bilgiye erişim kısıtlanması hassas bir konu olmakla beraber, çocukları korumanın kitlesel iletişimden daha önemli ve öncelikli olduğu Almanya Aile Bakanı tarafından ifade edilmiştir (Nebil, 2009).

Almanya’da eyaletlerin de çeşitli yöntemlerle İnternet içeriğine müdahalede bulunduğu görülmektedir. Örneğin, Almanya’nın en kalabalık eyaleti olan Kuzey Ren Westfalya’da yönetim, 2001’de 80’den fazla yerel İSS’dan, ırkçı ve neo-Nazi içerikler barındıran kara listedeki web sitelerine erişimi engellemelerini istemiştir. Kara listede yer alan web sitelerinin bir kısmının Almanya dışında barındırılıyor olması dikkat çekicidir. Yine aynı eyalette kamuoyundan gelen tepkilere rağmen aşırı sağ içerikli bütün web sitelerine DNS, IP veya Proxy engelleme yöntemi kullanarak erişimleri engellenmektedir (US Department of State Diplomacy in Action, 2005; Çamlı, 2010b). Benzer şekilde, Düsseldorf Bölge İdaresi, 2002 ve 2004 yılları arasında Kuzey Ren Westfalya Eyaleti’ndeki İSS’larını aşırı sağcı içeriğe erişimi engellemeye zorlayan 90 karar almıştır (Akdeniz ve Altıparmak, 2008: 79).

Almanya’da telif hakkı ihlalleri ve hakaret gibi sebeplerle, kamuoyunda tartışmalara neden olan bazı erişim engelleme olayları da vuku bulmuştur. Bunlardan birisi, 2007’de Alman Müzik Telif Hakkı Sahipleri İttifakı (GEMA)’nın girişimiyle telif haklarını ihlal ettiği gerekçesiyle dünyanın en büyük dosya paylaşım sitelerinden birisi olan “rapidshare.com” web sitesinin erişiminin engellenmesidir. Rapidshare, kullanıcıları tarafından yüklenen içerikten sorumlu tutulmayacağını belirtmesine rağmen, dosyalar kaldırılncaya kadar erişim yasağı devam etmiştir (Heise, 2007).

Diğeri ise, kişilik haklarını ihlal ettiği gerekçesiyle Wikipedia’nın Almanca versiyonu olan “www.wikipedia.de” sitesine uygulanan yaptırımdır. Alman Sol Parti Federal milletvekili Lutz Heilmann, Wikipedia’da yer alan özgeçmişinde asılsız bilgilerin yer aldığı gerekçesiyle site hakkında engelleme kararı aldırılmıştır. Böylece, hukuka aykırı bir sayfa için online ansiklopediye erişim engellenmiştir (Techcrunch, 2008).

Almanya’da İnternet içeriğinin düzenlenmesiyle ilgili olarak kapalı kullanıcı grupları kavramı geliştirilmekte ve kullanılmaktadır. Bu uygulamaya göre örneğin bir yetişkin pornosu sitesi herkese açık hizmet verememektedir. Bu tür sitelere girişte mutlaka kimlik ve yaş doğrulama sistemi bulunmakta ve üyelik yolu ile hizmet verilmektedir. Bu da iki aşamada olmaktadır. İlk aşamada yaş doğrulaması yapılmaktadır. İkinci aşamada doğrudan iletişim ile bankalarınkine benzer bir yolla

kimlik doğrulaması yapılmaktadır. Bu şekilde yetişkinler için olan içeriğe çocukların erişimi engellenmeye çalışılmaktadır. Ayrıca verilen bilgiler bir veri tabanına kaydedilmekte ve düzenli olarak doğrulukları kontrol edilmektedir. Bu konu Almanya’da ciddi bir biçimde tartışılmaktadır. Porno kaset kiralarken yüz yüze kimlik doğrulaması yapıldığı, ama İnternet ortamındaki uygulamada verilen kimlik bilgilerinin ele geçirilmiş olabileceği, bundan dolayı biyometrik doğrulama sistemlerinin kullanılması gerektiği ifade edilmektedir (Bozkurt, 2012: 53).

Sonuç olarak İnternet içeriğinin düzenlenmesi bağlamında Almanya örneğinde öne çıkan bazı özelliklerin altını çizmek gerekirse; birincisi, Almanya’nın AB’nin belirlemiş olduğu temel ilkeleri gözeterek, İnterneti diğer medya araçlarından birisi, İnternet içeriğini de bir yayın türü olarak gördüğünü, dolayısıyla İnternet için ayrı bir özel yasal düzenleme ve uygulama biçimi geliştirmek yerine bu alanı, genel olarak medya ve elektronik iletişim araçlarının yayın ve kullanımıyla ilgili düzenlemeler ve uygulamalar içinde ele aldığını söyleyebiliriz. Bu durumda, ifade ve iletişim özgürlüğü konusundaki eleştirilere rağmen, Almanya Devleti’nin sadece İnternet içeriğine değil, bir bütün olarak medya araçlarına ve yayınlarına yönelik düzenleme yapma ve müdahalede bulunma iradesini ortaya koyduğu gözlemlenmektedir.

İkincisi; dünyadaki genel eğilime paralel olarak Almanya’nın da çocuk pornografisi, ırkçılık, vahşet ve şiddet ile telif hakları ihlallerine ait İnternet içerik türlerini yasadışı kabul etmekle birlikte, tarihsel nedenlerle aşırı sağ/Nazi aktivitelerine, etnik ve dini ayrımcılığa ve nefrete, antisemitizme ait içeriklerin yanında genç ve yetişkin pornografisini de yasadışı içerik kapsamına aldığı görülmektedir. Buna göre Almanya’da hem federal ölçekte hem de eyaletler bazında, yasadışı ve zararlı olarak kabul edilen söz konusu içerik türleriyle ciddi bir mücadele yürütülmektedir.

Üçüncüsü; yasadışı içerikle yürütülen mücadele açısından Almanya, federatif devlet yapısına ve İnternetin kaotik özelliğine rağmen ulusal ölçekte İnternetin disipline edilmesi, yönetilmesi, kuralların detaylı ve açık bir biçimde ortaya konulması bakımından örnek ülkelerden birisidir. Almanya, yasadışı ve zararlı İnternet içeriklerinin neler olduğu, bunlara karşı mücadelenin hangi yöntemlerle, nasıl ve

kimler tarafından yapılacağı; bu süreçte görevli ve sorumlu kurum ve kuruluşların kimler olacağı, hangi mekanizmaların işletileceği gibi konularda detaylı kuralları belirlemiş ve yerleşik uygulamaları geliştirmiştir.

Dördüncüsü, Almanya’da yasadışı İnternet içeriğiyle mücadele konusunda her ne kadar FSM gibi ilgili sektörde yer alan şirketlerin kendi kendilerine disipline olması ve öz düzenleme uygulamaları geliştirmeleri desteklenmekte ve mevcut öz düzenleme kurumları ile işbirliği içinde çalışılsa da, KJM ve BpiM gibi federatif yasal yetkilerle donatılmış güçlü düzenleyici kamu kurumlarının sistem üzerinde etkin olduğu ve belirleyici aktör oldukları görülmektedir. Bu çerçevede öz düzenleme uygulamalarının “gönüllük” esasından daha ziyade “zorunlu gönüllük” biçiminde tezahür ettiği, dolayısıyla içerik düzenlemesi konusunda yönetsel yaklaşımının “birlikte düzenleme” ve “yönetişim” odaklı olduğu söylenebilir.

2.5.2.6 Rusya Federasyonu

Rusya 68 milyon İnternet kullanıcısı ile sayısal olarak Avrupa ülkeleri içinde en önde gözükse de %48’lik İnternet kullanım oranı ile gerilerde yer alan bir ülkedir (internetworldstats, 2012e). Fakat, devlet politikası olarak son yıllarda ekonomik kalkınma için bilgi teknolojilerine büyük yatırımlar yapılmakta, İnternet altyapısını güçlendirmeye ve kullanımı artırmaya çalışmaktadır. Bunun yanında içerik düzenlenmesi konusunda Rusya, ulusal güvenlik kaygılarına öncelik veren ve İnternetin bir bütün olarak devletin denetimi ve kontrolünde varlığını sürdürmesini öngören bir yaklaşım içindedir.

2.5.2.6.1 Yasal Çerçeve

Rusya Federasyonu Anayasası 29. maddesi ile ifade özgürlüğünü garanti altına almakta ve kısıtlamayı yasaklamaktadır. Anayasa, 23, 24 ve 25. maddeleri ile gizlilik ve veri koruma, bilgi edinme hakkı ve iletişimin gizliliği haklarını tanımaktadır (Constitution, 2013). 2003 tarihli Haberleşme Yasası iletişim ve kişisel gizlilikle ilgili kısıtlamaların ancak bir mahkeme kararı ile mümkün olabileceğini düzenlemektedir (Minkomsvjaz, 2003).

Diğer yandan Rusya Federal Yasası ülkede çocuk haklarının garanti altına alındığını belirterek, kamu yetkililerinin şiddet, zulüm ve pornografi içeren, uyuşturucu ve zararlı madde kullanımını teşvik eden basılı malzeme, ses ve video ürünlerinin dağıtımını da dahil olmak üzere; çocukların sağlık, ahlaki ve ruhsal gelişimine zararlı her türlü bilgi, propaganda, ürünlere karşı korunması için gerekli tedbirleri almakla görevli olduklarını vurgulamaktadır (Friendly Runet Foundation, 2012a).

Bu çerçevede, Rus Ceza Yasası gerçek veya simüle olarak 18 yaşından küçük kişilerin yer aldığı ve açık cinsel faaliyetleri ya da cinsel amaçlı olarak bir çocuğun cinsel organlarını gösteren görüntülerin yer aldığı malzemelerin üretimini, depolamasını ve dağıtımını, değişen şartlara göre 6 aydan 8 yıla kadar hapis cezası ile müeyyideye bağlamıştır. Yasa’da ayrıca online terörist faaliyetler, ulusal, ırksal veya dinsel düşmanlığı teşvik eden, insan onuruna aykırı içerikler yasaklanmış ve bu suçlar için 2 yıla kadar hapis cezası öngörülmüştür (Russian Criminal Code, 2013).

Hükümet’in 2002’de çıkardığı Aşırılık Aktivitelerine Karşı Mücadele Federal Yasası (RG, 2013), ülkede ve ülke dışında genel olarak tüm özgürlüklere, özelde ise İnternet özgürlüğüne yönelik bir tehdit olarak değerlendirilmiştir (Verkovsky, 2011). Bu Yasa gerekçe gösterilerek muhalif görüşlerin dile getirildiği web sitelerin, forumların yasadışı kabul edilerek kapatılmalarının kolayca mümkün hale geldiği dile getirilmiştir. Bu bağlamda İçişleri Bakanlığı bünyesinde İnternet ortamında siber kurallara uygunluğu izleyen “K” birimi kurulmuş ve bu birim online nefret söylemi ve karalama dahil olmak üzere bilgi teknolojileri alanında suçları soruşturmakla görevlendirilmiştir (OpenNet, 2010b). Nitekim ilerleyen zamanlarda “K” birimi ve bu Yasa’nın uygulamasında sansür endişelerini haklı çıkaracak bazı olumsuz örneklerin yaşandığı görülmüştür.⁵⁶

Bu Yasa dışında Rus hükümeti suçların ve terörizmin önlenmesi gerekçesiyle İnterneti gözetim altına almaya yönelik bazı düzenlemeler de yapmıştır. 1995’de

⁵⁶ Örneğin 2007 yılında “hc-rodina.ru” adlı spor sitesi, forum bölümünde yayınlanan hükümet temsilcileri hakkındaki yorumlar nedeniyle kapatılmıştır (Pingvinov, 2007). Başka bir örnekte, bir blogger Putin’i dazlak olarak tasvir eden bir karikatürü yayınladığı için bir yıl hapis cezasına çarptırılmıştır (CNews, 2008).

çıkarılan ve 2008 yılına kadar birçok değişiklikler geçiren SORM Yasası bunlardan birisidir. Bu Yasa’da yapılan son değişikliklerle FSB (Federal Güvenlik Servisi) tüm İnternet trafiğini izlemeye yetkili kılınmıştır. Buna göre, İSS’lar yargı kararı olmaksızın kendi sunucularından geçen tüm İnternet trafiğine ait verileri FSB’ye sağlamakla yükümlü tutulmuştur. Hatta Başkan Putin daha sonra SORM altında İnternet trafiğini izleme yetkisini FSB dışında vergi polisi, İçişleri Bakanlığı, Sınır Muhafızları, Kremlin ve Cumhurbaşkanlığı Güvenlik Servisi, Parlamento Güvenlik Hizmetleri ve Dış İstihbarat Servisi’ne de vermiştir (OpenNet, 2010b).

2.5.2.6.2 İçerik Düzenleme Politikası

Rusya’da İnternet bir medya türü olarak algılanarak düzenlemelere konu edilmiştir. Bu nedenle diğer medya ürünlerinin sorumluluk rejimine dahil edilerek web sitelerinin resmi tescil ve kayıt sistemine tabi olması gerektiği iddia edilmiştir. Fakat tüm web sitelerinin kayıt altına alınabilmesinin uygulanabilirliği mümkün görülmediği için Kitle İletişimi Yasası’nda yapılan değişiklikle “gönüllü kayıt” ile bir nevi akredite olma sistemi getirilmiştir. Yeni değişiklik kayıt altına girerek kendisini tescil ettiren web sitelerine bir takım avantajlar sağlayarak (vergi indirimi ve teşvik verilmesi, akredite olarak bazı programları takibe yetkili olmak gibi) “gönüllü kayıt” uygulamasını teşvik etmiştir. Nitekim, 2004 yılında, 1.296 kayıtlı web site var iken bu sayı 2009’a kadar yaklaşık 20 bine ulaşmıştır (OpenNet, 2010b).

İnternetin bir medya türü olarak görülmesi nedeniyle Rusya’da İnternetle ilgili genel sorumlu kurum Rusya Federasyonu İletişim ve Kitle Haberleşme Bakanlığı olmuştur. Bakanlık bünyesinde tüm basılı, işitsel ve görsel medya ürünlerinden ve dolayısı ile özel olarak İnternet içeriklerinden sorumlu birim başlangıçta Rospechat (Basın ve Kitle İletişim Federal Ajansı) idi. Daha sonra 2009’da çıkarılan Kanun Hükmünde Kararname ile yine aynı Bakanlığın bünyesinde Roskomnadzor (Bilgi Teknolojileri ve Kitle İletişimi, İletişim Denetleme Federal Servisi) kurulmuş ve içerik konusu da dahil tüm İnternetle ilgili düzenleme ve denetleme işlemleri bu kamu kurumun uhdesine verilmiştir (RSOC, 2013a).

Roskomnadzor, radyo ve televizyon yayıncılığı yanında tüm İnternet yayıncılığından, İnternet aktörlerinin (İSS'lar, hostingler, içerik sağlayıcılar) lisans, kayıt, gözetim ve denetiminden sorumlu tutulmuştur. Bu çerçevede tüm diğer medya içeriklerinin olduğu gibi İnternet içeriklerinin de çocukların korunması çerçevesinde yaş gruplarına ve konularına göre kategorize edilerek sınıflandırılmasıyla görevlendirilmiştir (RSOC, 2013b). Ülkede ayrıca İnternetle ilgili bağımsız bir düzenleyici kurum oluşturulmamıştır (OpenNet, 2010b).

Rusya'da ulusal güvenliği sağlama ve terörle mücadele kapsamında İnternet içeriğine müdahale etme politikası dışında, yasadışı ve zararlı İnternet içeriği konusunda çocukların korunması bağlamında çocukların cinsel istismarı ve onlara zarar verecek diğer içerikler mücadele kapsamında ön plana çıkmaktadır. Bu çerçevede Rusya'da yasadışı içerikle mücadele kapsamında faaliyet gösteren INHOPE üyesi iki ihbar merkezi bulunmaktadır. Bunlardan Friendly Runet, İnternet ortamının güvenli bir hale getirilmesi ve özellikle çocukların cinsel istismarı ve uyuşturucu kullanımının teşvikine ait içeriklerle mücadele amacı ile Rusya'nın önde gelen İnternet endüstrisi aktörlerinin bir araya gelerek oluşturdukları bir STK olan Friendly Runet Foundation tarafından kurulmuştur (Friendly Runet Foundation, 2012b).

Fakat, bu Merkezin kuruluşunda Rusya Federasyonu İçişleri Bakanlığı'nın bizzat katılımı olduğu gibi finansmanını da Rospechat yapmaktadır. Rusça ve İngilizce dillerinde "www.friendlyrunet.ru" adresinden yayın yapan Merkez, 2010 yılında INHOPE'a üye olmuştur. İhbar merkezinin faaliyetleri Rusya'daki birçok resmi kurum, bakanlık ve Rus Ortodoks Kilisesi tarafından desteklenmektedir. Ayrıca ülkenin önde gelen birçok İnternet, haberleşme ve teknoloji şirketleri ihbar merkezi ile işbirliği yapmaktadır (Friendly Runet Foundation, 2012c).

Merkez, çocukların cinsel istismarı ve uyuşturucu kullanımını teşvik eden içeriklere ilişkin olarak e-posta ve çevrimiçi form yolu ile ihbar kabul etmekte ve ihbarları diğer INHOPE üyesi ihbar merkezleri gibi değerlendirmekte ve sonuçlandırmaktadır. E-posta adresi girilmiş ise, ihbarın değerlendirilmesinin her aşamasında ihbarı yapana durum ile ilgili bilgi verilmektedir (Friendly Runet Foundation, 2012d).

Friendly Runet, web sayfası güvenli İnternet kullanımı konusunda farkındalığın artırılması amacıyla çocuklar, gençler, ebeveynler ve eğitimciler için güvenli İnternet kullanımına yönelik zengin içerikler sunmakta, içerik riskleri, teknik anlamda güvenlik riskleri ve iletişim riskleri hakkında detaylı bilgiler vermektedir (Friendly Runet Foundation, 2012e). Ayrıca Rusya’da “www.interneshka.ru” adresinden Rusça ve İngilizce dillerinde yayın yapan ve sadece çocuklara hitap eden bir başka güvenli İnternet bilinçlendirme projesi de aktif olarak faaliyetlerine devam etmektedir (Interneshka, 2013).

2008 yılında kurulan ve Rusya’da faaliyet gösteren diğer bir INHOPE üyesi ihbar merkezi ise Saferunet’dir. Rusya Federasyonu’nca desteklenen bir grup STK’ca kurulan bu Merkez, “www.saferunet.ru” adresinden Rusça ve İngilizce dillerinde yayın yapmaktadır. Aynı zamanda INSAFE üyesi bir güvenli İnternet merkezi olarak da çalışan Saferunet, bilinçlendirme ve yardım hattı işlevlerinin tümünü içine almaktadır. Finansmanını Rospechat’ın yaptığı Merkez, hükümet, polis teşkilatı, İnternet sektörü ve STK’lar ile işbirliği halinde faaliyetlerini sürdürmektedir (Saferunet, 2013a).

İhbar merkezi, İnternet ortamındaki çocukların cinsel istismarı içerikleri, ırkçılık, yabancı düşmanlığı, terörizm propagandası, grooming, siber zorbalık, dini mezheplerin propagandası, şiddet, suça teşvik, uyuşturucu madde reklamı ve satışı, finansal ve yazılımsal saldırılar ile ilgili ihbarları kabul etmektedir (Saferunet, 2013b). İhbar alındıktan sonraki süreç burada da INHOPE üyesi diğer ihbar merkezlerindeki benzerlik göstermektedir. Sadece ihbar ile tespit edilen yasadışı içerik ülkede barındırılıyor ise İSS’sı ve yer sağlayıcısı yanında alan adını aldığı alan adı kayıt şirketine de bilgi verilmektedir (Saferunet, 2013a).

Saferunet web sitesi, ayrıca yardım hattı ve bilinçlendirme görevlerini de yerine getirmektedir. Yardım hattı telefon, e-posta ve çevrimiçi form ile İnternet ve bilgisayar konularında gençlere ve ebeveynlere danışmanlık ve psikolojik yardım sağlamaktadır (Saferunet, 2013c). Bilinçlendirme için sitede İnternet ortamında karşılaşılabilecek tüm tehlikeler, saldırılar ve bunlara maruz kalınması durumunda

yapılması gerekenler detaylı bir biçimde anlatılmaktadır (Saferunet, 2013d). Bu konuda INSAFE üyesi web siteleri arasında en kapsamlı ve kullanımı en kolay olanlardan birisidir ve son derece günceldir. Güvenli İnternet Kullanımı, siber suçlarla mücadele gibi konularda dünyadaki tüm gelişmeleri izlemekte ve takipçilerine ulaştırmaktadır (Bozkurt, 2012: 89). Rusya’da ayrıca bir de İnternet etiği konusunda yayın yapan güncel bir bilgilendirme ve bilinçlendirme sitesi de vardır (Etika, 2013).

“Saferunet” ana portalından ayrı olarak Rusya’da güncel çocuk güvenliği konularına ayrılmış birçok özel proje vardır. Aralık 2008’de başlayan “Ne Dopusti” (Olmasına İzin Verme) özel projesi, kaçırılma sorunu ve kaçırılmış çocukların yasadışı içerik üretmek için istismara maruz kalmasına odaklanmıştır. Proje, Rusya Kayıp ve İstismara Uğramış Çocuklar Ulusal Merkezi tarafından yürütülmekte ve İnterneti kullanarak, mağdurları bulmak ve mağdurların rehabilitasyonu ile ilgilenmektedir (Nedopusti, 2013). “Huliganam.net” projesi sanal tacize odaklanırken (Saferunet, 2013e), “Narkomanam.net” ise İnternet üzerinden çocuklar ve gençler arasında uyuşturucu dağıtımı sorunu üzerinde çalışmalar yapmaktadır (Narkomanam, 2013).

Diğer yandan, Temmuz 2012’de Başkan Putin’in imzası ile yürürlüğe giren yeni bir yasa ile Roskomnadzor Kurumu’na mahkeme kararı olmaksızın bazı içerikleri kara listeye alma ve bu sitelere erişimi engelleme imkanı verilmiştir. Yasaya göre, çocuklara cinsel taciz ve çocuk pornosu, intihara yönlendirme ve uyuşturucu kullanımını teşvik eden sitelerin erişimi engellenecektir (Hürriyet, 01.11.2012) ve Roskomnadzor Kurumu “zapret-info.gov.ru” sitesinde, yasaklanmış sitelerden oluşan “kara liste”yi yayınlanacaktır. Ayrıca isteyen herkes bilgi kirliliği oluşturduğu veya zararlı olduğunu düşündüğü her türlü siteyi “zapret-info.gov.ru” üzerinden ihbar edebilecektir. Toplanan bilgilere göre söz konusu İnternet siteleri uygunsuz bulunursa “kara liste” ye eklenecek ve İSS’lar ve yer sağlayıcılar üzerinden Kurum’un insiyatifi ile kapatılabilecektir (Haberrus, 03.11.2012).

Yasanın kabul edilmesinin ardından, insan hakları örgütleri ülkede sansürü artıracaklarını savundukları bu Yasa’yı şiddetle eleştirirken, Rus arama motoru devi

Yandex, sosyal medya portalı Mail.ru ve Wikipedia'nın Rusça bölümü, yasanın İnternette yargısız sansüre yol açacağını ve bir şekilde kendilerine erişimin de engellenebileceğini ileri sürerek durumu protesto etmiştir (Hürriyet, 01.11.2012).

Rusya'da büyük ISP'ler ya devlete ait ya da önemli bir devlet katılımını içermektedir (OpenNet, 2010b). Bunun da etkisi ile devlet politikası olan çocuk istismarıyla mücadele kapsamında Rusya'daki büyük İSS'lar 2010 yılında kendi aralarında yaptıkları özel bir anlaşma ile çocuk pornografisine ait içeriklerle mücadele edeceklerini deklare etmişlerdir (Friendly Runet Foundation, 2012f). Bunun dışında Rusya'daki İSS ve içerik sağlayıcıların çoğu kendilerine yasadışı içerik bildirilmesi durumunda içeriği kaldırma veya engelleme konusunda gerekeni yapacağına dair ilgili kamu kurumları ile resmi anlaşmalar imzalamıştır (OpenNet, 2010b). Diğer yandan, 2012'de Google Arama Motoru ve Youtube Video Servisi Roskomnadzor Kurumu ile "zapret-info.gov.ru" sitesinde yayınlanan "kara liste" yi referans alarak Rusya'da erişim engelleme yapmak üzerine anlaşmıştır (Haberrus, 03.11.2012).

2007 Temmuz'unda Putin, Rusya'yı küresel bir bilgi teknolojisi gücü yapmak istediğini ve bunun için bir adım olarak Rusya, Birleşik Devletler Topluluğu ve Bulgaristan'ın kullanacağı Kiril dilinde, kendi kendine yeten bir World Wide Web başlatmakta kararlı olduklarını açıklamıştır. Rusya, Çin'in dışında bu iradeyi ortaya koyan tek ülkedir. 2008 Haziran'ında, ICANN Kiril ve Çince dil tabanlı web teklifini görüşmüş ve bu fikrin İnternetin geliştirilmesi için doğru bir hareket olsa da, aynı zamanda İnternette devlet sansürünü daha kolay bir hale getireceğine ilişkin endişelerini de dile getirmiştir. Rusça web sitelerinin yönetiminin bir kuruluşun elinde yoğunlaştığı durumunda, bağımsız düşüncelerin yer aldığı online medya ve blogcuların sansür ile karşı karşıya kalabileceğini savunmuştur (OpenNet, 2010b).

Görüldüğü gibi Rusya Federasyonu'nun İnternetin düzenlenmesiyle ilgili olarak daha çok üzerinde durduğu konu, ulusal güvenliğe zarar vermek ve terörist faaliyetlerde bulunmak için İnternetin bir araç olarak kullanılmasıdır. Fakat bu konuların yoruma açık olmalarından dolayı hükümetin bunu bir gerekçe olarak değerlendirerek muhalif

görüşlerin İnternette yer bulmasını engellemeye ve iletişim özgürlüğünü zedeleyici uygulamalara vesile kılacağı noktasında ciddi eleştiriler yapılmaktadır.

Rusya çocuk istismarı ve pornosu, şiddet, ırkçılık ve yabancı düşmanlığı, intihara yönlendirme ve uyuşturucu kullanımını teşvik etme gibi konulara ilişkin İnternet içerikleri ile mücadele etmektedir. Bu amaçla yürütülen çalışmalarda temel yönetsel yaklaşımın devletin doğrudan müdahale ve mücadele etmesi yönünde olduğu görülmektedir. Sektördeki en güçlü kuruluşların devlete ait olmasının da sağladığı avantajla, içerik düzenlemesine ve uygulamasına ilişkin her türlü faaliyetin içinde kamunun varlığı gözlemlenmektedir. Ülkede genel olarak ve bu alanda güçlü STK'ların bulunmaması da bu sonucun ortaya çıkmasına katkıda bulunmaktadır.

2.5.2.7 Brezilya

Brezilya 90 milyona yaklaşan İnternet kullanıcısı ile %46'ya yaklaşan İnternet kullanım oranına sahiptir (internetworldstats, 2012d). Ülkenin demokratik ülkelere örnek olabilecek yönetim prensibini esas alan kendine özgü bir İnternet yönetimi ve yasadışı ve zararlı İnternet içeriği ile mücadele yöntemi ve sistemi vardır.

2.5.2.7.1 Yasal Çerçeve

Brezilya yasalarına göre çocuk pornografisi, ırkçılık, yabancı düşmanlığı, dini hoşgörüsüzlük, eşcinsel düşmanlığı, hayvanlara karşı kötü muamele ve insan kaçakçılığı zararlı ve yasadışı içerik olarak kabul edilmiştir (SaferNet Brasil, 2013b).

Bunlardan özellikle çocuk pornografisi en çok üzerinde durulan konulardan birisidir. Brezilya çocuk pornografisi konusunda BM Çocuk Haklarına Dair Sözleşme'ye ek çocuk pornografisi ile ilgili seçmeli protokolü 2004 yılında onaylamış ve iç hukukuna uyarlamıştır. Buna göre, Çocukların ve Ergenlerin Statüsü Yasası ile her türlü iletişim ortamında olduğu gibi İnternet ortamında da temsil, gerçek ya da simüle edilmiş olarak cinsel aktivite yapan bir çocuğun ya da cinsel amaçlı olarak cinsel uzuvlarının yer aldığı görüntülerin üretilmesi, satılması, tedarik edilmesi, dağıtılması veya yayınlanması suç kabul edilmiştir (Planalto, 2013a).

1988 Brezilya Federal Cumhuriyeti Anayasası'nın temel amaçlarından birisi köken, ırk, cinsiyet ve renk ayrımcılığının önlemesidir (Planalto, 2013b). Bu nedenle 1989 tarihli Irk Veya Renk Önyargılarından Kaynaklanan Suçlar Yasası ile Brezilya'da ırkçılık, yabancı düşmanlığı, Neo-Nazizm ve dini ayrımcılık yasaklanmış ve suç olarak düzenlenmiştir. Buna göre, herhangi bir birey ya da gruba yönelik olarak ırk, renk, din, soy ya da ulusal veya etnik köken, yaş ve cinsiyet gözetilerek nefret, ayrımcılık veya şiddeti teşvik eden her türlü yazılı, sesli veya görüntülü materyal yasaklı olarak belirlenmiştir. Bu bağlamda ülkede eşcinsel ayrımcılık ve düşmanlık da yasaklanmıştır. Dolayısıyla bahsi geçen konulara ilişkin İnternet içerikleri de yasadışı görülerek mücadele kapsamına alınmıştır (Planalto, 2013c).

Brezilya'da, yasaklı içerik türlerinden birisi de insan ticaretine ait materyallerdir. Ülkede, ülke içinde veya diğer ülkelerle bağlantılı olarak cinsel sömürü amacıyla ya da çocuk işçi olarak veya organ kaçakçılığı için insan ticareti yapmak suçtur. Aynı şekilde organ ticareti de yasaklanmıştır. Bu tür faaliyetlerin İnternet ortamında yapılması ya da teşvik edilmesi de suç kabul edilmiştir (SaferNet Brasil, 2013b).

Diğer yandan, Brezilya'da hayvanlara kötü muameleyi gösteren içerikler zararlı içerik olarak değerlendirilmektedir. Buna göre, evcilleştirilmiş veya yabani tüm hayvanlara yönelik istismar, yaralama veya sakatlamaya dair içerikler kötü muamele kapsamında istenmeyen içeriktir (SaferNet Brasil, 2013b).

2.5.2.7.2 İçerik Düzenleme Politikası

Brezilya'da İnternet yönetim sistemi, yönetim temelinde, kamu kurumları, özel sektör kuruluşları ve STK'ların değişik konu ve düzlemler bağlamında özel anlaşmalar yapma ve işbirliği geliştirmeleri üzerine oturmuştur. Ülkede İnternet yönetişimi sisteminin merkezinde birisi kamu, diğeri STK olmak üzere iki kurum vardır. Sistemin merkezindeki kamu kurumu İnternet Yürütme Kurulu (CGI.br), STK ise "SaferNet Brasil" dir.

Brezilya'nın İnternet yönetişimi sistemi, İnternetin yönetilmesi ve kullanımı konusundaki kararların toplumun etkin katılımı ile alınmasına ilişkin yenilikçi bir

deneyimdir. Çok-terafli, Őeffaf ve demokratik ilkelere dayandırılarak, ũlkedeki İnternet faaliyetlerinin koordinasyonu ve entegrasyonu Brezilya İnternet Yũrũtme Kurulu tarafından yũrũtũlũrken, bu Kurum’un en bũyũk partneri ve destekŐisi “SaferNet Brasil” dir (CGI.br, 2013a).

1995 tarihli Bakanlar Kurulu Kararı (CGI.br, 2013b) ile UlaŐtırma Bakanlıđı ile Bilim, Teknoloji ve İnvasyon Bakanlıđınca oluŐturulan Brezilya İnternet Yũrũtme Kurulu, 2003’de Cumhurbaşkanlıđı Kararnamesi ile kısmi deđiŐikliđe uđramıŐtır (CGI.br, 2013c). Brezilya İnternet Yũrũtme Kurulu’nun sorumlulukları arasında teknik kalitenin yũkseltilmesi, sunulan hizmetlerin geliŐtirilmesi ve yaygınlaŐtırılması, e-gũvenlik farkındalıđının artırılması vardır (CGI.br, 2013d).

Kurul’un resmi gŕev ve sorumlulukları ūunlardır: İnternet faaliyetlerinin dũzenlenmesine iliŐkin politikalar ve usuller geliŐtirmek, İnternet hizmetleri iŐin teknik standartları ve prosedurleri belirlemek, İnternet kullanımı ve geliŐimi ile ilgili stratejik direktifler oluŐturmak, ũlke ađları ve hizmetlerinin gũvenliđi iŐin ŐalıŐmalar yapmak ve teknik standartları belirlemek, IP atama ve alan adları kaydını koordine etmek, İnternet hizmetleri ile ilgili veri, gŕsterge ve istatistiklerin toplanması ve bilgilerin yaygınlaŐtırılması (CGI.br, 2013d).

Őoklu-paydaŐ yapısı olan İnternet Yũrũtme Kurulu, bũnyesinde hũkũmetten, iŐ-ticaret sektŕrũnden, yazar ve dũŐũnũrlerden ve akademik topluluktan temsilciler barındırmaktadır. Kurul, hũkũmet kanadından 9, sivil kanattan ise 12 olmak ũzere toplam 21 ũyeden oluŐmaktadır (CGI.br, 2013e). 2004 Temmuz’undan bu yana, Kurul’daki sivil toplum temsilcileri demokratik yŕntemlerde seŐilmekte ve İnternet ile ilgili tartıŐmalara ve gŕrũŐmelere hũkũmet ile birlikte dođrudan katkı sađlamaktadır. Ayrıca, Kurul’un yılda bir defa ũlkenin tũm bŕlgelerinden ve Brezilya toplumunun bũtũn sektŕrlerden katılımcıların yer aldıđı ve İnternet konuları ũzerine tartıŐmaların yapıldıđı ŕzel toplantıları da bulunmaktadır (CGI.br, 2013f).

Kurulun ayrıca ũlkede İnternetin iŐletilmesi ve geliŐtirilmesiyle ilgili ŕnemli alanlarda projeler geliŐtirmek ve koordinasyon sađlamaktan sorumlu ŐalıŐma

komiteleri bulunmaktadır. Bu komitelerden birisinin konusu da İnternet içeriğidir. Bu komite 10 kişilik ekibi ile Portekizce kaliteli içerik üretmekten yasadışı ve zararlı içerik sorununa değin akla gelebilecek tüm içerik sorunlarına ilişkin olarak, incelemeler ve araştırmalar yapmak ve yaptırmak; çalıştay, seminer ve toplantılar düzenlemek; ilgili tüm kamu, özel ve akademik kurumlarla işbirliği ve yardımlaşma imkanları aramak; projeler yapmak ve yaptırmak gibi faaliyetler yürütmektedir (CGI.br, 2013g).

Brezilya İnternet yönetim sisteminin diğer önemli unsuru olan “SaferNet Brasil” ise, “Bilgi Toplumunda İnsan Haklarının Korunması” sloganı ile İnternetin güvenli kullanımını sağlamak, başta çocuklar olmak üzere tüm toplum kesimlerini İnternetten gelebilecek zararlardan korumak ve insan hakları ihlallerinin önüne geçebilmek amacıyla kurulmuş kar amacı gütmeyen bir STK’dır (SaferNet Brasil, 2013c). Bir grup bilgisayar uzmanı, araştırmacı, hukukçu ve akademisyen tarafından 2004 yılında kurulan “SaferNet Brasil”, kuruluşundan bu yana İnternetin çocuk ve gençlerin cinsel istismarına yönelik görüntülerin üretimi ve yayılması, ırkçılık, Neo-Nazizm, dini hoşgörüsüzlük, insanlara ve hayvanlara karşı kötü muamele gibi suçlarda kullanımını önlemek için kalıcı ve etkili bir mücadele vermektedir (SaferNet Brasil, 2013d).

“SaferNet Brasil” bu çerçevede Federal Hükümet, Federal Kamu Bakanlığı-Federal Devlet Başsavcılığı Ofisi, Federal Polis Teşkilatı, Cumhurbaşkanlığına bağlı Özel İnsan Hakları Sekreterliği, İnternet Yürütme Kurulu ve Federal Çocuk Cinsel Tacizlerinin Soruşturulması Özel Senato Komisyonu gibi kamu kurumları yanında, Avukatlar Genel Ulusal Konseyi ve Brezilya Çocuk gibi STK’lar ve Google, MySpace, yerli büyük Telekomünikasyon Şirketleri (Telekom Brezilya, HI, TIM) ve Brezilyalı İnternet Sağlayıcıları Derneği ile yakın işbirliği içinde çalışmaktadır. Dernek, bahsi geçen devlet ve özel kurumlarla işbirliği anlaşmaları yapmakta veya diğerleri arasında yapılan anlaşmalara taraf olmaktadır (SaferNet Brasil, 2013d).

“SaferNet Brasil” in en yakın çalıştığı ve işbirliği yaptığı kamu kurumlarından birisi Federal Devlet Başsavcılığı ve bunun üzerinden Eyalet Başsavcılıkları’dır. Dernek,

2006 yılından bu yana Eyalet Başsavcılıkları ile ayrı ayrı teknik, bilimsel ve operasyonel işbirliği anlaşması imzalamaktadır.⁵⁷ Bu çerçevede Başsavcılıklar, “SaferNet Brasil” ile birlikte bir yandan sanal suçlara karşı mücadelede verirken diğer yandan ebeveynler, öğretmenler ve öğrenciler için eğitimler düzenleyerek Brezilya’da İnternetin daha güvenli olması için tanıtım çalışmalarına destek olmaktadır. Ayrıca, Brezilya İnternet Yürütme Kurulu, Polis Teşkilatı, “SaferNet Brasil”, STK’lar ve özel sektör ile birlikte çalışarak, sanal suçlar karşısındaki mücadelede yerel mevzuat, teknoloji ve işlem altyapısının güçlenmesi amacına yönelik çalışmalar yürütmektedir (SaferNet Brasil, 2013e).

Başsavcılıklar ile “SaferNet Brasil” ortaklığında yürütülen önemli bazı çalışmalar şunlardır (SaferNet Brasil, 2013e):

- Bilişim Suçları İçin Ulusal Şikayet Merkezi oluşturulmuş ve 2006 yılından bu yana “SaferNet Brasil” in yönetiminde ulusal ihbar merkezi olarak faaliyetlerini sürdürmektedir (SaferNet Brasil, 2013f). INHOPE üyesi olan Merkez, çocuk pornografisi, ırkçılık, dinsel hoşgörüsüzlük, Neo-Nazizm, yabancı düşmanlığı, eşcinsel düşmanlığı, insanlığa karşı işlenen suçları (soykırım, katliam vb.) kışkırtma ve hayvan istismarına karşı içeriklerle ilgili ihbar ve şikayetleri “www.denunciar.org.br” web adresinden almaktadır (SaferNet Brasil, 2013g). Merkez, ihbarları anonim olarak da alabilmekte ve her aşamada ihbarda bulunana bilgi vermektedir. İhbarlar önce Merkez’deki uzman hukukçu ve bilgi teknolojisi uzmanlarınca hukuki ve teknik analize tabi tutulmaktadır. İçerik yasadışı ve ülke içinde barındırılıyor ise ilgili Başsavcılığa ve Polise gönderilmektedir. Ayrıca, ilgili İSS’den içeriğin kaldırılması talep edilmektedir. İçerik yurtdışı kaynaklı ise ilgili ülkenin INHOPE üyesi ihbar merkezlerine, bu yoksa İnterpol üzerinden ilgili ülkeye yönlendirilmektedir (SaferNet Brasil, 2013h).

⁵⁷ Anlaşmalar için Bkz. Sao Paulo Başsavcılığı (29/03/2006), <http://www.safernet.org.br/site/institucional/parcerias/mpf-sp>; Rio Grande do Sul Başsavcılığı (25/10/2006), <http://www.safernet.org.br/site/institucional/parcerias/mpf-rs>; Rio de Janeiro Başsavcılığı (13/11/2006), <http://www.safernet.org.br/site/institucional/parcerias/mpf-rj>; Goiás Başsavcılığı (12/03/2007), <http://www.safernet.org.br/site/institucional/parcerias/mpf-go>, Parceria Başsavcılığı (14/06/2007), <http://www.safernet.org.br/site/institucional/parcerias/mpf-pr> (28.2.2013)

- 2005 yılında Brezilya'nın ana İnternet hizmet sağlayıcıları ile işbirliği anlaşması yapılmıştır. Buna göre, hizmet sağlayıcılar, İnterneti suç işleme amacıyla kullanan Brezilyalı kullanıcıların tespit edilmesi ve savcıların kovuşturma yapılabilmesi için işbirliği ve destek sağlamayı kabul etmişlerdir.
- 2 Temmuz 2008'de "SaferNet Brezilya", Federal Devlet Başsavcılığıyla Google firması arasında, "on-line çocuk güvenliği" üzerine bir uluslararası anlaşma imzalanmıştır. Bu anlaşma ile Google Brezilya, Orkut servisi kullanılarak yapılmış olan mesajlaşma, video paylaşımı, imaj, foto işlemlerindeki trafik bilgilerini 180 gün süre ile saklamak, adli makamlardan veya soruşturmaya yetkili mercilerden gelecek talepler doğrultusunda bunları göndermek ve takibat konusu olan materyalleri daha uzun süre saklamak, Savcılar Ofisi ile aralarında on-line bağlantılar kurmak, ihbar edilen materyali 72 saat içerisinde yayından kaldırmak, web sayfasında yasal uyarılar ve ihbar hatları oluşturmak, çocuk pornosu ve istismarına ilişkin mücadelede yeni metodlar ve araçlar ortaya çıktığında bunları kullanmak, bu konuda mücadele eden uluslararası kuruluşlarla işbirliği yapmak vb. yükümlülükler altına girmiştir (SaferNet Brasil, 2013₁, 2013₂).
- Başsavcılık, 2005 yılına "Sanal Suçlar: Araştırmalar için Uygulama Kılavuzu" yayınlamıştır. Bu yayın Brezilya İnternet Yürütme Kurulu'nun desteği ile ülke çapında hakimler ve diğer yasa uygulayıcılarına dağıtılmıştır.
- Federal Çocuk Cinsel Tacizlerinin Soruşturulması Özel Senato Komisyonu'na teknik destek sağlanmaktadır.

"SaferNet Brezilya", Federal Polis Teşkilatı ve Cumhurbaşkanlığına bağlı Özel İnsan Hakları Sekreterliği ile 2008 yılında İnternette insan haklarına karşı işlenen suçlarla mücadele edilmesiyle ilgili üçlü bir işbirliği anlaşması imzalamıştır. Buna göre, başta çocuk pornografisi olmak üzere insan haklarına karşı işlenen suçlarla ilgili mücadelenin daha etkili bir biçimde yürütülebilmesi için tarafların ortak hareket etmesi öngörülmüştür. Bu çerçevede söz konusu içeriklere ilişkin şikayetlerin 24 saatte sonuçlandırılması, içeriğin kaldırılması ve cezai işlem görmesini sağlamaya yönelik tedbirlerin alınması; bu tip suçlarla başa çıkmak için yeni teknolojiler oluşturmak ve geliştirmek için ortak çalışmalar yapılması; ortak kurslar, çalıştaylar

ve diğer eğitim faaliyetleri yoluyla bilgi alışverişinde bulunulması; konunun uzmanlarınca teknik not, rapor, doküman vs. hazırlanması ve yayınlanması; İnternetin güvenli ve etik kullanımı konusunda toplumda farkındalık oluşturacak ortak kampanyalar yapılması ve yapılanların teşvik edilmesi hususlarında birlikte hareket etmek konusunda anlaşmışlardır (SaferNet Brasil, 2013j, 2013k).

2008 yılında ise, Brezilya'nın önde gelen telekomünikasyon şirketleri ile (Telekom Brezilya, HI, TIM) Brezilya Federal Devlet Başsavcılığı ve Eyalet Başsavcılıkları, Federal Polis Departmanı ve "SaferNet Brezilya" ve İnternet Yürütme Kurulu çocuk pornografisi ve İnternet ortamında çocuklar ve ergenlerin istismarını ortadan kaldırmak için ortak mücadele yürütülmesi konusunda bir sözleşme imzaladılar. Buna göre, etkili mücadele için taraflarca tam bir işbirliği içinde hareket edilmesi ve alınacak yeni tedbirlerin neler olabileceği konusunda birlikte çalışmalar yapılması karara bağlanmıştır. Bu çerçevede, İSS'ların söz konusu içeriğin en hızlı bir şekilde kaldırılmasını temin etmesi, sorunun izlenmesi ve önlenmesi için İnternet Yürütme Kurulu bünyesinde bir daimi komite oluşturulması öngörülmüştür. Bu Komite'nin ayrıca, İnternetin güvenli kullanımı hakkında toplumu bilinçlendirmek için ortak kampanyalar düzenlemesi ve çocuklara yönelik cinsel suçlarla mücadele için teknoloji geliştirmek amacıyla çalışmalar/araştırmalar yapması kararlaştırılmıştır (SaferNet Brasil, 2013l, 2013m).

Ülkede "SaferNet Brezilya" tarafından Federal Devlet Başsavcılığı, Polis Teşkilatı ve İnsan Hakları Özel Sekreterliği'nin işbirliği ve desteği ile işlettiği bir Brezilya Yardım Hattı da bulunmaktadır. Bu hat "Helpline.br" adresinden toplumun her kesimine çevrimiçi online ve ücretsiz bir hattan telefonla İnternetin güvenli kullanımı ile ilgili yardım ve destek hizmetleri sunarken, aynı zamanda çevrimiçi cinsel taciz, şiddet, şantaj, aşağılama vb. olumsuz deneyimler yaşayan çocuklar ve ergenlere bilgi vererek rehberlik yapmaktadır. Ayrıca talep edenlere profesyonel ekibi ile psikolojik destek sağlamaktadır (SaferNet Brasil, 2013n).

"SaferNet Brezilya" ayrıca, resmi web sitesinde "Yasama Gözlemevi" (Observatório do Legislativo) adında bir platform oluşturmuştur. Burada, Temsilciler Meclisi ve

Senato’da bilişim suçlarıyla ilgilenen yasama birimleri ve kişiler ile STK’ları ve İnternet kullanıcılarını bir iletişim mecrasında buluşturmayı amaçlamıştır. İnternetle ve bilişim suçlarıyla ilgili yapılan yasama çalışmalarına, hazırlıklara, presedürlere ait bilgilerin verildiği ve takibinin yapıldığı; fikir ve düşüncelerin paylaşıldığı, istek, talep ve önerilerin ortaya konulduğu; projelerin sunulduğu, analiz, değerlendirme ve tartışmaların yapıldığı bir etkileşim ortamı oluşturulmaya çalışılmıştır. Bu şekilde özellikle seçilmişlere, konunun tarafı olan diğer kesimlerin taleplerini iletebilecekleri bir zemin oluşturulmuştur (SaferNet Brasil, 2013o).

Bütün bunların dışında “SaferNet Brezilya” ülkede İnternetin güvenli kullanımı konusunda bilinçlendirme faaliyetlerini yürüten en etkin STK’dır. Dernek, yukarıda sayılan ortaklarıyla birlikte, bu alanda faaliyet gösteren başka bir STK olan Brezilya Çocuk’u da yanına alarak, MySpace firması ile yapmış olduğu ve bilinçlendirme çalışmalarında ortak hareket etmeyi öngören özel anlaşmayla (SaferNet Brasil, 2013ö, 2013p), güvenli İnternet faaliyetlerinin merkezi olmaya devam etmektedir (SaferNet Brasil, 2013r). “SaferNet Brasil” son üç yıldır, BM’in İnternet yönetim sürecine ilişkin uluslararası faaliyetlerine katılım sağlamış ve gelişen ülkelerde çocuklara karşı işlenen cinsel suçların önlenmesi ve mücadelesi konularının tartışılması için iki büyük çalıştay düzenlemiştir (Safer Internet Day, 2013).

Nética platformu, SaferNet Brasil ve diğer ortaklarca “new.netica.org.br” adresinden eğitim almış tüm öğretmen ve sosyal hizmet görevlilerinin kullanımına açılmıştır. Eğitim setindeki tüm e-güvenlik materyalleri online olarak mevcuttur; projeler ve yeni fikirlerin geliştirilmesi için birçok farklı kaynak bulunmaktadır (Netica, 2013).

Görüldüğü gibi, İnternete ilişkin konularda ve İnternet içerik düzenlemesinde Federatif Devlet yapısı içinde Brezilya örneği, yönetim temelli farklı ve özgün bir model ortaya koymaktadır. İnternetle ilgili kamu, özel, STK tüm tarafların özel anlaşmalar yaparak uygulama zenginliği oluşturduğu bu model, mümkün olan en üst seviyede sivil toplumu ve sektörü temsilci kurumları ile karar ve uygulama süreçlerine katmayı öngörmektedir. Bu birlikte yönetme modelinde, devlet eli ile özellikle STK’lara öncelik ve inisiyatif sağlanmaya çalışılması dikkat çekmektedir.

2.5.2.8 Çin Halk Cumhuriyeti

Çin Halk Cumhuriyeti 2012 yılı itibariyle, 538 milyon İnternet kullanıcısı ile %40,1'lik İnternet kullanım oranına sahiptir (internetworldstats, 2012f). Bu kullanıcı sayısı ile Çin, Dünyanın en çok İnternet kullanıcısı bulunan ülkesidir ve bu sayı Dünyadaki toplam İnternet kullanıcılarının oransal olarak %22,4'üne tekabül etmektedir (internetworldstats, 2012g). Dolayısıyla Çin, Dünyanın en büyük İnternet aktörlerinden birisidir. Bunun yanında Çin, ülkede İnternet içeriğine uyguladığı sansür ve İnternet üzerinde kurulan denetim ve kontrol açısından da dünyada en çok eleştirilen ülkelerin başında gelmektedir (Wolfgarten, 2005/2006).

Çin'de her ne kadar ifade hürriyeti, özgürlükler ve insan haklarına saygı konuları anayasada düzenlenmekte ve güvence altına alındığı belirtilse de Çin Komünist Partisi diğer tüm medya ve iletişim araçlarını olduğu gibi İnterneti de kontrol ve denetim altında tutmaktadır (Deibert vd., 2008: 265). Nitekim Çin, 1990 yılında İnternet ağına dahil olmuş fakat gerekli denetim ve kontrol sistemlerini kuruncaya kadar İnterneti kamusal kullanıma açmamıştır (Kaya, 2010: 61).

Çin ülkenin geniş coğrafyasının tamamında etkin olan dünyanın en sofistike İnternet erişim engelleme ve takip sistemini kullanmaktadır (Dailybits 2008). Bu amaçla geliştirdiği resmi adı “Altın Kalkan Projesi” olan ve “Büyük Ateş Duvarı” olarak da anılan proje, Çin Halk Cumhuriyeti Sosyal Güvenlik Bakanlığı tarafından yürütülen bir sansür ve gözetim projesidir (Fallows, J. 2008). 2002'da etkin hale gelen Proje, Çin halkının güvenliği için oluşturulduğu iddia edilen güçlü bir dijital izleme ağıdır. Bu sistem ülke genelinde her bir İnternet noktasını kontrol edebildiği için Büyük Çin Seddi'ne benzetilerek Büyük Çin İnternet Duvarı veya Çin Güvenlik Seddi olarak da adlandırılmaktadır (Goldsmith ve Wu, 2006: 92; Wikipedia, 2011a). Çin bu sistemle hem ülkeden dışarıya hem de dışardan Çin'e olan veri akışını kontrol ederken, diğer yandan yasak sitelere erişimi engellemekte ve yasak kelimeler yazıldığı zaman bağlantıyı keserek gönderilmesine izin vermemektedir (Clayton, Richard, vd., 2006).

Çin, İnterneti kamusal alanının bir uzantısı olarak görmekte ve devlet tarafından denetlenmesi gerektiğine inanmaktadır. Bu nedenle İnternetin kullanılmaya başlandığı ilk dönemlerden itibaren istemediği içeriklere erişimini engellemeye ve vatandaşlarının İnternet aktivitelerini takip etmeye dayalı bir sistem kurmuştur (Kaya, 2010: 61). Nitekim Çin sosyal engelleme yöntemlerini de kullanarak, her İnternet bağlantı noktasında yer alan takip sistemleri sayesinde ülke genelinde erişim engellemeyi başarıyla sürdürmektedir (Deibert vd., 2008: 264). Ülkede bu işle ilgili olarak 30.000 kişinin görev yaptığı tahmin edilmektedir (Dailybits, 2008).

Çin her ne kadar komünist devlet sistemi nedeniyle siyasal ve yönetsel açıdan kapalı bir yapıya sahip olsa da, ekonomik gelişimin teknolojik altyapının güçlü olmasına bağlı olduğunun farkında olarak, İnternetin ekonomik kalkınmaya olan katkısından dolayı İnterneti tamamen yasaklamamaktadır. Hatta bir yandan dünyanın en gelişmiş ağ altyapısına sahip olmak için büyük yatırımlar yaparken, diğer yandan Dünya Ticaret Örgütü'ne üye olmak için, telekomünikasyon sektörü de dahil, birçok alanda yabancı yatırımcılara karşı sınırlamaları kaldıracağı taahhüdünde bulunmaktadır. Bu nedenle yabancı sermayenin Çin'deki yatırımlarının artmasının Çin'deki İnternet yasaklarını belirli bir ölçüde yumuşattığı dile getirilmektedir (Kaya, 2010: 61-62).

Bu noktada aslında Çin birçok otoriter devletin İnternetle ilgili karşılaştığı temel bir ikilemi yaşamaktadır. Bir yandan İnternet'in ülke genelinde yaygınlaşmasının ülkesine beraberinde kontrol edemeyeceği miktarda bilgi akışı getireceğinin farkında olmasına rağmen, gelişmekte olan ekonomisine katkıda bulunması için İnterneti yaygınlaştırmaya çalışmakta; diğer yandan ise komünist düzeni korumak için vatandaşlarının İnternetteki her adımını izlemekte ve istenmeyen içeriğe anında müdahale etmektedir (Goldsmith ve Wu, 2006: 89,101). Nitekim Çin, 2010 yılında İnternet stratejilerini açıklayan bir "whitepaper" deklare etmiştir (Information Office of the State Council, 2010). Bu belgede, bahsi geçen ikilem açık bir şekilde kendisini göstermiştir. Belgede İnternetin yaygınlaştırılması ve zımni olarak sansür politikaları birlikte savunulmaktadır. Bu durum Çin'de İnternet özgürlüğünün devletin komünizm ilkelerine aykırı bulmadığı sınırlar içerisinde ve izin verilen alanlarda varlığını sürdürmesi sonucunu doğurmaktadır (Talbot, 2010; Kaya, 2010: 62).

Diğer yandan, Çin'in kurduğu ve Büyük Çin İnternet Duvarı olarak anılan sistemin CISCO, Yahoo, Google, Microsoft gibi ABD şirketlerinin çeşitli düzeylerdeki teknolojik işbirliğiyle geliştirilmiş olması da ilgi çekici bir noktadır. Routerların taşınan veriyi ağda kaybetmek için de kullanılabileceğini fark eden Çin, dünyanın en büyük router üreticisi olan CISCO firmasından tüm Çin'i kapsayacak bir İnternet duvarı geliştirmesini istemiştir. İnternet duvarı, çalışanların İnternette zararlı sitelere girmelerini engelleyen ve ziyaret ettikleri siteleri kaydeden klasik İnternet filtreleme sistemlerinden esinlenerek üretilirken, İnternet bağlantı hızında önemli bir yavaşlamaya da neden olmamaktadır. İnternet duvarının bu kadar hızlı çalışması, iletmesi gereken tüm postaları çöpe atan postacının hızına benzetilmektedir (Goldsmith ve Wu, 2006: 93-94; Zuckerman, 2008).

Çin, Yahoo, Google, Microsoft gibi ABD menşeli büyük bilişim şirketlerini işbirliğine zorlamakta ve ülkede faaliyet gösterebilmelerini sistemlerini ülkenin İnternet politikalarıyla uyumlu hale getirmeleri şartına bağlamaktadır (Ifex, 2011). Bu işbirliği ile erişim engelleme ve takip politikasını başarıyla sürdürmektedir. Buna göre, bir suç şüphesi olduğunda Çinli yetkililerin isteği üzerine gereken bilgiler iletişimin ve özel verilerin gizliliği gibi sorgulamalara tabi tutulmaksızın bizzat bu büyük şirketler tarafından Çinli makamlara sunulmaktadır (Kaya, 2010: 63). Nitekim 2006 yılında, sadece Yahoo'nun kendi kullanıcılara ait bilgileri Çin devleti ile paylaşması sonucunda bir bölümü gazeteci 52 kişi İnternet faaliyetleri nedeniyle tutuklanmıştır (Deibert vd., 2008: 266). Yine bu işbirliğinin bir sonucu olarak, bu şirketlerin sunduğu arama motoru, blog gibi servislerde özgürlük ve demokrasi gibi kelimelerin kullanılması yasaklanmıştır (Goldsmith ve Wu, 2006: 95).

Bu büyük ABD şirketlerinin, Çin hükümeti ile İnternet üzerinden temel hak ve hürriyetleri kısıtlamaya yönelik olarak işbirliği yapmaları çeşitli tepkilere neden olmaktadır. Şirketler, faaliyet gösterdikleri ülkelerdeki yasalara uymak zorunda olduklarını gerekçe göstererek yapmış oldukları işbirliğini haklı kılmaya

çalışmaktadır.⁵⁸ Buna rağmen söz konusu şirketlerin ticari çıkarları için Çin’de kendi kurumsal ilkelerini açıkça çiğnedikleri görülmektedir (Kaya, 2010: 63).

Çin’in hangi İnternet içeriğine müdahale edeceği ve bu mücadeleden sorumlu kamu kurumun hangisi olduğu 25.11.2005 tarihli “Provisions on the Administration of Internet News Information Services” isimli Enformasyon Teknolojileri Bakanlığı düzenlemesinde belirlenmiştir. Bu düzenlemeye göre ülkede İnternet içeriğinin düzenlenmesi ve kontrolünden sorumlu kurum olarak Enformasyon Teknolojileri Bakanlığı belirlenmiştir. Düzenlemenin 19. maddesinde ise; anayasada yer alan ilkeleri ihlal eden, ulusal güvenliği ve bütünlüğü tehdit eden, asılsız söylentilere yol açan, kamu düzenini bozan, dirlik ve esenliği ihlal eden, sosyal düzeni bozan toplantı veya gösteriler düzenlenmesini teşvik eden, yasadışı bir oluşum adına hareket eden, devlet sırlarını ifşa eden, ulusal menfaatlere zarar veren, ırkçılığa sevk eden, dinle ilgili politikaları ihlal eden ve batıl inançlar yayan, müstehcenliği, pornografiyi, kumarı, şiddeti, terörü yayan veya suça teşvik eden, üçüncü kişilere hakaret eden veya onların yasal hak ve menfaatlerini ihlal eden veya diğer kanunlarca yasaklanan her türlü içeriğin engelleneceği kayıt altına alınmıştır (News.xinhuanet, 2005).

Yasaklara ilişkin yasal sınırların bu kadar kapsamlı tutulması nedeniyle Çin’deki İnternet sitelerinin erişime engellenmesine yönelik uygulamalar müstehcenlik ve pornografi ile birlikte siyasi, dini, diplomatik ve eğitim gibi konuları da kapsayan geniş bir alana yayılmıştır (Bulut, 2009).

⁵⁸ 2006’da İnternet Yönetişimi Forumu (IGF)’nin, “Açıklık” başlıklı oturumunda söz konusu şirketlere yapılan eleştiriler için bkz. BBC News, “**Microsoft Considers China Policy**”, 01.11.2006, <http://news.bbc.co.uk/2/hi/technology/6102180.stm> (13.12.2011); Keza, Uluslararası Af Örgütü (UAÖ) Genel Sekreteri Irene Khan konuyla ilgili şunları söylemiştir: “UAÖ giderek büyüyen bu küresel eğilimden kaygı duymaktadır. İster Çin yetkililerinin taleplerine direnemedikleri için, isterse hükümetin kaygılarını tahmin ettikleri için olsun, insan haklarını ihlal eden kısıtlamalar uygulayan şirketler son derece basiretsizdir. Endüstrinin Çin hükümetiyle gerek zımnı gerekse yazılı anlaşmalar yapması, IT endüstrisinin herkes için, her yerde ve her zaman bilgi edinme özgürlüğünü savunduğu iddialarıyla çatışmaktadır... Küresel şirketler ve Çin yetkilileri arasındaki anlaşmalar, Çin’de İnternet sansürünün bir norm olarak yerleşmesini sağladı. İnternet şirketleri bu yaptıklarına mazeret olarak Çin yasalarını gösteriyor. Aslında bu tür anlaşmalar ve bunların sonucunda ortaya çıkan oto-sansür hem uluslararası standartları hem de ifade özgürlüğünü koruma altına alan Çin Anayasası’nı ihlal ediyor. İnternet, sınırsız bir dünyada kısıtsız bilgiye erişimin müjdesini vermişti. Oysaki hükümetlere yardım eden şirketler o ülkenin vatandaşlarının bilgiye erişimini engellemek üzere sınırlar inşa ediyorlar.” (Amnesty, 2011).

Bu düzenlemeyle devlet tarafından tehlikeli ve hassas görülen her konu yasaklı içerik kapsamına alınmış ve keyfi uygulamalara zemin hazırlanmıştır. Keza, ülkede bu tür uygulamalara sıkça rastlanmaktadır. Örneğin, Çin Uluslararası Çalışma Örgütü'ne üye olmasına rağmen ülkedeki işçi haklarına uygunluğu takip eden sitelere erişim engellenmektedir (Deibert vd., 2008: 267). Yine, ulusal güvenlik sebebiyle Doğu Türkistan, Uygur, Tibet, Moğol gibi azınlık siteleri engellenirken; din politikalarına aykırılık gerekçesiyle de Hristiyan, Müslüman, Yahudi veya Hindu dinlerine ilişkin içerikler engellemeye uğramaktadır (Goldsmith ve Wu, 2006: 94). Benzer şekilde, içlerinde Çin'in en büyük arama motoru olan "Baidu. com"⁵⁹ da yer aldığı arama motorları tarafından demokrasi, insan hakları, diktatörlük, zulüm, 4 Haziran (Tiananmen olayları), Tibet bağımsızlığı, Dalai Lama, Falun Gong gibi kelimelere sansür uygulanmaktadır (China Digital Times, 2009). Ayrıca, Youtube gibi bazı sosyal ağların da erişimi Çin otoritesince engellenmektedir (OpenNet, 24. 03.2009).

Diğer yandan Çin'de her türlü müstehcenlik ve pornografik içeriğe karşı katı bir mücadele yürütülmekte ve genel ahlaka aykırı ilişkilerin yazıldığı ve yayımlandığı İnternet blogları da dahil bu kapsamdaki her türlü içeriğe yönelik erişim engellemesi uygulanmaktadır. Bu çerçevede Çin, yetkilendirilmiş bulunduğu birçok kurum ile pornografiye karşı ciddi bir mücadele vermektedir (China.org, 2009).⁶⁰ Nitekim Çin hükümeti, pornografik içerikli siteleri engelleyen bir program geliştirmiş ve 2009'da "Yeşil Baraj Projesi" adıyla uygulamaya sokmuştur. Benzer şekilde "Google.cn" arama motorunun pornografik içerikli aramalara izin vermesinden dolayı Çin hükümetince uyarılmasından sonra "Google", Çin'de yayın yapan sunucusunda pornografik içeriği arama motorundan tamamen temizlemiştir (Topnews, 2009).

Çin İnternet Duvarı ile kurulan sistem, erişim engellemenin kapsamı bakımından hem İSS temelli hem ana İnternet omurgası temelli engelleme; teknik bakımdan ise

⁵⁹ Google arama motorunun İnternet sansürüne destek verme konusundaki isteksizliğinin bir sonucu olarak Çin hükümeti "Baidu. Com" adlı yerli arama motorunu geliştirmiş ve Çin'de kullanıma sokmuştur. Bu süreçte Çin, çok sayıda Amerikan mühendis ve yazılımcıyı Baidu'yu güçlendirmek için işe almıştır (Süer, 2010).

⁶⁰ Çin İnternette yer alan pornografik içerikle mücadelede ilginç yöntemlere de başvurmaktadır. Bunlardan birisi de porno siteleri bulup ihbar edenlerin devlet tarafından bin yuandan 10 bin yuana (2.100 lira) kadar ödüllendirilmesidir. (Hürriyet, 07.12.2009)

IP yoluyla, URL yoluyla, alan adı yoluyla ve içerik engelleme sistemleri kombine bir şekilde kullanılabilir. Çin sistemin etkinliğini korumak amacıyla bunun dışında erişim engellemelerini aşma yöntemleri ile ayrıca mücadele yürütmekte ve bu tür yöntemleri kullananları cezalandırmaktadır (Kaya, 2010: 62).

Çin İnternet Duvarı, insan hakları, demokrasi, siyasal reform, gibi bine yakın sözcüğe kelime bazlı içerik engellemesi tekniği ile otomatik olarak erişim engellemesi uygulamaktadır. Bu tür engellemelerin aşılması için ise içerik aldatması yöntemi yaygın olarak kullanılmaktadır. Çin'deki insan hakları siteleri demokrasi kelimesi yerine "lahana", çok partili sistem için ise "havuç" kelimesi kullanarak engellemeleri aşılabilmektedirler (Goldsmith ve Wu, 2006: 94, 103).

Çin, erişim engellemede sosyal teknikleri en çok kullanan ülkelerden birisidir. Çin'de kullanıcılar İnternete erişim sağladığında, onlara İnternette yapılan her şeyin kaydedildiği ve kuralları ihlal edenlerin ihbar edilmesi gerektiği ikazında bulunan Jingjing ve Chacha isimli iki çizgi polis karakteriyle karşılaşmaktadırlar (ZDNet, 2006). Bunun yanında, Çin sohbet odalarında propaganda yapmak üzere çok miktarda ajan provakatör görevlendirmektedir (Goldsmith ve Wu, 2006: 98).

Ayrıca, devletten faaliyet belgesi almış ve ülke genelinde faaliyet gösteren her biri en az bir yabancı İnternet omurgasına bağlı olan yedi İSS'ya kullanıcılarının İnternet bilgilerini, ziyaret sürelerini ve yaptıkları aktiviteleri en az 60 gün süreyle saklama zorunluluğu getirilmiştir. Aynı şekilde tüm İnternet kafelerin filtreleme programı kullanma ve müşterilerinin İnternete erişim için kimlik bilgilerini sisteme girmelerini sağlama ve bu kayıtları tutma zorunluluğu vardır. Keza, her İnternet bağlantısı üyeliği için polis karakoluna isteklinin kendisini kayıt ettirmesi gerekmektedir (Roberts vd., 2009: 10; Deibert vd., 2008: 265).

Çin, İnternetteki alan adı sahiplerini de kayıt altına almaya çalışmaktadır. Nitekim hükümet Google ve dünyanın en büyük hosting firması olan Go Daddy gibi büyük şirketlerden domain başvurularında imza ve resim talep etmiş ve bu şirketleri ilk defa

web sitesi kayıt ettirenlerden geriye dönük belge istemek zorunda bırakmıştır (Hernandez, 2010).

Bunun yanında Çin kablosuz İnternet bağlantılarını da sıkı denetime almıştır. WIFI olarak adlandırılan ve İnternette anonim gezinmeleri mümkün kılan sistem yerine, Çin 2003’de kendi kablosuz ağ standardını geliştirmiş ve WAPI (Authentication and Privacy Infrastructure) sistemini uygulamaya başlamıştır. Ülke genelinde kullanılması zorunlu kılınan WAPI’nın WIFI’den temel farkı, bağlanmak için onaylı bir kullanıcı adının girilmesinin zorunlu olmasıdır (Goldsmith ve Wu, 2006: 101).

Tüm bu tedbirlerle Çin, İnterneti kontrol ve denetim altında tutarken kullanıcılar, içerik, yer ve İSS’lar üzerinde psikolojik baskı oluşturarak kendiliklerinden sakıncalı veya muhalif içerikten uzak durmalarını ve bir nevi oto sansür uygulamalarını da sağlamaktadır (Fallows, 2008). Çin’de devlet İnternete ilişkin sansür politikalarını, yasalar, idari yönetmelikler ve gayri resmi önlemlerin yanında, Cisco, Yahoo ve Google gibi firmaların da destek sağladığı resmi yasal kısıtlamalar ve sözsüz işbirliği uygulamaları karmaşası içerisinde yürüttüğü için, sansüre nasıl karşı çıkılacağına ve kimin sorumlu tutulacağına belirlenmesi de zorlaşmaktadır (OpenNet, 09.08.2012a; Internet Society of China, 2002).

İnternet içerik düzenlemesi konusunda Çin’de birçok kamu kurumunun görev aldığı karmaşık bir yapı vardır. Bu yapıda Enformasyon Bakanlığı, Kamu Güvenliği Bakanlığı, Sanayi ve Ticaret Bakanlığı, Kültür Bakanlığı, Sivil İşler Bakanlığı yanında İnternet Yasadışı Bilgi Raporlama Merkezi (CIIRC), Devlet Konseyi Bilgilendirme Ofisi, Çin İnternet Ağı Bilgi Merkezi, Çin İnternet Bilgi Merkezi ve koluk güçleri bulunmaktadır. Fakat bu sistemin merkezinde 2004’de kurulan ve Enformasyon Bakanlığı ve Devlet Konseyi Bilgilendirme Ofisi gözetiminde diğer tüm kurumlarla koordineli çalışan CIIRC bulunmaktadır (Chinainternetwatch, 2012).

CIIRC’in görevleri şunlardır: İnternette yer alan yasadışı ve zararlı içeriklere ilişkin ihbar ve şikayetleri almak, bu tür içeriklerle ilgili olarak kolluk ve idari makamlara yardımda bulunmak, İnternet sektöründe öz düzenleme girişimlerini teşvik etmek,

İnternet kullanımı ve etiği konusunda halka yönelik eğitim çalışmaları yapmak, benzer işlevler gören diğer ulusal ve uluslararası kuruluşlar ile işbirliği geliştirmek ve uluslararası arenada İnternet konusunda yaygın olan endişeleri giderme ve sorunları çözme çabalarına katkıda bulunmak (Chinainternetwatch, 2012).

Bu çerçevede CIIRC, Çin sınırları içinde başkalarının haklarını ihlal, etnik nefret, iftira ve hakaret, müstehcenlik ve pornografi, kumar, şiddet, terör ve teröre yataklık, telif haklarını ihlal ve küçüklerin sağlıklı büyümeleri için zararlı içeriklere yönelik olarak “www. net.china.cn” sitesinden ihbarları alarak değerlendirmekte ve diğer ilgili kamu kurumları ile bunları paylaşmaktadır. CIIRC, öz düzenleme çalışmaları ile ilgili olarak ise, sektörün ülke çapındaki öz düzenleme kuruluşu olan Çin İnternet Derneği ile işbirliği içerisinde çalışmalar yapmaktadır. CIIRC ayrıca, ebeveynler, öğretmenler, öğrenciler ve özellikle küçükler için yönelik olarak İnternet güvenliğiyle ilgili çeşitli bilinçlendirme aktiviteleri ve etkinlikler gerçekleştirmektedir (Chinainternetwatch, 2012).

Sonuç olarak, Çin’de İnternetin gelişmesi için yatırım yapıp, kullanıcılar katlanarak artmaya devam ederken, hükümet de vatandaşlarının erişim yeteneğini sınırlamak ve kontrol altına almak için yoğun çaba sarfetmektedir. Bunun için hükümet, İSS’ler ve içerik sağlayıcılar dahil olmak üzere tüm aktörler üzerinden teknik filtrelemeyi geliştirme konusunda azami gayret göstermektedir. Bu nedenle Çin’in İnternete ilişkin bu tutumu, yasakçı ve engelleme yapmaya dayalı İnternet politikası, İnternetin Çin’i nasıl etkileyeceğinden ziyade, Çin’in İnterneti nasıl etkilediği ve şekillendirdiği tartışmalarını beraberinde getirmektedir (Goldsmith ve Wu, 2006: 104).

2.5.2.9 Farklı Ülkelerin Önemli Bazı Uygulamaları

Yasadışı ve zararlı İnternet içerikleri ile mücadele edilmesiyle ilgili olarak bazı ülkelerde dikkat çeken bir takım uygulamalar bulunmaktadır. Özellikle çocuk istismarının engellenmesi ve zararlarının azaltılmasına yönelik sosyal tedbirleri de içeren uygulamalardan bir kaçına değinmek faydalı olacaktır.

İtalya’da çocuk psikiyatristi Prof. Ernesto Caffo tarafından kurulan Telefono Azzurro Derneğinin kurduğu ve işlettiği aynı adlı ihbar ve yardım merkezinin, ihbar ve yardım hattı dışında acil ekibi, araştırma merkezi, eğitim merkezi, uluslararası işbirlikleri ile bir bütün olarak çocuk haklarının korunması ve toplum içinde bir çocuk kültürünün gelişmesi için yürüttüğü faaliyetler dikkat çekicidir (Azzurro, 2013a).

Telefono Azzurro, bu çerçevede kurduğu Ulusal Psikolojik Danışma Merkezi ile çocukların ve gençlerin karşılaştığı kötü muamele, istismar, bağımlılık benzeri her türlü soruna iki telefon hattı ve “www.azzurro.it” web sitesi ile profesyonel danışmanlık hizmeti sunmaktadır (Azzurro, 2013b). Ayrıca, Mavi Çatılar (Tetti Azzurri) adlı çocuk koruma evleri açarak istismar mağdurlarına barınma, tedavi, rehabilitasyon, hukuk danışmanlığı ve eğitim hizmeti vermektedir (Azzurro, 2013c).

Telefono Azzurro, dünyada 160’den fazla ülkede bulunan ve tüm çocuk yardım hattı merkezlerini bir araya getiren kuruluş olan CHI (Child Helpline International- Uluslararası Çocuk Yardım Hattı), çocukların cinsel istismarına ve kayıp çocuklara yönelik küresel mücadele veren ICMEC ve Avrupa’da kayıp ve istismara uğrayan çocuklar için çalışmalar yapan “Missing Children Europe” üyesidir (Azzurro, 2013d).

Diğer bir dikkat çekici uygulama ise, Belçika’da Child Focus adlı kendini kayıp, kaçırılmış ve cinsel istismara uğramış çocuklara adayan STK’nın işlettiği Stopchildporno İhbar Merkezi tarafından gerçekleştirilmektedir. Merkez, İnternet kullanıcılarının çocukların cinsel istismarı içerikleri konusunda bilgilendirilmesi ve bilinçlendirilmesi, ihlallere ilişkin ihbarların teşviki ve bu mücadeleye katılımın sağlanması konularında çalışmalar yapmaktadır. Merkez, genel yaklaşım ve politikaları belirlemek için polis kamu kurumları ve sektör temsilcileri, STK’lar ve akademisyenlerden oluşan bir uzmanlar komitesi kurmuştur. Bu komitede en az yılda 3 kere toplanmakta ve politikaları belirlemektedir (Stopchildporno, 2013a, 2013b).

Benzer şekilde Danimarka’da ise, Cyberhus isminde bir yardım hattı bulunmaktadır. Bu hattın, daha çok öğretmen, pedagog, sosyal çalışmacı ve psikoloji öğrencileri

tarafından gönüllü olarak çocuk istismarına karşı çocuklar ve gençler için online danışmanlık hizmeti sunulmaktadır (Cyberhus, 2013).

%93 İnternet kullanım oranıyla (internetworldstats, 2012e) ve çocuk pornografisinin yaygınlığı ile dikkat çeken bir ülke olan Hollanda'da ise, çocukların cinsel istismarı içeriklerine müptela olmuş olan insanlara yönelik olarak bazı tıbbi yardımlar sunulmaktadır. Aile içi şiddet, saldırganlık ve cinsel davranış bozuklukları ve özellikle çocuklara karşı cinsel yönelimleri olan 12 yaş üzeri kişiler konusunda uzmanlaşmış ve Hollanda genelindeki 9 şubede 300 çalışanı ile hizmet sunan Da Waag adındaki klinikler zinciri bunların en çok bilinenidir. Adli bakım uzmanlarının oluşturduğu Zorg Voor Veilig adlı STK tarafından işletilen ve tüm hizmetlerin ücretsiz verildiği bu kliniklere başvuran kişilere psikolog, psikoterapist veya psikiyatristlerce tedavi uygulanmaktadır. Tedavi seansları gruplar halinde olabildiği gibi, tek kişilik de uygulanabilmektedir. Ayrıca merkeze gelmekten çekinen kişiler için kendi evlerinde tek kişilik tedavi seansları da düzenlenebilmektedir. Polis de bazı kişileri bu merkezlere yönlendirebilmektedir (Dewaagnederland, 2013).

Bunun yanında, çocuk pornografisi sektörünün önemli ülkelerinden olan Hollanda'nın, çocuk pornografisinin önlenmesiyle ilgili gerekli çabayı göstermediği kanısını güçlendiren bazı uygulamaları da bulunmaktadır. Örneğin, ülkenin INHOPE üyesi Meldpunt Kinderporno İnternet İhbar Merkezi, Hollanda Ceza Yasası (Wetboek van Strafrecht) nın 240b maddesi çocukların cinsel istismarı içeriklerinin sadece İnternet ortamında halka yayınlanmasını suç kabul ettiği için ihbarları bu çerçevede kabul etmektedir (Meldpunt-kinderporno, 2013a).

Bunun dışında İnternet ortamında bu nevi içerikleri aramak ve araştırmakla uğraşmadığı gibi kişisel bilgisayarlarda bulunan çocukların cinsel istismarı içerikleri ile ilgili ihbarları da kabul etmemekte, bu şikayetlerin polise yapılması gerektiğini belirtmektedir. Keza, toplu bir şekilde gönderilmeyen, bir kişiden diğer bir kişiye gönderilen ve çocukların cinsel istismarı içerikleri barındıran e-postalar ile ilgili ihbarları da kabul etmemektedir. Ayrıca çocukları içeren erotik hikayelerin, çocuk içermeyen yetişkin pornografisinin, çıplak çocuk resimleri ile ilgili içeriklerin ihbar

edilmemesi gerektiği özellikle vurgulanmaktadır. Çünkü tüm bu sayılanlar Hollanda yasalarına göre yasak kabul edilmemiştir. İhbar Merkezi'nin ücretli bir telefon hattı ile ihbarları kabul etmesi de ilginçtir (Meldpunt-kinderporno, 2013b).

İspanya'da ise, INHOPE üyesi Protegeles İnternet İhbar Merkezi'nin diğer İnternet ihbar merkezlerinden en önemli farkı, çalışanların sadece içerikle ilgili gelen ihbarları değerlendirmekle kalmayıp, aynı zamanda sürekli İnterneti tarayarak yasadışı içerik araştırması yapmasıdır. Merkez, çocuk güvenliği uzmanları, bilgisayar teknisyenleri, çocuk eğitimi uzmanları, haberleşme, ticaret ve finans uzmanları gibi birçok konuda uzmanlaşmış personelden oluşmaktadır. Bu uzmanlardan bir kısmı tam zamanlı çalışırken bir kısmı da ihtiyaç duyulduğunda çalışmalara katılmaktadır. Çalışanlar, sürekli olarak özel eğitimlere tabi tutulmakta ve düzenli psikolojik yardım almaktadır (Protegeles, 2013).

Protegeles'in, özel olarak grooming konusunda “www.quenoteladen.es” adresinden yardım ve destek hizmeti sunan bir web sitesi ve pedofililerin bu hastalıklarından kurtulmaları için faydalı bilimsel bilgiler sunan ve “www.anaymia.com” adresinden İspanyolca dilinde yayın yapan bir web sitesi bulunmaktadır.

Benzer bir çalışmayı da Yunanistan Güvenli İnternet Merkezi Yardım Hattı işleterek yapmaktadır. Bu hat İnternet, cep telefonu ve online oyunların kullanımında karşılaşılan taciz, bağımlılık, zararlı içerik, pedofili, vb. sorunlarla ilgili çocuklara, gençlere, ailelere, eğitimcilere, tüm özel ve kamu kurumlarına destek ve danışmanlık hizmeti sağlamaktadır. Atina Üniversitesi P&A Kyriakou Çocuk Hastanesi Genç Sağlığı Birimi'nin desteklediği ve yönettiği Yardım Hattı'nda çalışan personel hem teknik konularda hem de pedagojik konularda özel eğitim almış kişilerden oluşmaktadır (Saferinternet.gr, 2013).

Güney Kore'de de yasadışı ve zararlı İnternet içerikleriyle mücadele konusunda dikkate değer uygulamalar söz konusudur. Ülkede, tüm elektronik haberleşme ve yayıncılık hizmetleriyle ilgili düzenleyici kurum olan ve İnternetle ilgili temel politikaları ve yayın içeriğini de düzenleyen KCSC (Kore İletişim Standartları

Komisyonu)’nin tepe yönetimi; Başkanı eski bir savcı olan, çoğunluğu akademisyen olan ve sektörden gelenlerinde bulunduğu 9 kişiden oluşmaktadır (ICEC, 2013a).

KCSC alt komisyonları yayın ve telekomünikasyon standartları ile ilgilenmekte ve genel etik ilkeleri veya kodları geliştirmek için çalışmaktadır. Bu kapsamda İnternet içeriğine ilişkin derecelendirme görevini de yerine getirmektedir. Buna göre, web sitelerinin yetişkin olmayan kişilerin erişimine uygunluğu konusunda değerlendirme hizmeti sağlamaktadır (Deibert vd., 2008: 371). Böylece web siteleri, yaygın olarak ebeveynler ve okullar tarafından kullanılan filtreleme programlarına uyumlu hale getirilmekte ve filtrelemelerin etkinliği artırılmaktadır (Kaya, 2010: 68).

KCSC derecelendirme konusunda iki türlü hizmet vermektedir; birincisi, self-rating (öz değerlendirme), diğeri third party rating (üçüncü şahıs derecelendirme)’dir. Öz değerlendirmede yerli içerik sağlayıcılar, KCSC’nin bu konuyla ilgili birimi olan Bilgi İletişim Etiği Komitesi’nin “SafeNet Değerlendirme Standartları” olan “çıplaklık”, “cinsel ilişki”, “şiddet”, “dil” ve “diğerleri”nden oluşan beş kategorinin beş derecesine göre kendilerini değerlendirmekte ve KCSC’nin kendine ait web adresinden sunduğu etiketleme hizmetinden faydalanmaktadır. Bu etiketlemeye ait bilgileri de web sitelerinde yayınlamaktadırlar (Safenet.ne, 2013a).

Bilgi İletişim Etik Komitesi, İnternet kullanıcılarına ve içerik sağlayıcılara sunduğu filtreleme yazılımında bu verileri kullanmaktadır. Yabancı menşeli müstehcen ve şiddet içeriği için ise, üçüncü taraf bir kuruluş olarak KCSC Bilgi İletişim Etik Komitesi, verilen standartlara uygun olarak yabancı içerik derecelendirme veritabanı oluşturmakta ve kullanıcılara sunmaktadır (Safenet.ne, 2013a).

“Bilgi İletişim Etiği Komitesi SafeNet Değerlendirme Standartları”nın neler olduğu Şekil 2.2’de görülmektedir. Bu içerikte bulunabilecek her türlü örnek ise en ince detayına kadar Komisyonun web adresinde yayınlanmaktadır (Safenet.ne, 2013b).

Şekil 0.2. Bilgi İletişim Etiği Komitesi SafeNet Değerlendirme Standartları

	Çıplaklık	Cinsel İlişki	Şiddet	Dil	Diğerleri
4.Seviye	Genital görüntüler	Seks suçları veya açık cinsel eylemler	Zalimce öldürme	Açık cinsellik içeren bir dil	1.
3.Seviye	Çıplak insan figürü	Açık olmayan cinsel eylemler	Öldürme	Şiddetli argo	- Uyuşturucu kullanmanın tanıtımı -Silah kullanmanın tanıtımı -Kumar
2.Seviye	Kısmi çıplaklık	Giyimli cinsel temas	Yaralama	Kaba argo	2.
1.Seviye	Dekolte giyim	Tutkulu öpüşme	Kavga	Yaygın argo	-Alkol kullanmanın tanıtımı -Sigara kullanmanın tanıtımı
0.Seviye	Yukarıdakilerin hiçbiri	Yukarıdakilerin hiçbiri	Yukarıdakilerin hiçbiri	Yukarıdakilerin hiçbiri	

Kaynak: <http://www.safenet.ne.kr/rstan.do> (25.02.2013)

“Bilgi İletişim Etiği Komitesi SafeNet Değerlendirme Standartları”na dayalı olarak Komitenin İnternet içeriklerine ilişkin yaş gruplarına göre tavsiyeleri Şekil 2.3’tedir.

Şekil 0.3. Bilgi İletişim Etiği Komitesi SafeNet Yaş Gruplarına Göre Tavsiyeler

Kategoriler	Çıplaklık	Cinsel İlişki	Şiddet	Dil
İlkokul çağındaki kızlar ve erkekler dahil herkes için	1. Seviye	0 Seviye	1. Seviye	0 Seviye
Ortaöğretim çağındaki kızlar ve erkekler dahil 12 yaş üstü	2. Seviye	2. Seviye	2. Seviye	1. Seviye
Lise çağındaki kızlar ve erkekler dahil 15 yaş üstü	2. Seviye	2. Seviye	3. Seviye	2. Seviye
Yetişkinler için 18 yaş üstü	3. Seviye	3. Seviye	4. Seviye	4. Seviye

Kaynak: <http://www.safenet.ne.kr/drstan.do#part02> (25.02.2013)

Keza, KCSC bünyesinde “Illegal&Harmfull Information Report Center” adındaki INHOPE üyesi İnternet içerik ihbar merkezinden yönetilen, “Cyber-Patrol (Siber Devriye)” adında, gönüllülük esasına göre çalışan, fahri/gönüllü İnternet izleyicileri diyebileceğimiz bir etkinlik grubu faaliyet göstermektedir. Temel görevleri İnterneti sürekli izleyip zararlı içeriğin ihbar vb. yöntemlerle yayılmasını engellemek olan grup’a 20 yaşını dolduran herkes gönüllü olmak için başvurabilmektedir. Üyelik

süresi bir yıldır. Grup üyeleri faydalı olabilecek bilgileri paylaşarak da ortak bir İnternet etiği oluşturmaya çalışmaktadır (Singo, 2013a, 2013b).

Güney Kore’de İnternet içeriğiyle ilgili olarak İnternet etiği önemli bir gündem maddesini oluşturmaktadır. Bu konuda KT Kültür Vakfı, daha güvenli bir İnternet ortamının oluşturulması için “Nethics” kampanyası, reklamlar, eğitim materyalleri, araştırmalar, analizler, ilgili yurtdışı kurumlarla paylaşımlar gibi çeşitli çalışmaları gerçekleştirerek İnternet kullanımının iyileşmesini amaçlamaktadır (KTCF, 2013).

Singapur’da ise, diğer tüm medya sektörünün (dijital medya, film, video oyunları, müzik, radyo, TV benzeri her çeşit yayıncılık) olduğu gibi İnternetin yönetiminden de sorumlu düzenleyici özerk kamu kurumu olan MDA (Medya Geliştirme Kurumu)’nın örnek uygulamaları vardır. Kamu-özel-STK’lardan ve üniversitelerden gelen 15 üyeden oluşan Yönetim Kurulu bulunan MDA (MDA, 2013a), danışma komiteleriyle birlikte çalışmaktadır. MDA bünyesinde yayın içeriklerinin toplum değerleri ile senkronize olmasını sağlamak amacıyla her biri farklı yayıncılık alanında istişari nitelikte kurulan on danışma komitesi ve iki itiraz komitesi bulunmaktadır. Bu komitelerin içerik düzenlemesi için önemli bir mihenk taşı olduğu; çeşitli yaş grupları, ırklar, dinler ve meslekleri temsil eden üyelerin toplumun geri bildirim ve rehberlik talebini karşıladıkları, değişen ihtiyaçlara ve beklentilere göre içerik düzenlemelerini gözden geçirdikleri belirtilmektedir (MDA, 2013b).

İran ise, İnternet ortamında propaganda yapmak, insanları yönlendirmek ve online bilgiyi şekillendirmek için farklı bir strateji uygulamaktadır. Devrim Muhafızlarının kontrolü altındaki gönüllüleri devreye sokarak on binlerce blog oluşturulmakta ve yazılmaktadır. Buna İnternet üzerinde bir tür kelime destekli savaş da denilmektedir (BBC News-Persian, 2008). Öte yandan, İran’ın ulusal bir intranet ya da diğer bir deyim ile “helal İnternet” projesi bulunmaktadır. Buna göre, Gmail, Google, Yahoo ve Hotmail gibi popüler Batılı İnternet araçlarına erişimin ve hizmetlerin olmadığı, tamamen yerli arama motorlarının, hizmet servislerinin ve zararsız içeriklerin bulunduğu "helal internet" in en kısa sürede hayata geçirilmesi planlanmaktadır

(Gayathri, 2012). Nitekim, İran'ın "Yahak" isimli yerli arama motoru çalışmasının bu projenin bir parçası olduğu dile getirilmektedir (SMH, 2012)

Görüldüğü gibi Dünya uygulamaları, tezde yer alan altıncı, yedinci, sekizinci, dokuzuncu ve onuncu alt hipotezlerimizi doğrular mahiyette sonuçlar ortaya koymaktadır. Nitekim, altıncı alt hipotezde savunulduğu gibi, tüm zorluk ve sınırlılıklarına rağmen İnternetin düzenlenmesi, İnternet ortamında yapılan ve suç teşkil eden içeriklerle mücadele edilmesi düşüncesinin ve uygulamasının tüm dünyada giderek daha güçlü bir şekilde hissedildiği görülmektedir. Keza, zamanla İnternet düzenlemelerinin nitelik ve niceliklerinin değiştiği ve devletlerin çeşitli sosyal, kültürel, siyasal, yönetsel veya ekonomik sebeplerle İnternet içeriğine doğrudan ya da dolaylı olarak müdahale etmeye başladıklarına tanık olunmaktadır.

Yine, yedinci alt hipotezde belirtildiği gibi, ülkelerin sosyal, kültürel ve tarihsel özellikleri İnternet olgusuna yaklaşımlarını, yasadışı veya zararlı kabul ettikleri içeriklerin tür ve kapsamalarını belirleme ve bu içerikle mücadele yöntemleri konusunda farklı tavırlar almalarını etkilemektedir. Buna göre de dünyada İnternet içerik düzenlemeleri ve filtreleme konusunda farklı uygulamalar ortaya çıkmaktadır. Bazı ülkeler, çeşitli sebeplerle çok sayıda içerik türüne, geniş kapsamlı katı filtreleme ve erişim engelleme uygulamaları yapmaktayken, bazı ülkelerde sınırlı müdahaleyi ve daha yumuşak tedbirler uygulamayı tercih edebilmektedir.

Keza, dokuzuncu alt hipotezde belirtildiği gibi, dünya incelemeleri, demokratik ülkelerin genelinde İnternet içerik düzenlemesine ilişkin yönetsel yaklaşımın “birlikte düzenleme” yöntemini tercih etme şeklinde tezahür ettiğini ortaya koymaktadır. Keza, temel yaklaşımı ne olursa olsun hemen her ülkenin öz düzenleme yaklaşımlarını teşvik ettikleri görülmektedir.

Son olarak, sekizinci ve onuncu alt hipotezlerde belirtilen hususların, demokratik değerlere önem veren ülkelerde İnternet içerik düzenlemelerine ve uygulamalarına esas yapıldığını söyleyebiliriz. Yani, demokratik ülkelerin sakıncalarından dolayı erişim engelleme yöntemini çok fazla tercih etmedikleri, son çare olarak gördükleri

ve müdahaleyi mümkün olduğunca sınırlı tutmaya çalıştıkları gözlemlenmektedir. Bunun yerine, uyar-kaldır mekanizmalarını işletmeye çalıştıkları, küresel şirketlerle özel anlaşmalar yapma, öz düzenleme uygulamalarını geliştirme, bilinçlendirme ve İnternet çalışmalarını artırma, sivil toplumun gücünü kullanma, pozitif içeriğin çoğalmasını sağlama gibi yöntemleri kullandıkları görülmektedir. Bu arada, demokratik ülkelerde erişim engellemelerine karşı gösterilen tepkilerin de bu sonucun ortaya çıkmasında etken olduğunu belirtmek gerekmektedir.

Buraya kadar çalışma kapsamında Birinci ve İkinci bölümünde ele alınan konular ve bu konular etrafında tartışılan ve değerlendirilen ilk on alt hipotez, tezimizin temelini oluşturan “İnternet içerik düzenlemesi sorunu”nun bilgi toplumu ve İnternet arka planını, aktörlerini, etkileyen değişkenleri, boyutlarını, sınırlayan unsurları, ilgili konu ve alanları ortaya çıkartmıştır. Böylece, sorunun büyük fotoğrafı yakalanmaya çalışılmıştır. Sorunun giriftliği, karmaşıklığı ve dinamikliği, dolayısıyla çözümünün birçok değişkene ve aktöre bağlı olduğu ve zor olduğu görülmektedir.

Çözüm için önce, çok aktörlü/boyutlu, dinamik ve sınır tanımaz kendine özgü yapısı ile İnternet gerçeğini anlamak ve kavramak için, İnternet olgusunu bütün bu özellikleri ile ve bütüncüllüğü içerisinde ele almak gerekmektedir. Parçalara ayırarak teknik, ekonomik, sosyal, siyasal, yönetim vs. tek bir yönü veya tek bir aktörü üzerinden İnternet gerçekliğini anlamak ve bulmak mümkün değildir. Çünkü, İnternet tüm bu yönleri ve aktörleri ile ve bunların girift bir şekilde birbiri içine geçmesi ve zincirleme olarak birbirini etkilemesiyle bir bütün olarak dinamik bir yapıdır. Bu nedenle, İnternetle ilgili herhangi bir olay, durum veya sorunu İnternetin bu bütünlüğü içinden yalıtarak incelemek, analiz etmek, tespit, sonuç ve çözüm üretmek yanıltıcı olacaktır.

Dolayısıyla, İnternet olgusunun bir alt başlığı ve parçası olan İnternet içerik düzenlemesi konusunu İnternetin bu çok yönlü ve aktörlü bütünlüğünden ayırıştırarak ele almak, steril ortam oluşturarak analizlere konu edinmek, buna göre sonuçlar çıkarmak ve çözümler üretmek doğru olmayacaktır. Bunun yerine, konunun bizzat

doğasının ortaya koyduğu özelliklerle birlikte, bütünlüğün içerisindeki yeri ve diğer yön ve aktörlerle etkileşimlerini de kapsayacak bir şekilde incelemek gerekmektedir.

Bu yüzden, İnternet içerik düzenlemesine ilişkin strateji ve politikalar genel bilgi toplumu ve İnternet strateji ve politikalarından bağımsız olarak düşünülmemelidir. Bilakis, tüm alt konulara ait strateji ve politikaları belirleyen, belirli bir sistematik içinde eldeki verilere göre oluşturulmuş bütüncül bilgi toplumu ve İnternet strateji ve politikaları olmalıdır. Dolayısıyla, ülkelerin İnternet içerik düzenlemelerine ilişkin sorunlarına çözüm bulabilmeleri için önce İnternetin çok yönlü, çok aktörlü ve dinamik yapısıyla uyumlu, aynı türden özelliklere sahip çok yönlü, çok aktörlü ve dinamik bütüncül İnternet stratejileri ve politikaları oluşturmaları gerekmektedir. Daha sonra, İnternetin beraberinde getirdiği risk ve tehditlerin bertaraf edilmesi ve güvenli İnternet kullanımı bağlamında yasadışı ve zararlı içeriklerle mücadeleyi öngören İnternet içerik düzenlemesine ilişkin strateji ve politikalar, bu bütüncül strateji ve politikaların omurgası üzerine oturtulmalıdır.

Nitekim, tezin onbirinci alt hipotezinde, daha önce ilk on hipotez kapsamında tanımlanan ve dinamikleri ortaya konulan sorunun çözümünün temel şartı olarak, bahsi geçen bütüncül bilgi toplumu ve İnternet stratejisi ve politikalarının oluşturması ve uygulanması gereği savunulmuştur. Keza, İnternet içerik düzenlemesi sorununun, bu bütüncül bilgi toplumu ve İnternet politikalarının bir parçası olarak ele alınarak belirlenmiş ve sorunun teknik, ekonomik, sosyal, siyasal, yönetsel tüm boyutlarını içine alan uygun kamu politikaları, karar ve uygulamalarıyla çözüme kavuşturulabileceği öngörülmüştür. Ayrıca, hipotezde, tüm bu süreçlerin kamu kurumlarının gözetim ve denetiminde, ilgili tüm tarafların katılımıyla birlikte düzenleme yaklaşımı ile gerçekleştirilmesinin gereği tekrar vurgulanmaktadır.

Onikinci alt hipotezde ise, bu gereklilik ve önceki hipotezlerde sayılan gereklilikler yerine getirilmiş olsa dahi, sorunun son bulmayacağı; yasadışı ve zararlı İnternet içeriklerinin tamamen önlenmesinin mümkün olmayacağı kabul edilmektedir. Söz konusu gerekliliklerin yerine getirilmesi ile birlikte, uygun yöntem ve yaklaşımlar içeren strateji ve politikalar geliştirilmesi ve uygulanması ile sorunun minimize

edilebileceđi öngörölmektedir. Onbirinci ve onikinci alt hipotezlerde dile getirilen bu görüşlerin gerekçelerinin ise, çalışmanın ilk iki bölümünde ele alınan konularda ve ilk on hipotezde ve bu hipotezler etrafında yapılan tartışma ve değerlendirmelerde mevcut olduđu görölmektedir.

Üçüncü bölümde ise, İnternet içerik düzenleme sorunun Türkiye tarafı ele alınacak ve yeni hipotezler bağlamında tartışılarak değerlendirilecektir.

ÜÇÜNCÜ BÖLÜM

TÜRKİYE’DE İNTERNET İÇERİĞİNİN DÜZENLENMESİ VE TİB ÖRNEĞİ

Bu bölümde, önceki bölümlerde alt hipotezler ile çerçevesi çizilen içerik düzenlemesi sorununun Türkiye boyutu yeni hipotezler ile mercek altına alınacaktır. Önce, Türkiye’de İnternet içeriğinden kaynaklanan ele alınacaktır. Daha sonra İnternetin ve İnternet içerik düzenlemelerinin tarihçesine, 5651 sayılı İnternet içeriğinin düzenlenmesine ilişkin yasanın çıkmasına kadar yaşanan gelişmelere ve yapılan tartışmalara değinilecektir. Akabinde 5651 sayılı Yasa’nın çıkarılması ve sonrasında yaşananlar, yeni Yasa’nın konuyu ele alış biçimi, öngördüğü hukuksal ve örgütsel yapı ve TİB’in durumu, yasanın bugüne kadar yaşanan süreçteki uygulamaları ve ortaya çıkardığı sonuçlar ve tüm bunlarla ilgili yürütülen tartışmalar ortaya konulmaya çalışılacaktır.

3.1 TÜRKİYE’DE İNTERNETTEN KAYNAKLANAN SORUNLAR

Bu başlık altında önce İnternetin Türkiye’deki gelişimi ve kullanım özelliklerine, daha sonra, ağırlıklı olarak İnternet içeriğinin ülkemizde meydana getirdiği toplumsal sorunlara, güvenlik ve mahremiyet problemlerine değinilecektir. Son olarak da İnternet kafeler ele alınacaktır.

3.1.1 Türkiye’de İnternetin Gelişimi ve Kullanımı

Bu kısımda kısaca Türkiye’de İnternetin tarihsel gelişimine değindikten sonra Türkiye’deki İnternet kullanımının temel özellikleri incelenecektir.

3.1.1.1 Türkiye’de İnternetin Gelişimi

Türkiye’de genel amaçlı kullanım sağlayan geniş alan bilgisayar ağı, 1986 yılında tesis edilen EARN (European Academic and Research Network) bağlantılı TÜVEKA (Türkiye Üniversiteler ve Araştırma Kurumları Ağı)’dır. İlerleyen yıllarda bu ağın ihtiyaçlara cevap vermemesi üzerine, 1991 yılı sonlarına doğru ODTÜ ve TUBİTAK

işbirliği ile İnternet teknolojilerini kullanan yeni bir ağın tesis edilmesi yönünde çalışmalar yapmak üzere DPT'nin bit projesi olarak TR-NET (Türkiye İnternet Çalışma Grubu) kurulmuştur (ODTÜ, 2013).

Bu Proje Grubu'nun çalışmaları sonucunda ilk yurtdışı İnternet bağlantısı 12 Nisan 1993 tarihinde ODTÜ'de gerçekleştirilmiştir. PTT'ye 1992 yılında yapılan başvurunun sonuçlanmasını takiben, ODTÜ Bilgi İşlem Daire Başkanlığı sistem salonundaki yönlendiriciler kullanılarak, 64 Kbps kapasiteli kiralık hat ile, Washington'da bulunan NSFNet (National Science Foundation Network)'e İnternet bağlantısı kurulmuştur (ODTÜ, 2013). Bu hat uzun süre ülkenin tek çıkışı olmuştur. Daha sonra 1994'te Ege Üniversitesi, 1995'te de Bilkent, Boğaziçi ve İstanbul Teknik Üniversiteleri tarafından İnternet bağlantısı sağlanmıştır (Sınar, 2001: 111).

1996 yılında, TÜBİTAK bünyesinde kurulan ULAKBİM (Ulusal Akademik Bilgi Merkezi)'nin, Ulusal Akademik Araştırma Ağı (ULAKNET)'ni kurmasından sonra, ODTÜ üzerinden çıkış yapan üniversite ve araştırma kurumlarının bağlantıları kademeli olarak ULAKNET'e aktarılmıştır (ODTÜ, 2013).

Başlangıçta akademik çevrelerde bilimsel veri iletimi ve iletişim için kullanılan İnternet, daha sonra ticari ağ altyapısına ve bireysel kullanıma geçmiştir. 1995 yılında Türk Telekom tarafından açılan ihaleyi kazanan konsorsiyum tarafından TURNET, ticari kullanıcılara yönelik ilk kurulan omurga olarak 1996 yılında hizmet vermeye başlamıştır. Ancak zaman içinde kişisel bağlantı isteklerinin artması ve TURNET çıkışlarının bu talepler karşısında yetersiz kalması üzerine 1999 yılı içerisinde, ticari ağ altyapısını sağlamak için TTNNet isimli yeni bir oluşum faaliyete geçirilmiş ve 2000 yılından itibaren ticari kullanıcılar TTNNet omurgası üzerinden İnternet erişimine sahip olmaya başlamışlardır (Sınar, 2001: 113). TTNNet'in kurulmasıyla İnternet hızla yaygınlaşmış ve kullanıcı sayısı ve kullanımı artmıştır. Günümüzde birçok özel servis sağlayıcı (Superonline vb) ile birlikte kablo net, General Packet Radio Service (GPRS) ve Asymmetric Digital Subscriber Line (ADSL) altyapısını kullanarak İnternet'e bağlanılabilmektedir.

3.1.1.2 Türkiye’de İnternet Kullanımı

BTK verilerine göre, Türkiye’de 2012 yılı İnternet kullanım oranı, %42,5 sabit, %12,5 mobil olmak üzere toplamda %55’tir. 1998-2011 yılları arası İnternet kullanımındaki artış oranı %14.6’dur. Aynı dönemde AB’ndeki artış %245’tir. Genişband İnternet kullanımında bir önceki yıla göre artış %82’dir (BTK, 2012).

Dünyaca ünlü “internetworldstats.com” web sitesinin verilerine göre Türkiye’de 2000 yılında yaklaşık 2 milyon İnternet kullanıcısı varken, bu sayı 2012 Haziran’ı itibariyle 36 milyonu geçmiştir. Türkiye’nin İnternet kullanım oranı ise %45,7’yi bulmuştur. Ulaştığı bu rakam ile Türkiye, İnternet kullanıcı sayısını esas alan “Top 20 Ülkeler” sıralamasında onbeşinci sıraya yükselmiştir. Türkiye’nin tüm dünyadaki toplam İnternet kullanıcıları arasındaki oransal payı ise %1,5 dur.⁶¹

Avrupa ülkeleri arasında Türkiye İnternet kullanıcı sayısı bakımından Rusya (68 milyon), Almanya (67.5 milyon), İngiltere (52,7 milyon) ve Fransa (52,2 milyon)’nın ardından beşinci sırada yer almaktadır. Türkiye’nin kullanıcı sayısı Avrupa’daki toplam İnternet kullanıcılarının %7,3’ünü oluşturmaktadır. Fakat, İnternet kullanım oranı baz alındığında Avrupa ülkelerinin ortalaması olan %63,2’nin oldukça altında kalmaktadır (internetworldstats, 2012e). Benzer şekilde, Türkiye %45,7’lik İnternet kullanım oranı ile dünya ortaması olan %34.3’ün üzerinde bir orana sahip olsa da, en yüksek kullanım oranına sahip elli ülke arasına girememektedir.⁶²

TÜİK’in verilerine göre ise, 2005 yılında ülke genelinde İnternet kullanım oranı %17,6 iken 2012 sonu itibariyle oran %47,4’e ulaşmıştır. Tablo 3.1’de 2005-2012 yılları arasında İnternet kullanımının artış ivmesi görülmektedir. Her geçen yıl artış gösteren kullanıcı sayısı yedi yıl içinde neredeyse üç katına çıkmıştır.

⁶¹ Bu listedeki ilk 5 ülkenin sırasıyla “Dünyadaki toplam kullanıcılar arasındaki oransal payları”, “kullanıcı sayısı” ve “kullanım oranı”na ait rakamlar şöyledir; 1. Çin: %22,4, 538 milyon, %40,1, 2. ABD: %10,2, 245 milyon, %78,1, 3. Hindistan: %5,7, 137 milyon, %11,4, 4. Japonya: %4,2, 101 milyon, %79,5, 5. Brezilya: %3,7, 88,5 milyon, %45,6 (internetworldstats, 2012h).

⁶² Bu listedeki ilk 10 ülke ve kullanıcı oranları şöyledir; 1. İzlanda: %97,8, 2. Norveç: %97,2, 3. İsveç: %92,9, 4. Falkland Adası: %92,4, 5. Lüksemburg: %91,4, 6. Grönland: %90,2, 7. Avustralya: %89,8, 8. Hollanda: %89,5, 9. Danimarka: %89, 10. Finlandiya: %88,6 (internetworldstats, 2012i).

Tablo 0.1. Türkiye’de Cinsiyete Göre İnternet Kullanıcı Oranları

Yıl	Toplam (%)	Erkek(%)	Kadın(%)
2005	17,6	24,0	11,1
2007	30,1	39,2	20,7
2008	35,9	45,4	26,6
2009	38,1	48,6	28,0
2010	41,6	51,8	31,7
2011	45,0	54,9	35,3
2012	47,4	58,1	37,0

Kaynak: TÜİK, 2012, http://www.tuik.gov.tr/VeriBilgi.do?alt_id=60 (04.03.2013)

Tablo 3.1’de 2005-2012 yılları arasında İnternet kullanımının kadın ve erkekler açısından gelişim trendi de ortaya çıkmaktadır. Rakamların incelenmesinden, zaman içerisinde her ne kadar erkek ve kadın kullanımı arasındaki oransal makasın giderek azalma eğiliminde olduğu görülse de, halen toplam kullanımın yaklaşık %60’ını erkekler, %40’ı kadınlar oluşturmaktadır.

Tablo 3.2. Türkiye’de yaş gruplarına göre İnternet kullanım oranlarının gelişimini göstermektedir. Verilerden açık bir şekilde Türkiye’deki İnternet kullanıcılarının daha çok gençlerden oluştuğu anlaşılmaktadır.

Tablo 0.2. Türkiye’de Yaş Gruplarına Göre İnternet Kullanıcı Oranları (%)

Yaş	2005	2007	2008	2009	2010	2011	2012
16-24	27,2	50,4	54,8	59,4	62,9	65,8	67,7
25-34	16,7	32,3	41,4	45,1	50,6	55,1	58,5
35-44	9,7	23,8	29,3	30,2	34,7	39,7	42,6
45-54	6,3	14,8	19,4	18,6	22,4	22,7	25,5
55-64	2,3	4,8	6,9	6,2	7,8	10,4	11,9
65-74	0,9	1,4	1,6	2,0	2,7	2,7	3,6
TOPLAM	17,6	30,1	35,9	38,1	41,6	45,0	47,4

Kaynak: TÜİK, 2012, http://www.tuik.gov.tr/VeriBilgi.do?alt_id=60 (04.03.2013)

TÜİK'in 2012 yılı Nisan ayı verilerine göre Türkiye genelinde hanelerin %47,2'si evden İnternete erişim imkanına sahiptir. Bu oran 2011 yılının aynı ayında %42,9 olarak bulunmuştur. İnternet erişim imkanı olan hane oranı kentsel yerlerde % 55,5 iken, kırsal yerlerde % 27,3'tür (TÜİK, 2012).

Aynı araştırmada, 16-74 yaş grubundaki tüm bireylerin %37,8'inin İnterneti düzenli olarak, hemen hemen her gün veya haftada en az bir defa kullandığı tespit edilmiştir. Aynı dönem ve yaş grubunda İnternet kullanan bireylerin arasında düzenli İnternet kullanım oranı ise %88,5 olup, bu oran kentsel yerlerde %89,7, kırsal yerlerde %82,5 ve İstanbul bölgesinde %90,7 olarak gerçekleşmiştir (TÜİK, 2012).

Araştırmaya göre, bireylerin İnternet kullanımı eğitim seviyesine paralel olarak artmaktadır. Yüksekokul, fakülte ve daha üstü eğitime sahip olanlar %93, lise ve dengi %76,4, ilköğretim/ortaokul ve dengi %57,6, ilkokul %17,7 ve bir okul bitirmemiş olanlar %3,5 oranında İnternet kullanmaktadır. Yüksekokul, fakülte ve daha üstü eğitime sahip kadınların İnternet kullanımı (%92,8) erkeklere (%93,1) oldukça yakın düzeyde olup eğitim seviyesi düştükçe kadın ve erkek arasındaki fark artmaktadır. İşgücü durumuna göre en çok İnternet kullananlar ise öğrenciler %89,9, işverenler %76,6, ücretli/maaşlılar %66 ve işsizler %54,4'tür (TÜİK, 2012).

Aynı araştırmada, kullanıcıların İnterneti en çok %72,5 ile çevrimiçi haber, gazete ya da dergi okuma, haber indirme için kullandığı görülmüştür. Bunu %66,8 ile e-posta gönderme/alma, %61,3 ile mal ve hizmetler hakkında bilgi arama, %49,1 ile oyun, müzik, film, görüntü indirme ve oynama takip etmiştir (TÜİK, 2012).

Araştırmada, kullanıcıların %70'inin İnterneti evde, %33,8'nin işyerinde, %17,8'nin arkadaş, akraba vb.nin evinde, %16'sının İnternet kafelerde, %7,2'nin eğitim alınan yerde, %5,9'nun ise kablosuz bağlantı yapılabilen yerlerde takip etmektedir. İnternet kafelerde İnternet kullanımı bir önceki yılın aynı döneminde %18,7 idi. Araştırmaya göre, İnternete kablosuz olarak bağlanmak için kullanıcıların %23,7'si cep telefonu veya akıllı telefon, %15,6'sı dizüstü bilgisayar (laptop, notebook veya netbook), %1,3'ü ise dokunmatik ekranlı tablet bilgisayar kullanmaktadır (TÜİK, 2012).

Araştırma, kullanıcıların İnternet üzerinden mal veya hizmet satın alma oranını %21,8 olarak tespit etmiştir. Önceki yıl bu oran %18,6 olarak bulunmuştu. Ayrıca, araştırmada, kullanıcıların kamu kurum/kuruluşları ile iletişimde İnternet kullanma oranının %45,1 olduğu bulunmuştur. Bu oran önceki yılın aynı döneminde %38,9 olarak gerçekleştirilmişti. Kullanım amaçları arasında kamu kuruluşlarına ait web sitelerinden bilgi edinme %42,9 ile ilk sırayı almıştır (TÜİK, 2012).

TTNET'in 2012 yılı ilk çeyreğine ilişkin araştırmasına göre, Türkiye'de İnternet kullanım oranı %45; bunların %60,9'unun erkek, %39,1'inin kadın, %50,9'nun ise 18-34 yaş aralığında yer aldığı tespit edilmiştir. Kullanıcıların İnterneti kullanım amaçları ise şu şekilde belirlenmiştir; %87 İnternette sörf yapmak (gezme/inceleme), %82 Facebook'a girmek, %76 e-posta kontrolü, %71 yazılı mesajlaşma/chat yapma, %67 müzik/radyo dinleme, %66 film/video izleme, %61 haber/gazete okuma, %59 görüntülü-sesli görüşme, %56 sesli görüşme, %55 oyun oynama, %54 müzik indirme, %45 CD-DVD oyunları, %44 film/video indirme, %41 TV izleme, %37 diğer sosyal medya, %32 e-devlet işlemleri, %31 Twitter, %29 yazılım indirme, %24 İnternette alışveriş ve %23 İnternet bankacılığı (Zaman, 06.11.2012).

Bu Araştırmanın ortaya koyduğu diğer bir bulgu ise evde İnternet kullanımının artışı göstermesi olmuştur. İnternet kullanımında evden bağlanma oranı 2010 yılında %58 iken, 2012 yılında bu rakam %66'ya ulaşmıştır. Geçmiş yıllarda Türkiye'deki İnternet kullanım alışkanlıklarında önemli bir yer tutan İnternet kafelerden İnternete bağlanma oranı ise düşüş göstermektedir (Zaman, 06.11.2012).

TTNET'in 2011'deki diğer bir araştırmasında, tüm İnternet trafiğinde bandı en çok meşgul eden aktiviteler şöyle sıralanmaktadır: %40 video izlemek, %28 İnternette gezinmek, %11 dosya indirmek, %3,7 Tivibu servisi, %0,8 anlık mesajlaşma, %0,2 oyun ve %9,4 diğer faaliyetler (TTNET blog, 2011).

2007 yılında yaptırılan bir araştırmaya göre, Türkiye nüfusunun %77'si İnternet kullanmaktadır. İnternetin kullanım amaçları ise sırasıyla şöyledir: %67,71 bilgi edinme, %42,12 haber okuma, %40,42 eğitim, ders, araştırma, %38,18 haberleşme,

%2,12 bahis oynama ve %2,39 iş amaçlı. Bireylerin bir seferlik İnternet kullanım süreleri ise şu şekilde belirmiştir: %12 30 dk. altı, %28,36 30 dk.-1 saat, %53 30 dk.-3 saat, %11 3 saatten fazla. Ailede İnternet kullanmayanların oranı ise, anneler %76.7, babalar %22.8 ve çocuklar %0.6 olarak bulunmuştur (ATHGM. 2012).

2012 tarihli bir TÜBİTAK projesinde ise, Türkiye’de İnternet kullanım tarzları incelenmiş ve tipolojileri tespit edilerek kategorize edilmiştir. Belirlenen bazı kategoriler ve kullanıcı özellikleri şöyledir: “Seyirciler”; genelde İnternet’te sörf yapan, e-posta alıp gönderen, arama motorlarını kullanan, haber okuyan ve blogları takip edenler, “sosyallesiciler”; İnternet’i sosyal ağlar ve iletişim için kullananlar, “üreticiler”; aktif olarak yeni içerikler üretenler, “eleştiriciler”; içeriği izlemekle kalmayıp yorumlar yapan ve tartışmalara katılan, haber alma yanında haber de ekleyen, içerikleri puanlayan ve yorumlayanlardır (Alternatif Bilişim, 2012a).

Söz konusu araştırmaya göre, ülkemizde kullanıcıların %83,1’i “seyirciler”, %58,4’ü “sosyallesiciler”, %33,6’sı “üreticiler” ve %16,4’ “eleştiriciler” kategorisinde yer almaktadır. Bu sonuçlardan Türkiyeli kullanıcıların ‘seyirci’ niteliğinin daha ağır bastığı görülmektedir. İnternet kullanıcısı İnternet’i yoğun bir şekilde izlemekte fakat içerik üretmekten kaçınmaktadır. “Eleştiriciler” ise İnternet kullanıcıları arasında küçük bir azınlığı teşkil etmektedir (Alternatif Bilişim Derneği, 2012a).

İlginç olan, İnternet kullanım sıklığına bakıldığında skalanın “ya hep ya hiç” arasında gidip gelmekte olmasıdır. Yani, İnternet kullanmaya başlayan kişi her gün İnternet’e giren kişiye dönüşmektedir. İnternet’i “nadiren” kullananlar hiçe yakındır. Bununla birlikte kullanım sıklığına eşlik eden bir derinlikten bahsetmek mümkün gözükmemektedir. Düzenli İnternet kullanıcısı, İnterneti üretici amaçla kullanmamakta, genellikle izlemekte ve sosyal ağlara takılmaktadır. İçerik üretmekten ve demokratik kamusalılığın belkemiğini oluşturan İnternet’i tartışma için kullanma alışkanlığından yoksundur (Alternatif Bilişim Derneği, 2012a).

Türkiye’de İnternetin hızla yaygınlaştığının ve kullanımının arttığının diğer bir göstergesi de İnternet aboneliği sayısındaki artıştır. BTK verilerine göre, 2008

yılında 6 milyon civarında olan İnternet abone sayısı (sabit, mobil, kablo, fiber vb.) üç katından daha fazla artarak, 2012 yılı son çeyreğinde 20 milyonu geçmiş bulunmaktadır. 2011 yılı rakamları ise 14 milyon civarında gözükmemektedir. Buna göre, son bir yıllık artış %42,3 olmuştur (BTK, 2013a: 26).

BTK verilerinin gösterdiği diğer bir önemli sonuç ise, mobil (cep telefonundan) İnternet aboneliğinin genel abonelik artışının çok daha üzerinde olduğudur. 2011 yılında 4.9 milyon olan mobil İnternet aboneliği %108,9'luk artış ile 2012 yılında 10,2 milyona ulaşmıştır (BTK, 2013a: 27). Bu durum Türkiye’de İnternet bağlantısının ve kullanımının giderek daha fazla cep telefonları üzerinden gerçekleştirilmeye başlandığının bir göstergesi olarak değerlendirilebilir.

Dijital dünyayla ilgili ölçümler yapan ve bunları yayınlayan “comScore”un bir raporuna göre, online video yaygınlığı bakımından Türkiye’deki İnternet kullanıcıları Dünyada ilk sırada yer almaktadır. Türkiyeli kullanıcıların %93,6’sı İnternette video izlemektedir.⁶³ Aynı şirketin bir başka raporuna göre, Türkiyeli kullanıcılar spor sitelerini ziyarette Avrupa birincisidir. Türkiye’deki spor siteleri bir aylık süre zarfında toplamda 16,4 milyon defa tekil ziyaretçi tarafından görüntülenmiştir. Bu rakamın toplam İnternet kullanıcılarına oranına bakıldığında Türkiye’nin %70 ile Avrupa ortalamasının çok üstünde, tüm ülkeler içinde birinci sırada olduğu görülmektedir. Bu oran Avrupa ortalamasında %45.8 olarak tespit edilmiştir.⁶⁴

Dünyadaki İnternet kullanıcılarının blogları ziyaret etme durumlarını ölçümleyen “comScore”un başka bir raporunda, Türkiye Dünya dördüncüsü olmuştur. Rapora göre, Türkiye’deki toplam kullanıcıların %81,9’u blog ziyareti yapmaktadır.⁶⁵ Ayrıca, “2013 Europe Digital Future in Focus” adlı “comScore”un hazırladığı

⁶³ 2011 yılı Ekim ayını esas alan bu rapora göre, ikinci Kanada %90,9, üçüncü Şili %90,2 ile Türkiye’yi takip etmektedir. Kullanıcı başına aylık en çok online video izleme bakımından ise Kanada 303’le birinci, ABD 286 ile ikinci, İngiltere 268 ile üçüncü sırada yer alırken Türkiye 250 video ile 4. sırayı işgal etmektedir. Bu Türkiye’de her bir kullanıcının her gün yaklaşık 10 video izlediği anlamına gelmektedir (Comscore, 14.10.2011).

⁶⁴ 2011 yılı Şubat ayını esas alan bu rapora göre, %69,8 ile İrlanda ikinci, %65,9 ile İspanya üçüncü sırada yer almaktadır (Webrazzi, 12.12.2012).

⁶⁵ 2011 yılı Haziran ayını esas alan bu rapora göre, Tayvan %85,5 ile birinci, Brezilya %85,2 ile ikinci ve Güney Kore ise %84,9 ile üçüncü sırada yer almaktadır (Webrazzi, 26.08.2011).

Rapor'da Türkiye'nin, 15-24 yaş arası genç İnternet kullanıcıları bakımından Avrupa'da en büyük paya sahip ülke olduğu belirtmektedir (Comscore, 21.03.2013).

Google'nin yayınladığı arama trendlerine göre ise, Türkiye'den 2004 yılından 16.04.2013 tarihine kadar en çok aranan terimler ve arama hacmi endeksleri şu şekildedir: 1. Facebook 100, 2. Youtube 20, 3. Mynet 15, 4. Face 15, 5. Oyun 15, 6. İndir 10, 7. Sahibinden 10, 8. Milliyet 10, 9. Oyunlar 10, 10. E-okul 10. Dünyada sıralama ise şöyledir: 1. Facebook 100, 2. Youtube 45, 3. Google 30, 4. İndir 25, 5. You 25, 6. Yahoo 20, 7. Hotmail 20, 8. Oyun 15, 9. E-mail 10, 10. Ebay 10 (Google, 22.08.2013). Müstehcen olabilecek arama terimlerine filtre uygulandığı için bu tür terimler bu listede yer almamaktadır.

İnternet trafiği hakkında yayınladığı istatistiklerle dünyada meşhur olan Alexa verilerine göre, 22.08.2013 tarihi itibarıyla, son bir ay içerisinde Türkiye'den en çok ziyaret edilen ilk on web sitesinin sıralaması şöyledir: 1. Google Türkiye, 2. Facebook, 3. YouTube, 4. Google, 5. Milliyet Gazetesi, 6. Hürriyet Gazetesi, 7. Sahibinden.com, 8. Windows Live, 9. Twitter, 10. Blogstop.com (Alexa, 2013b).

BTK'nın 2012 verilerine göre Türkiye'deki İnternet kullanıcılarının 60 saniyelik zaman kesiti içerisinde yaptıkları aktiviteler şu şekildedir: 168.000.000 e-posta gönderimi, Facebook'da 695.000 durum güncellemesi, 416 İnternet sitesini hackleme girişimi, Flickr'a 6.600 fotoğraf yüklemesi, Twitter'da 320'den fazla yeni hesap açılıyor, Skype'da 6.150 saat konuşma yapılıyor, 694.445 kez arama yapılıyor, Youtube'da toplamda 25 saati bulan 600'den fazla video paylaşıyor, Pandora'da 23.000 saatlik müzik akışı oluyor, 70'den fazla alan adı alınıyor (BTK, 2012).

TİB'nin yaptığı teknik değerlendirmeler neticesinde Türk İnternet kullanıcılarının içerik bakımından %73 oranında müstehcen siteleri, %13 oranında haber sitelerini, %4 oranında sohbet ve arkadaşlık sitelerini, %4 oranında oyun sitelerini ve %3 oranında iş ve alışveriş sitelerini ziyaret ettikleri tespit edilmiştir. Bu çalışmada, web sitelerine erişim sıklığı, toplam bant genişliği kullanımı, kullanıcının bu web

sitelerinde geçirdiği süreler değerlendirilmemiştir, sadece en fazla erişilen web siteleri içeriklerine göre kategorize edilmiştir (TİB, 2010).

Tüm bu araştırma ve raporlarda yer alan verilerden yola çıkarak, Türkiye’deki İnternet kullanımının sayısal, oransal ve kullanım miktarı ve süresi bakımından hızla arttığı söylenilebilir. Ülke nüfusunun genç olması ve gençlerin de teknolojiye daha yatkın olmalarının da etkisiyle İnternet kullanıcılarının çoğunun genç olduğu ve trendin bu yönde devam edeceği görülmektedir. İnternet kullanımının yüksekliğinde erkek ve eğitilmiş olma karakteri ön plana çıkmaktadır. Ülkemizde kullanıcılar daha çok evlerinden veya cep telefonları ile İnternete bağlanmayı tercih etmektedirler.

Diğer yandan Türkiye’de İnternetin Facebook, Google ve Hotmail gibi batılı platformların egemenliği altında olduğu görülmektedir (Beger vd., 2011). Türkiye’deki İnternet kullanıcıları İnterneti bu platformların sundukları imkanlardan yararlanarak daha çok eğlenme, vakit geçirme, haber okuma ve iletişim kurma amacıyla kullanmaktadır. Bu nedenle, İnternette en çok yapılan aktiviteler sörf yapma, sanal sohbetler, sosyal ağ faaliyetleri, video seyretme, oyun, müzik, film, görüntü, yazılım indirme, oyun oynama, çevrimiçi haber, gazete veya dergi okuma, spor ve sağlık sitelerini gezme, blogları ziyaret, e-posta gönderme/alma ve görüntülü/sesli görüşme yapmak olarak belirmektedir. Ayrıca, çok olmamakla birlikte, eğitim amaçlı olarak, araştırma ve inceleme yapmak için, e-ticaret, sanal alışveriş, İnternet bankacılığı, e-devlet hizmetlerinden yararlanma, mal ve hizmetler hakkında bilgi alma gibi maksatlarla İnternetin kullanıldığı görülmektedir.

3.1.2 Türkiye’de İnternetin Getirdiği Sorunlar

İnternet kullanımının hızla arttığı ve yaygınlaştığı ülkemizde, yasadışı ve zararlı İnternet içeriğinin oluşturduğu risk ve tehlikelerle birlikte İnternetin yanlış kullanımından da kaynaklanan bir takım toplumsal sorunlar ve güvenlik sorunları yaşanmaktadır.

3.1.2.1 Toplumsal Sorunlar

Türkiye’de, genellikle yasadışı ve zararlı içerikten ve İnternetin yanlış kullanımından kaynaklanan toplumsal sorunları; aileler üzerindeki olumsuz etkileri ile çocuklar ve gençler açısından oluşan riskler ve sorunlar temelinde ele alabiliriz.

3.1.2.1.1 Aile Üzerindeki Olumsuz Etkileri

Bilişim alanında yaşanan değişimler, özellikle mobil telefonların ve İnternetin yaygın olarak kullanılmaya başlaması hem yapı, hem fonksiyonları hem de aile üyelerinin ilişkileri açısından aile yapımızı olumsuz yönde etkilemiştir ve etkilemeye devam etmektedir (TBMM, 2012: 473). Örfi, ahlaki ve dini olarak kabul edilmeyen birçok duruma İnternet ortamında izlenme ve yaşama imkanı doğmuş ve toplumdaki ahlaki çözülme ve yozlaşma adeta kendine yeni bir mecra bulmuştur (Turan, 2008: 73).

Bu olumsuzlukları dünyayla paralel olarak üç noktada toplayabiliriz. Bunlardan birincisi, İnternetin aşırı kullanımının aile içi iletişime verdiği zarardır. Günümüz ailesinde bu sorunun öznesi daha çok çocuklar ve gençler olarak gözükmemektedir. Türkiye’de İnternet kullanımının özelliklerini ortaya koyan araştırma verileri, çocuklar ve gençlerin artan bir şekilde genel olarak İnternette ve bilgisayar oyunlarında aşırı zaman harcadıklarını göstermektedir. Nitekim, Youth Insight’in 2012’deki 15-30 yaş grubundaki liseli ve üniversiteli gençleri kapsayan araştırmasına göre, üniversiteli gençlerin %97’si haftada en az 42 saatini, liseli gençlerin %97’si de haftada en az 31 saatini İnternet başında geçirmektedir. Bu tablo gençlerin klasik medyadan giderek uzaklaştığını ve İnternete yöneldiğini ortaya koymaktadır.⁶⁶

Araştırma’ya göre, gençlerin hayatında İnternet artık aynı zamanda “sosyal paylaşım siteleri” anlamına da gelmektedir. Nitekim, üniversitelilerin %87’si, liselilerin ise %67’si İnternete girme amacının sosyal paylaşım sitelerinde dolaşmak olduğunu

⁶⁶ Üniversiteli gençlerin %72’si haftada en az 14 saatini TV izleyerek, %69’u haftada en az 8 saatini gazete okuyarak, %57’si de haftada en az 10 saat radyo dinleyerek zaman geçirmektedir. Bu oranlar liselilerde ise sırasıyla şöyledir: Haftada 14 saat TV izleyenler %80, 8 saat gazete okuyanlar %44, 10 saat radyo dinleyenler %33. Ayrıca, üniversiteli gençlerin %28’i dergi okurken, liseli gençlerde bu oran %9’da kalmaktadır (Marketing Türkiye, 2012: 77-78).

belirtmektedir. Araştırma, gençlerin yarıya yakınının İnternete cep telefonlarından bağlandıklarını, liselilerin %22'sinin, üniversitelilerin ise %41'inin İnternette alışveriş yaptığını ortaya koymuştur. Keza, üniversitelilerin %88'inin, liseli gençlerin %73'ünün e-posta kullandıkları tespit edilmiştir (Marketing Türkiye, 2012: 77-78).

İlköğretim 2. kademe ve lise öğrencileri üzerinde yapılan 2011 tarihli bir araştırmaya göre, ilköğretim 2. kademe öğrencilerinin %71,7'sinin, lise öğrencilerinin %86,2'sinin evinde İnternet bağlantısı bulunmaktadır. Ekonomik durumu fakir/muhtaç olan öğrencilerin bile evlerinde İnternet bulunma oranı %40,5'tir. Cep telefonunda İnternet erişimi bulunma oranı ise şöyledir: İlköğretim 2. kademe öğrencileri %57,7, lise öğrencileri %68,1 (Mutlu Çocuklar Derneği, 2011:16-17, 21).

Araştırmada, ilköğretim 2. kademe öğrencilerinin %76,9'unun, liselilerin %81'inin haftada en az bir gün; ilköğretim öğrencilerinin %19,5'inin lise öğrencilerinin %23,7'sinin her gün İnternet kullandıkları görülmüştür. Araştırma, bu öğrencilerin bilgisayar, İnternet ve cep telefonu ile geçirdikleri günlük toplam sürenin 5-6 saat olduğunu ortaya koymuştur (Mutlu Çocuklar Derneği, 2011: 26-27,78).

Çocukların İnternet kullanım amaçları arasında sohbet %47,8, film-müzik indirme-paylaşma %47,6, oyun %47,6, e-posta ve haberleşme %37,7, haber ve bilgilere erişim %21,5 ve blog-form yazma vb. %6,4 yer tutmaktadır. Öğrencilerin e-posta, blog, web site veya forum sahibi olma açısından durumu ise şöyledir: e-posta %82,7, blog %9,8, web site veya forum %14 (Mutlu Çocuklar Derneği, 2011: 50-51,55).

“ComScore”un yayınladığı bir rapora göre ise, Avrupa'nın en aktif İnternet kullanıcıları Türkiye'de bulunmaktadır. 2011 yılı Ağustos ayını esas alan Rapor'da, ülke kullanıcılarının bir hafta içinde İnternette geçirdikleri süre açısından bakıldığında ilk sırayı 34,7 saat ile İngiltere, ikinci sırada 32,8 saat ile Hollanda ve üçüncü sırada 32,7 saat ile Türkiye yer almasına rağmen, ziyaretçi başına sayfa görüntüleme bakımından Türkiye aylık 3.706 sayfa ile ilk sırada 3.205'le İngiltere ikinci ve 3.181 ile Hollanda üçüncü sırada bulunmaktadır. Raporda, İnternette

geçirilen süre açısından dünya ortalamasının haftada 23,6 saat, sayfa görüntüleme ortamasının ise 2.211 sayfa olduğu belirtilmektedir (ComScore, 18.10.2011).

Rapora göre Türkiye kullanıcıları bir ay içerisinde İnternette toplam 45,3 milyar dakika geçirmektedir. En çok vakit harcadıkları site ise, harcanan toplam zamanın yaklaşık %30'unu oluşturan, 13,1 milyar dk. ile Facebook'dur. Daha sonra 4 milyar dk. ile Microsoft siteleri ve 3,9 milyar dk. ile Google siteleri gelmektedir. Yine de son ikisinin toplamı Facebook'a yetişmemektedir (ComScore, 18.10.2011).⁶⁷

Keza, "comScore"un raporlarına yansıyan, video izleme yaygınlığı konusunda dünya'da ilk sırada yer almamız ComScore (14.10.2011), ziyaretçi başına sayfa görüntüleme bakımından Avrupa'da birinci olmamız (ComScore, 18.10.2011), spor sitelerini ziyaret konusundaki Avrupa liderliğimiz (Webrazzi, 12.12.2012) ve haftalık İnternet kullanımındaki Avrupa üçüncülüğümüz (ComScore, 18.10.2011) teknolojiyi kullanma konusundaki üstün başarımızın birer nişanesi olarak görülebileceği gibi; bu üstün başarıların toplumsal bir bedeli olarak, aile içi ilişkiler ve iletişim ve benzeri konularda ortaya çıkabilecek sorunların habercisi olarak da algılanabilir. Yani, bu durum aynı zamanda, çocuklarımızın ve gençlerimizin ailesi ve yakınlarıyla beraber olmak ve onlarla hoşça vakit geçirmek yerine, sanal alemde nelere zaman ve emek harcadıklarının fotoğrafını da vermektedir.

Diğer yandan, TTNET'in araştırmasında ortaya çıkan, ülkemizde İnternet kullanımının en çok akşam saat 21.00 ile 24.00 arasında gerçekleştiriliyor olması (TTNET blog, 2011) sonucu da konumuz açısından endişe verici olarak değerlendirilebilir. Bu durum şöyle yorumlanabilir; gün içinde çok az İnternete girenler veya hiç girmeyenler akşam yemeğinden sonra çoğunlukla bilgisayar başına oturmakta ve İnternet kullanım oranı günün son 3 saatinde zirve yapmaktadır. Halbuki, bu saatler daha ziyade ailenin bir araya gelebildiği ve birlikte olarak, görüşme, konuşma, dertleşme, paylaşma yani kısaca yüzyüze iletişim kurabildiği

⁶⁷ Küresel devlerin ardından sıralama şu şekilde devam etmektedir: Mynet 1,360 milyar dk., Aksoy Group (Sahibinden.com'un etkisiyle) 0,991 milyar dk., Demirören-Karacan Gazetecilik 0,973 milyar dk., Hürriyet İnternet Grubu 0,519 milyar dk., Doğan Gazetecilik 0,263 milyar dk. Doğan Online 0,240 milyar dk. ve Turkuvaz Yayın 0,237 milyar dk (ComScore, 18.10.2011).

zamanlardır. Bu araştırma verisi, aile bireylerinin, ailenin iç iletişimi için en kritik zaman dilimini İnternete feda ettikleri sonucunu ortaya çıkarmaktadır.

İnternetin aile üzerinde meydana getirdiği olumsuz etkilerin ikinci noktası ise, eşlerin birbirlerini “aldatma”larını kolaylaştırması ve sonu aile facialarına ve boşanmalara kadar varan sorunların yaşanmasına neden olmasıdır. İnternetin yaygınlaşması ve yeni teknolojik imkanlar sunarak anlık görüntülü yazışmaların başlaması ile birlikte eşler arasında “aldatma” temelli evlilik birlikteliğini sarsacak yeni boşanma gerekçeleri ortaya çıkmıştır. Öyle ki, İnternetle birlikte “aldatma” olgusu kendisine basit, kolay ve cazibe uyandıran yeni bir mecra bulmuştur denilebilir.⁶⁸

Nitekim, Avrupa Cinsel Sağlık Birliği tarafından Türkiye’de yapılan “Modern Hayat ve Cinsellik Araştırması”na göre, kadınların “yeni duygusal deneyimler” için, erkeklerin ise yalnızlık, eşiyle kavgalı olması ve yeni cinsel deneyim isteği gibi sebeplerle İnternette ilişkilere yöneldiği görülmüştür. Araştırmada, “İnternette ilişki düşünür müsünüz?” şeklindeki soruya kadınların %34,3’ünün erkeklerin %55,9’unun olumlu cevap verdikleri belirtilmektedir (Stargazete.com, 14.02.2009).

Her zaman aldatma veya boşanma ile sonuçlanmasa da, İnternet ortamının popüler sayfaları olan sosyal paylaşım sitelerinin ikili ilişkilerde kıskançlık ve güvensizlik gibi olumsuz davranışlara neden olduğu bilinmektedir. Nitekim, İnternet yazışmalarının eşler arasında güven ortamını sarsacak sonuçlara yol açtığı konusunda medyaya yansımış çok sayıda örnek olay bulunmaktadır.

İnternetin aile üzerindeki olumsuz etkilerinin bir diğer noktasını ise, barındırdığı zararlı ve sakıncalı içerikler oluşturmaktadır. Ülkemizde İnternetin belki de en çok eleştirildiği yönü, barındırdığı ve kullanıcılarına sunduğu müstehcenlik, fuhuş, şiddet, uyuşturucuya teşvik, kumar gibi sakıncalı ve zararlı içeriklerdir.

⁶⁸ Psikiyatri Uzm. Dr. Oğuz Tan anlatıyor: “Evliliği kötü olmayanlar, aldatmayı asla düşünmeyenler, karakteri aldatmaya uygun olmayanlar bile İnternette aldatabilirler. Çünkü; önce her şey masum niyetlerle başlar: ‘Sadece sohbet etmek istiyorum’ gibi. Sohbet flörte dönüşünce, kendini aldatmak kolaydır: ‘Nasıl olsa birbirimizi görmemiz bile mümkün değil’. Bir de bakarsınız, ateş bacayı sarmış. Bu tür aldatma, sinsice ruhu ele geçirdiği, aldatma niyetini olmayanı bile baştan çıkardığı için, en iyisi, evlilerin İnternet sohbetlerinden tamamıyla uzak durmalıdır.”(Haber7, 13.08.2009).

Nitekim, TİB İnternet Bilgi İhbar Merkezi'ne Nisan 2012 tarihine kadar yapılan toplam 500.244 adet ihbarın türleri ve yüzdelik oranlarına ait şu veriler bu olguya işaret etmektedir: Müstehcenlik %48,37, Fuhuş %8, Atatürk Aleyhine İşlenen Suçlar %7,35, Bahis %6,58, Çocukların Cinsel İstismarı %4,51, İntihara Yönlendirme %3,85, Sağlık İçin Tehlikeli Madde Temini %0,62, Uyuşturucu/Uyarıcı Madde Kullanılmasını Kolaylaştırma %0,16 (Dolu, 2012).

Keza, bir başka araştırma, ebeveynlerin %90'ının çocuklarının İnternet kullanımı esnasında müstehcenlik, şiddet ve kötü niyetli kişilerle arkadaşlık gibi çeşitli risklerle karşı karşıya olduklarına ilişkin kaygı taşıdıklarını ortaya koymuştur (Teknoloji Bilinçlendirme Platformu, 2010: 11-12). Başka bir çalışmada ise, ana-babaların İnternetle ilgili gördükleri riskler önem sırasına göre; uzun süre oyun oynamaya bağlı asosyal kişilik, pornografik içerik ve kötü niyetli sanal sohbetten doğacak tehlikeler ve İnternet bağımlılığı olarak tespit edilmiştir (Bensghir ve Altınok, 2005: 63).

Ülkemizde İnternetin ailede/toplumsal yapıda meydana getirdiği zararlar bakımından en çok gündeme gelen konu şüphesiz müstehcenliktir. İsteyerek/istemeyerek kolayca ulaşılan bu tür içeriklerin bireyleri kısa sürede bağımlı hale getirdiği, gördüklerini yapma konusunda tahrik ettiği ve yeni cinsel arayışlara ittiği, kişilerin sosyal hayatını altüst ettiği ve psikolojik dengesini bozduğu, eşler ile ilişkilerde sorunlara sebep olduğu, aile içi huzursuzluklara ve boşanmalara neden olduğu bilinmektedir.⁶⁹

⁶⁹ Bakırköy Ruh Sağlığı ve Hastalıkları Hastanesi'ne İnternet ve pornografi bağımlılığı şikayetiyle başvuruda bulunan iki vakanın kısa hikayeleri şöyledir: *Birinci vaka:* Hasta 30 yaşında, erkek, ilkokul mezunu, işçi, boşanmış, 1 çocuk sahibi, anne, babası ve çocuğuyla yaşıyor. Haftada en az 4 gün, sabah 08.00 ile akşam 17.00 saatleri arasında, neredeyse aralıksız olarak çeşitli türlerde porno film izliyor. Bunun yanında İnternet kullanımı nedeniyle derecesi ilerlemiş boyun fıtığı var. Sekiz senedir aşırı İnternet kullanıyor. Bu süre içinde İnternet bağımlılığı nedeniyle çok kere işe gitmediği veya mesai saatleri içerisinde işini terk ettiği için 20'den fazla iş değiştirmiş. Yaklaşık 1,5 sene önce 7 yıllık eşi şiddetli geçimsizlik nedeniyle evi terketmiş. Özellikle aşırı porno izlemeye başlamasının ardından eşine karşı cinsel isteksizlik geliştiğini, eşiyle ilişkiye girse dahi tatminsizlik yaşadığını söylüyor. Neredeyse ailesiyle katıldığı hiçbir sosyal etkinlik yok. Tüm yaşantısı İnternette porno izleme etrafında geçiyor. Psikiyatrik muayenesinde duygudurumunun depresif olduğu, yoğun suçluluk ve intihar düşüncelerinin bulunduğu tespit edilmiş. *İkinci vaka:* Hasta 49 yaşında, erkek, lise mezunu, memur, 20 yıllık evli, 3 çocuklu, eşi ve çocuklarıyla yaşıyor. Düzenli iş hayatı olmasına rağmen, iş dışı tüm vaktini İnternette eğlence oyunları (okey vs.), İnternette tanıştığı kadınlarla sohbet, porno izleme gibi aktivitelerle geçiriyor. İşten çıkar çıkmaz İnternet kafede 1-2 saat civarında İnternet başında süre geçiriyor, evde ise çocukları ve eşiyle hemen hemen hiç konuşmuyor ve çocukları

Görüldüğü gibi, İnternet kullanımının yaygınlaşması, toplumun temel çekirdeği olan aile kurumunu olumsuz yönde etkileyecek ciddi riskler ve tehditleri de beraberinde getirmektedir. Bu risklerin ve tehditlerin farkında olarak, aile kurumunun korunması için önleyici tedbirler almak, kamu politikaları geliştirmek ve uygulamak, kamu otoritelerinin ve STK'ların öncelikli görevlerinden olmalıdır.

3.1.2.1.2 Çocuklar ve Gençler Üzerindeki Olumsuz Etkileri

Çocuklar ve gençler eskiden evlerinde, mahallelerinde ve okulda yaptıkları öğrenme, keşfetme, oyun oynama ve arkadaşlarıyla buluşma aktivitelerini bugün İnternet ortamında yapmaktadır (Alıkaşıfoğlu, 2012). Bu yönüyle aslında İnternet teknolojisi çocuklara ve gençlere eğitim, eğlence ve gelişimlerinin desteklenmesi konusunda büyük olanaklar sunmaktadır. Ancak, bu olanakların yanı sıra cinsel istismar, pornografi, fuhuş, siber zorbalık, şiddet, nefret, intihara yönlendirme, kumar, bahis ve şans oyunları ve uyuşturucuya teşvik gibi uygun olmayan içeriklerle karşılaşma; İnternet bağımlılığı, dijital oyunlar ve sosyal ağların riskleri ve tehlikeleriyle muhatap olmalarına neden olmakta ve önemli sorunlar ortaya çıkarmaktadır.

3.1.2.1.2.1 Cinsel İstismar, Pornografi ve Fuhuş

İnternetin pornografinin hızla yayılması ve kolayca erişimine yönelik sunduğu imkanlara mukabil, çocukların ve ergenlerin öne çıkan merak etme, deneme, risk alma, otoriteye kaşı çıkma eğilimleri ve doğru karar verme yetilerinin tam gelişmemiş olması, onları tüm dünyada olduğu gibi ülkemizde de riske ve cinsel istismara en açık grup haline getirmektedir. Aşırı ve bilinçsiz İnternet kullanımı bu riski daha da artırmaktadır (Alıkaşıfoğlu, 2012).

Nitekim, Türkiye’de yapılmış bir çok araştırmada bu konuya ilişkin bulgulara rastlamak mümkündür. Araştırmalarda, İnternetle ilgili olarak ailelerin çocukları için en çok endişe duydukları ve tehlike oluşturduğuna inandıkları konunun pornografik

uyuyana kadar yaklaşık 4-5 saat İnternet başında vakit geçiriyor. Yapılan psikiyatrik muayenede anksiyete düzeyinin yüksek olduğu, güvensiz yetersiz kişilik özellikleri ve depresif belirtilerin varlığı, endişe ve karamsarlık saptanmış.(Vakalara ait bilgiler Uzm. Dr. Ömer Şenormancı’dan alınmıştır.)

içerikler olduğu görülmektedir (ASAGEM, 2008). “EU Kids Online Türkiye” araştırması bu endişelerin haklılığını doğrulamaktadır. Bu çalışmada Türkiye’deki çocukların yaklaşık %13’ü İnternet’te cinsel içerikli fotoğraf gördüğünü; bunların %46’sı da gördükleri cinsel içerikli fotoğraflardan rahatsız olduğunu belirtmiştir. 9-16 yaş arasındaki çocukların %12’i cinsel içerikli mesaj aldığını, %4’ü de buna benzer mesaj yolladığını söylemiştir. Bu tür mesaj aldığını söyleyen çocukların %50’si bundan rahatsız olduğunu bildirmiştir. Aynı grup çocukların %14’ü yüz yüze tanışmadığı kişilerle İnternet’te görüşüğünü, sadece %2’si bu kişilerle İnternet dışında da buluştuğunu belirtmiştir (EU Kids Online, 2010).

Türkiye’de büyük çoğunluğu çocuklar ve gençlerden oluşan İnternet kullanıcılarının İnternette müstehcenlikle ilgili arama yapma durumu için Google istatistiklerine bakıldığında oldukça düşündürücü rakamlarla karşılaşmaktadır. Örneğin “porno” terimine 2004’ten 16.04.2013 tarihine kadar gösterilen bölgesel ilgiye bakıldığında Türkiye dünyada 4. sırada bulunmaktadır.⁷⁰ “Seks” teriminin aranmasında ise Özbekistan ve Türkmenistan’ın ardından üçüncü sırada yer almaktadır (Google, 16.04.2013b). İlginç bir durum ki, “porno” teriminin aranma düzeyi 2010 yılına kadar belli bir bandın içinde stabil olarak seyrederken, 2010 yılı Ağustos’undan sonra hızla artarak iki katına çıkmış ve 2013 yılı Martı’nda zirve yapmıştır. Aynı süre zarfında dünya’da “porno” teriminin en çok arandığı şehirler sıralamasında ise ilk üç sırayı İstanbul, İzmir ve Ankara almaktadır (Google, 16.04.2013a).⁷¹

Yine, BTK’nın 2012 verilerine göre Türkiye’deki İnternet kullanıcılarının 60 saniyelik zaman kesiti içerisinde yaptıkları aktiviteler içerisinde en dikkat çekici istatistiklerden birisi de 2 milyon kullanıcının çevrimiçi porno izlediğini gösteren rakamdır (BTK, 2012). Keza, TİB’nin yaptığı teknik değerlendirmelerde ülkedeki İnternet kullanıcılarının %73’ünün müstehcen siteleri ziyaret ettikleri görülmüştür

⁷⁰ Arama hacmi endekslerine göre sıralama şöyledir: 1. Ermenistan 100, 2. Arnavutluk 71, 3. Gürcistan 66, 4. Türkiye 65, 5. Kolombiya 51, 6. Romanya 50, 7. Moldova 48, 8. Peru 47, 9. Mali 46, 10. Kongo 46. (Google, 16.04.2013a).

⁷¹ Arama hacmi endekslerine göre sıralama şöyledir: 1. İstanbul 100, 2. İzmir 97, 3. Ankara 96, 4. Bogota 73, 5. Roma 67, 6. Mexico City 64, 7. Milano 62, 8. Buenos Aires 57, 9. Madrid 55, 10. Sao Paulo 48. (Google, 16.04.2013a).

(TİB, 2010). Nitekim, Türkiye’den İnternet pornografisine yönelik giderek artan kullanıcı talebi nedeniyle ülkemizde bu sektörün büyüdüğü ve dünyadaki büyük firmaların da Türkiye’ye gelmeye başladığı dile getirilmektedir (Par, 2013).

Benzer şekilde, çocuk pornografisi ve çocuk istismarı içerikleri tüm dünyayla birlikte, ülkemiz İnternet kullanıcılarının büyük çoğunluğunu oluşturan çocuklarımız ve gençlerimiz için de ahlaki tahribat, bağımlılık ve en önemlisi cinsel istismara maruz kalmak yönünden tehlikeler oluşturduğu görülmektedir.

Pedagog Barış Çiçek İnternette çocukların peşine düşmüş binlerce cinsel sapığın olduğuna dikkat çekmektedir. Nitekim, yıllardır sürdürdüğü araştırmanın bir parçası olarak herhangi bir cuma günü öğleden sonra İnternet sohbet sitelerinden birine “Begüm10” takma ismi ile giren Çiçek, kendisini 10 yaşında ve beşinci sınıf öğrencisi olarak tanıtmış ve şüphe çekmemek için de klavyeyi yavaş kullanmış ve kasıtlı imla hataları yapmıştır. “Begüm10”a ilk yarım saat içinde 43’ü cinsel içerikli, 100 mesaj gelmiştir. Begüm özellikle bu 43 kişiye ilk mesajda 10 yaşında olduğunu tekrar belirtmiş sadece bir kişi yaşı öğrendikten sonra özür dileyerek bağlantısını kesmiştir. Diğerleri ise görüşmeyi kesmediği gibi bağlantının kesilmemesi için olağanüstü çaba sarfetmiştir. Hepsi büyük bir istekle 10 yaşındaki bir çocuğa cinselliği öğretmeye çalışmışlardır (NTVMSNBC, 28.03.2011).

Pedagog Çiçek, 40 kontör karşılığı çocuklardan kamera görüntüsü istendiğini ve çocukların da bunun kötü bir şey olduğunu çoğu zaman anlamadığını belirtmektedir. Keza, pedofililer genellikle çevrelerinde sevilen insanlardır ama iç dünyalarında bir canavar beslemekte ve fırsatını bulduklarında hemen suça yönelmektedir. Buna mukabil çocukların duygularına ulaşmak ve birine bağlanmalarını sağlamak kolaydır, hele İnternette bu çok daha kolay başarılabilir. Çoğu zaman istismar edilen çocuklar, durumları vahim olduğu halde utançtan ya da suçlanmaktan korktukları için bunu ana-babalarına anlatamamaktadır (NTVMSNBC, 28.03.2011).

Yine, tamamına yakını Güney Amerika ve Uzak Doğu kaynaklı olan çocuk pornosu sitelerine ülkemizden çok ciddi giriş mevcuttur. Bu sitelerin erişimi 5651 sayılı

Kanun gereğince TİB tarafından resen engellenmektedir. Fakat, yurt dışı kaynaklı olmaları nedeniyle mücadelede güçlük çekilmekte; bu siteler erişimin engellenmesi üzerine aynı faaliyetlere başka siteler üzerinden devam etmektedir (BTK, 2012).

Ülkemizde çocuk pornografisi kadar tehlike oluşturan bir pornografik içerik türü de Türkçe yazılmış “seks hikaye” siteleridir. İnternet ortamında insan hayalinin sınır tanımaz ürünleri olarak sürekli yenilenerek yayınlanan bu tür hikayeler önü alınamaz bir hale gelmiştir. Siteden siteye opyalarak hızla yayılan ve özellikle ensest, hayvan, eş değiştirme, gay, lezbiyen, liseli, okul gibi başlıklarla yayına sunulan metin içerikli hikayeler çocukların ve gençlerin temiz dimağlarını kirletmektedir. Maalesef, ülkemiz kullanıcılarından ilgi de görmektedir.⁷²

Bazen bu tür Türkçe içerikler Facebook’ta da yer aldığı gibi, ücretsiz site araçları veya blog siteleri de bu türden pornografiyi yaymak için sıklıkla kullanılmaktadır. Dünyaca ünlü “www.wordpress.com” ve “www.blogspot.com” siteleri bunlardan ikisidir. Yüzmilyonlarca kullanıcısı olan bu ücretsiz sitelerde alt domain oluşturulması ve buradan pornografik içerik yayınlanması sadece on dakikayı almaktadır (İstanbul İnternet Kafeciler Esnaf Odası, 2012).

Bir de konunun fuhuş boyutu vardır. İnternet ortamında daha çok arkadaşlık, çöpçatanlık ve sohbet siteleri gibi sosyal ağ siteleri kullanılarak fuhuş aracılık ve teşvik fiili gerçekleştirilebilmektedir. Böylece hem maliyetler azaltılmakta hem de fuhuş aracılık alenen yapılmadığı ve genellikle şifreli yazışmalarla yapıldığı için gizlenme fiili için ideal bir ortam oluşturulmaktadır (Kaya, 2010: 112). Keza, TİB İnternet Bilgi İhbar Merkezi’ne Nisan 2012 tarihine kadar yapılan toplam 500.244 adet ihbarın %8’i fuhuş şikayetidir. Yani, İnternetin fuhuş amaçlı kullanıldığına ilişkin 40 bin civarında ihbar alınmıştır.⁷³

⁷² Örneğin, bir forum sitesinde, bir baba ile 13 yaşındaki kızı arasındaki ensest ilişkiyi pornografik bir şekilde anlatan bir metin, 2011 yılı içinde 30 günden kısa bir sürede 11.116 defa görüntülenmiştir (İstanbul İnternet Kafeciler Esnaf Odası, 2012)

⁷³ İhbarlardan birisi şöyledir: “..paraya ihtiyacı olan öğrenci bayanları iş ve para vaadiyle kandırarak modellik ve hatta fuhuşa zorluyorlar nette modellik yaparken çekilmiş görüntüleri dağıtma tehdidiyle benim ve arkadaşlarımın başına geldi kurtulamıyoruz lütfen yardım edin” (BTK, 2012).

3.1.2.1.2.2 Siber Zorbalık

Uzmanlar Türkiye’de İnterneti en çok kullanan grubun öğrenciler olduğundan hareketle ülkemizde siber zorbalık konusunda potansiyel bir riskin bulunduğunu belirtmektedir. Zaten okullarımızda özellikle gençler arasında ad takma, itme, çelme takmadan tutun da küfüre kadar varan çok geniş bir yelpazede fiziki akran zorbalığının ve şiddetin varlığı bilinmektedir. Bunun biraz şekil değiştirerek sanal ortama taşınması ve yaygınlaşması uzak bir ihtimal değildir (Ergene, 2012).

Nitekim ülkemizde gerçekleştirilen bilimsel çalışmalarda sorun açık bir şekilde kendisini göstermektedir. İlköğretim ikinci kademedeki öğrencilerle gerçekleştirilen bir araştırmada; öğrencilerin %32,6’sının en az bir kez sanal zorbalığa maruz kaldıkları, %22,5’inin ise bir ve daha fazla sanal zorbalık davranışlarını yaptıkları belirlenmiştir (Aydoğan vd., 2009). Başka bir araştırmada da, liselerde okuyan öğrenciler arasında siber zorbalık oranının %28, siber kurban oranının ise %30 olduğu görülmüştür (Erdur-Baker ve Kavşut, 2007: 31-42).

Yine liselere yönelik bir araştırmada ise öğrencilerin %35,7’sinin sanal zorbalık davranışları sergiledikleri, %23,8’inin hem zorba davranışlar gösterdikleri hem de kurban olarak seçildikleri tespit edilmiştir. Kız öğrencilerin ise %36’sının İnternet üzerinde zorbalık davranışlarına maruz kaldığı belirlenmiştir (Arıcak vd., 2008: 255).

Üniversite öğrencileri üzerinde yapılan bir araştırmada; öğrencilerin %22,5’inin sanal zorbalık yaptıkları, %55,3’ünün ise sanal zorbalığa hayatlarında en az bir kez maruz kaldıkları tespit edilmiştir. Ayrıca, erkek öğrencilerin bayanlara göre sanal zorbalık davranışlarını daha fazla yaptıkları görülmüştür (Dilmaç, 2009: 1307-1325).

Tüm bunların yanında, İnternet ortamının özellikle çocuklar ve gençler arasında küfür ve argo kullanımını yaygınlaştırdığı ve yalan söylemeyi alışkanlık haline getirdiği de belirtilmektedir (AREM, 2008:39). Bu çerçevede, MEB Fatih Projesi’nin öğrencilerin bilgiye ulaşmalarında çok ciddi bir kolaylık sağlamakla birlikte, gerekli tedbirler alınmazsa, sanal zorbalığın artması ve yaygınlaşması konusunda da kolaylaştırıcı bir etkiye sahip olabileceğinden endişe edilmektedir (Ergene, 2012).

Nitekim, kendisiyle mülakat yapılan Aydın da Fatih Projesi'yle, 17 milyon öğrenciye tablet dağıtılacağını ve bunun İnternete erişimi müthiş artıracığını, fakat aynı zamanda İnternetle birlikte ortaya çıkan risklerin artışına da ivme kazandıracağına dikkat çekmektedir (E. Sadık Aydın ile kişisel iletişim, 25.07.2013).

3.1.2.1.2.3 Şiddet, Nefret ve İntihara Yönlendirme

İnternet ortamında yer alan kavga, çatışma, işkence, savaş, cinayet, infaz, yaralama gibi vahşet ve şiddet konulu içerikler ülkemizde de yaygın olarak rağbet görmekte, izlenmekte ve paylaşılmaktadır. Türkiye'deki İnternet kullanıcılarının video izleme konusunda dünyada ilk sırada yer almasında (ComScore, 14.10.2011), video izlemenin tüm İnternet trafiğinde bandı en çok meşgul eden aktivite olarak ön plana çıkmasında (TTNET blog, 2011), Youtube'un uzun süre yasaklı olmasına rağmen, 2004'ten bu yana Türkiye'den Google aramalarında Facabook'tan sonra en çok aranan ikinci kelime olmasında (Google, 16.04.2013c) bu merakın izleri bulunabilir.

Benzer şekilde yabancı düşmanlığı, ırk, cinsiyet, din ve mezhep temelli ayrımcılık ve nefreti teşvik etme ve kışkırtmaya yönelik İnternet içerikleri de başta gençler olmak üzere tüm toplumsal kesimler üzerinde olumsuz tesirler meydana getirmekte ve sosyal barışı ve huzuru tehdit etmektedir. Nitekim, "İnternet Mecraları, Kanaat Oluşumu ve Dolaşımı: Kamusal ve Mahrem Arasında" isimli araştırmada, İnternet'te demokratik bir tartışma kültürünün olmadığı; ırkçı, mezhep ayrımcı, cinsel kimliği aşağılayan ve küçük düşüren nefret söyleminin var olduğu, kullanıcıların gerçek yaşamdaki kimliklerine yakın hatta benzer kişilerle iletişim kurdukları ve farklı olana tahammülsüzlük gösterdikleri tespit edilmiştir (Alternatif Bilişim Derneği, 2012a).

Türkiye'de özellikle de sosyal medya ve haber sitelerinin okuyucu yorumları nefret söyleminin giderek yükseldiği alanlar olarak dikkat çekmektedir. Bu konuda alarm vermenin vaktinin geldiği; İnternette yayılan nefret söylemine karşı kullanıcıların farkındalığını artırmak ve yeni medya ortamlarındaki karşı örgütlenmelerle barış dilini yaymak için harekete geçmek gerektiği dile getirilmektedir. Nefret söylemi yayan, farklı olanı hedef gösteren ve nefret suçunu teşvik eden haber sitelerini, okur

yorumlarını, web sitelerini, Facebook gruplarını, Twitter mesajlarını engelleme gerekliliği üzerinde durulmaktadır (Uçkan, 01.04.2013).

Ülkemizde intiharı özendir ve teşvik eden içerikler de özellikle gençler için risk oluşturmaktadır. Bilhassa psikolojik sorunlar yaşayan intihara eğilimli kişileri etkilemeye çalışarak onları intihara yönlendiren yazılar ve görüntüler barındıran siteler İnternet ortamında yer bulabilmektedir. İntihara yönlendiren web sitelerinin bir kısmı, satanizm gibi sapkın felsefi anlayış ve düşüncelerin propagandasını yaparak zayıf inançlı ve karakterli kişileri kandırmakta ve intihara sürüklemektedir. Ne yazık ki İnternette satanizmle ilgili yüzlerce siteyle karşılaşmak mümkündür. Satanist gruplar, İnternet siteleri, web sayfaları ve sohbet sitelerini yoğun ve organize bir şekilde kullanmaktadır (Bensghir ve Altınok, 2005: 26). Nitekim, TİB İnternet Bilgi İhbar Merkezi'ne Nisan 2012 tarihine kadar yapılan toplam 500.244 adet ihbarın %3,85'lük kısmına tekabül eden 19.264 tanesi intihara yönlendirme konusuyla ilgilidir (Dolu, 2012).

3.1.2.1.2.4 Kumar, Bahis, Şans Oyunları ve Uyuşturucuya Teşvik İçerikleri

Diğer ülkelerde olduğu gibi ülkemizde de İnternet, çocukların ve gençlerin kumar ve türevlerini oynama ve uyuşturucuya ve uyarıcı maddelere ulaşması konusunda erişimi kolaylaştırmıştır. Bu kolaylık gerçek hayatta kumarhanelerin veya gazinoların kapısından giremeyecek Türkiyeli İnternet kullanıcılarını hızla sanal gazinoların, online bahis ve şans oyunlarının müdavimi yapmaktadır. Üstelik ülkemizde sayıları her geçen gün artan “online kumarbaz” adı verilen yeni bir bağımlılık türü ortaya çıkarmıştır (Bensghir ve Altınok, 2005: 27).⁷⁴ Nitekim, Türkiye’de 1.5 milyon

⁷⁴ Bakırköy Ruh Sağlığı ve Hastalıkları Hastanesine İnternette kumar ve pornografi bağımlılığı şikayetiyle başvuruda bulunan bir vakanın kısa hikayesi şöyledir: Hasta 33 yaşında, lise mezunu, 10 yıllık evli, 2 çocuk sahibi ve 3,5 yıldır çalışmıyor. Son 4 yıldır eve geç geliyor veya hiç gelmiyor. Eşiyle ve çocuklarıyla hiç ilgilenmiyor. Aile, akrabaların yardımıyla geçimini sağlıyor. Hastanın İnternette seks ve kumar bağımlılığı 4 yıl önce her sabah işe gider gibi evden ayrılıp gün boyu İnternet kafeye gitmesiyle başlamış. Son 2 yıldır 200 TL’ye minik bir dükkan kiralamış ve burada bazen yeme, içme, tuvalet ihtiyacı dışında neredeyse 24 saat İnternette porno izleyip kumar oynuyormuş. Kiraladığı dükkandan ailesi ve arkadaşlarının haberi yokmuş. İnternette kumardan 50 bin TL kaybetmiş. Bunu ailesinden temin etmiş. (Bu vakaya ait bilgiler Uzm. Dr. Ömer Şenormancı’dan alınmıştır).

kişinin İnternette kumar ve bahis oynadığı, online kumar işletmelerinin yıllık cirolarının 1 milyar doları aştığı tahmin edilmektedir (Ankara Ticaret Odası, 2004).

Google’ın yayınladığı arama trendlerinde Türkiye’nin bahis sitelerine olan ilgisi açıkça görülmektedir. Facebook’un kendi altyapısında geliştirdiği ve 200 milyon üyesi ile dünyanın en büyük oyun platformu olan “Facebook Holdem Poker”in 2004 yılından 16.04.2013 tarihine kadar olan arama sonuçlarına göre Türkiye dünyada 7. sırada yer almaktadır.⁷⁵ 2012’de ise Türkiye Endonezya’dan sonra 2. sıradadır. Söz konusu terimin en çok arandığı şehirler sıralamasında ise, ilk onda dördüncü sırada İstanbul, beşinci sırada İzmir ve yedinci sırada Ankara bulunmaktadır.⁷⁶ 2012’de İstanbul, Jakarta’nın ardından ikinci sıradadır (Google, 16.04.2013d, 16.04.2013e).

Diğer yandan İnternet, uyuşturucu bağımlıları ve tacirlerine birçok konuda kolaylık ve geniş kitlelere ulaşma imkanı sunmakta; uyuşturucu maddelerin pazarlaması, satışı ve üretiminin her aşamasında yoğun bir şekilde kullanılmaktadır. Nitekim, e-mail gruplarında evde uyuşturucu madde yetiştirilmesinden türlerine, imalatından kullanımına kadar her türlü bilgi paylaşmakta ve kullanımı teşvik edilmektedir (Bensghir ve Altınok, 2005: 27). Keza, TİB Bilgi İhbar Merkezi’ne 2012 Nisan’ına kadar yapılan ihbarların 3.083 tanesi sağlık için tehlikeli madde temini, 820 tanesi de uyuşturucu/uyarıcı madde kullanılmasını kolaylaştırma konusudur (Dolu, 2012).

3.1.2.1.2.5 İnternet Bağımlılığı

İnternetin sunduğu imkanlar arttıkça ve çeşitlendikçe bireylerin İnternet kullanım sıklığı ve miktarı da giderek artmaktadır. Bu durum tüm dünyada olduğu gibi ülkemizde de İnternet bağımlılığı sorununu gündeme getirmektedir. Özellikle genç nüfusun yüksekliği, yeni gelişen bir ülke olmamız, İnternet kullanımının giderek yaygınlaşması, işsizlik ve İnternet kafelerin kontrolsüzce çoğalması ülkemizde İnternet bağımlılığı için uygun bir zemin oluşturmaktadır.

⁷⁵ Arama hacmi endekslerine göre sıralama şöyledir: 1. Endonezya 100, 2. Hırvatistan 79, 3. Bosna Hersek 75, 4. Sırbistan 40, 5. Yunanistan 26, 6. Filipinler 25, 7. Türkiye 25 (Google, 16.04.2013d).

⁷⁶ Arama hacmi endekslerine göre sıralama şöyledir: 1. Bandung (Endonezya) 100, 2. Jakarta 91, 3. Zagreb 69, 4. İstanbul 25, 5. İzmir 24, 6. Atina 22, 7. Ankara 19 (Google, 16.04.2013d).

Nitekim, yapılan bazı arařtırmalar Türkiye’deki İnternet bağımlılığının ipuçlarını vermektedir. Örneğın, Mutlu Çocuklar Derneğı’nın yapmış olduğı arařtırmada ilköğretim ikinci kademe ve lise öğrencilerinin 10 üzerinden 6,36’sı “bilgisayar ve İnternetsiz”, 5,69’u “cep telefonsuz”, 5’i “televizyonsuz” bir hayat düşünemediğini bildirmiştir (Mutlu Çocuklar Derneğı, 2011: 59). Keza, Youth Insight’ın liseli ve üniversiteli gençleri kapsayan arařtırmasında gençlerin 1/3’ü İnternetin “yokluğunda yaşayamayacakları bir şey” anlamına geldiğini belirtmiştir (Marketing Türkiye, 2012: 78). Bu tablo gençlerin İnternete tutkuyla bağlandıklarını ortaya koymaktadır.

Zaman içinde İnternet bağımlılığına ilişkin patolojik vakalar Türkiye’de de görülmeye başlamış ve ilk olarak 2011 yılında Bakırköy Ruh Sağlığı ve Hastalıkları Hastanesi’nde İnternet Bağımlılığı Kliniğı açılmıştır (Oktay, 2012). Ülkemizde de İnternet bağımlılığının siberseks bağımlılığı, siber ilişki bağımlılığı, online kumar bağımlılığı, bilgi bağımlılığı, bilgisayar ve İnternet oyunu bağımlılığı, İnternette alış-veriş bağımlılığı gibi türlerine ilişkin vakalar görülmektedir.

3.1.2.1.2.6 Dijital Oyunlar

Dijital oyunlar tüm dünyada olduğı gibi, ülkemizde de çocukların ve gençlerin İnternet kullanımında önemli bir yer tutmakta, fakat aşırı ve kontrolsüz kullanılması durumunda olumsuz etkiler meydana getirmektedir. Dijital oyunlarda yer alan kötü karakterlerin, kaba kuvvet ve şiddetin, cinsel çağrışımların, ayrımcılığı ve nefreti teşvik eden düşmanca tavırların, ahlaki değerlerden uzak rol modellerin ülkemiz çocukları ve gençleri üzerinde büyük tahribatlar yaptığı;⁷⁷ oyunların okul başarısını olumsuz yönde etkilediğı, fiziksel ve psikolojik sorunlara sebep olduğı ve bağımlılık oluşturduğı sıkça dile getirilmektedir (Dolu, 2012).

Diğeryandan, çevrimiçi dijital oyunların çocukların ve gençlerin yanlış kişi ve ortamlarla tanışmalarına vesile olduğı bilinmektedir. Son dönemde en popüler çevrimiçi oyun türü çoklu oyuncularla oynanan oyunlardır. Bunlarsa karşıdaki kişi

⁷⁷ Türkçe içeriğı sahip oyunlardan saygın bir gangster olmayı amaçlayan *Mafiatürk*, mafyavari bir hayatı teşvik eden *Konseyim*, vampir olarak hayatınızı sürdürmeyi konu alan *Bite Fight* gibi örneklerin sayıları her geçen gün artmaktadır.”(Güneş, 2012: 3).

ile anında mesajlaşma imkanı sağlamasından dolayı bazı riskler doğurduğu görülmektedir. Bu yüzden, dijital oyunların suç odakları tarafından kullanılmaya uygun özelliklerinin bulunduğu ve özellikle çocuk istismarı ve terör suçlarına hazırlık zemini oluşturmaya müsait olduğuna dikkat çekilmektedir (BTK, 2012).

Türkiye’de İnternetin oyun amaçlı olarak kullanımı yaygındır.⁷⁸ 20 milyon civarında dijital oyun kullanıcısının bulunduğu, bunların 15 milyon kadarının Facebook’dan oyun oynadığı tahmin edilmektedir (Dinç, 2012). Keza, yapılan bir araştırmada, 6-13 yaş grubundaki çocukların %95,2’sinin online oyun oynadığı tespit edilmiştir. Bu yaş grubu çocukların %49,1’inin başlıca İnternet kullanma nedeni online oyunlardır (Atıcı ve Batı, 2010). Nitekim, Dijital oyunların ülkemiz açısından ekonomik büyüklüğünün 150-200 milyon \$ olduğu tahmin edilmektedir (Dinç, 2012).

Dünyada bir ilk olan TÜDOF (Türkiye Dijital Oyunlar Federasyonu), 2011 yılında Gençlik ve Spor Bakanlığına bağlı bir federasyon olarak kurulmuştur. Ülkemizde dijital oyunlar ile ilgili kamu bilinci oluşturmak, sektör paydaşlarını bir araya toplamak, dijital oyunların gücünden yararlanmak gibi amaçlarla kurulmuş olan TÜDOF, ülkemizde Ulusal Oyun Derecelendirme sisteminin oluşturulması için de çalışmalar yürütmektedir (Dinç, 2012).

3.1.2.1.2.7 Sosyal ağlar

Türkiye’de, dünyadaki gelişme trendlerinin de ötesinde, neredeyse bir sosyal ağ ve özellikle Facebook çılgınlığı yaşanmaktadır. 2012 Mayıs itibariyle Facebook’un Türkiye’deki kullanıcı sayısı 32.131.260’dır (internetworldstats, 2012j). Aynı tarihte Türkiye’nin İnternet kullanıcı sayısı 36.455.000 olduğu dikkate alınırsa, ülkemizde Facebook kullanımının %88’i geçtiği ortaya çıkmaktadır. Bu oran aynı tarihler için dünyada %34,73, Avrupa’da %48,39’dur (internetworldstats, 2012j).

⁷⁸ TTNET araştırmasında İnternet kullanım amaçları arasında oyun oynama %55 olarak tespit edilmiştir (TTNET blog, 2011). Başka bir araştırmada ilköğretim 2. kademe ve lise öğrencilerinin İnternet kullanım amaçları içinde %47,6 ile oyun ilk üçte yer almıştır.(Mutlu Çocuklar Derneği, 2011: 55); Yine, Google Türkiye arama trendlerinde “oyun” terimi en çok aranan 5. kelime olmuştur (Google, 22.08.2013).

Dünyadaki İnternet kullanıcılarının sosyal ağlarda geçirdikleri süreyi 2012 Kasım ayı itibariyle ölçümleyen “comScore”, Türkiye’deki sosyal ağ kullanıcılarının aylık ortalama 8,6 saat ile bu sitelerde geçirilen süre bakımından dünyada beşinci sırada yer aldığını tespit etmiştir. Bu ortalama dünya genelinde 5,2 saattir.⁷⁹

Başka bir araştırmada, ilköğretim 2. kademe öğrencilerinin %74,9’unun Facebook, %14,9’unun ise Twitter adreslerinin, liselilerin %83,4’ünün Facebook, %23’ünün Twitter adreslerinin bulunduğu görülmüştür (Mutlu Çocuklar Derneği, 2011: 55).

Diğer bir rapordan Türkiye’deki Facebook kullanıcılarının yaşlara göre dağılımına baktığımızda; ilk sırayı %33’lük oranla 18-24 yaş aralığındaki kullanıcıların aldığını, 16-17 yaş ile 13-15 yaş aralığındaki kullanıcıların sayısının tüm kullanıcıların yaklaşık %20’sini oluşturduğu görülmektedir. 13-24 yaş aralığındaki kullanıcıların oranı ise %52’yi bulmaktadır (Socialbakers, 2011). Bu bağlamda, Facebook’u en çok gençler kullanıyor çıkarımını yapmak yanlış olmayacaktır.

Facebook kullanıcılarının yaş durumuyla ilgili ilginç bir bulgu da EU Kids Online Türkiye Araştırması’nda ortaya çıkmıştır. Buna göre, genel olarak çocukların %47’sinin sosyal paylaşım sitelerinde hesabı bulunurken, bu çocukların da 1/3’nün sosyal ağlara üyelik için alt sınır olan 13 yaşından küçük olduğu belirlenmiştir. Örneğin, sosyal paylaşım sitesi kullanan çocukların %85’inin profili bulunduğu Facebook’da, hesap oluşturma için 13 yaş sınırı konulmasına rağmen, hesabı bulunan tüm çocukların 1/3’ü 13 yaşının altındadır (EU Kids Online, 2010).

Ülkemizde özellikle gençler ve çocuklar arasında bu kadar yaygın olarak kullanılan sosyal ağların bir bütün olarak geleneksel iletişim tarzında ve sosyal ilişkilerde köklü değişimlere neden olduğu, güvenlik açısından bir takım sorunlar ve riskler taşıdığı bilinmektedir. Özellikle, konunun güvenlik boyutu açısından Facebook, YouTube, Twitter gibi sosyal paylaşım sitelerinin Türkiye’de irtibat bürosunun bulunmaması nedeniyle, ulusal mevzuatımızın uygulanmasında ve yurt içinden elde ettiği çok ciddi

⁷⁹ 1. sırasında 9,8 saat ile Arjantin, 2. sırada 9,7 saat ile Brezilya, 3. sırada 9,6 saat ile Rusya ve 4. sırada 8,7 saat ile Tayland bulunmaktadır (ComScore, 20.12.2012).

gelirleri üzerinden vergi gibi mali yükümlülöklere tabi tutulmasında, IP adreslerinin paylaşımı ve kişilik haklarının korunmasını teminen içeriğın çıkarılması gibi konularda işbirliğinin sağlanmasında sorunlar yaşanmaktadır (BTK, 2012).

3.1.2.2 Güvenlik Sorunu ve Mahremiyet İhlali

İnternetin, beraberinde bir takım güvenlik sorunları ve kişisel mahremiyet ihlalleri oluşturduğı bilinmektedir. Dünyanın diğerk ölkelerinde olduğı gibi ölkemizde de teknolojinin gelişmesiyle birlikte bilişim sistemleri kullanılarak işlenen suçlar hızlı bir şekilde artış göstermektedir (Şen, 2012).

Nitekim, Türkiye’deki İnternet kullanıcıları arasında korsan yazılım kullanımının yaygın oluşuna bağılı olarak, zararlı yazılıma maruz kalma riskleri de yükselmektedir. Alliance 2011 raporuna göre Türkiye’nin 2010’daki korsan yazılım kullanımı %62, bunun ekonomik büyüklüğü 516 milyon dolardır (BSA, 2011). Keza, başka bir araştırmada, İnternet kullanıcılarının %46,8’inin son bir yıl içinde İnternette güvenlikle ilgili sorunlarla karşılaştıkları görölmüştür. Bunların %36,4’ünün bilgisayar virüslerine maruz kaldıkları, %32’sinin de istenmeyen spam e-posta aldığı belirlenmiştir (DPT, 2011: 32).

Emniyet yetkilileri İnternet üzerinden işlenen suçlarda ve mağduriyette büyük bir artış olduğunu belirtmektedir. Hızla gelişen teknolojiyi ve sunduğı yeni imkanları etkili bir şekilde kullanan suçlulara ve suç örgütlerine karşılık, kolluk kuvvetleri ve Cumhuriyet Savcıları sınırlı kanun ve imkanlar ile mücadele etmektedir. İnternetin anomiliğinden ve karmaşık yapısından kaynaklanan nedenlerle, online işlenen suçlarda soruşturma yapmak için klasik suç soruşturması yöntemleriyle hareket edilmesinin yetersizliğı sonucunda failerin bulunamamasından dolayı çoğı zaman mağdurlar zararlarını sineye çekmek durumunda kalmaktadır (DPT, 2011: 32).

Bilişim suçlarından en fazla zarar görenler deneyimsizlikleri ve tekinsiz merakları ile çocuklar ve gençler olmaktadır. Nitekim, EU Kids Online Türkiye bulgularına göre, çocukların %42’si sosyal paylaşım sitesindeki hesaplarını kendi kişisel bilgilerinin herkes tarafından görölebileceğı “herkese açık” seçeneğı ile kullanmaktadır. Yine

çocukların 1/3'ü bu bilgilerini arkadaşları ile paylaşırken, %19'u adres bilgilerini, %8'i ise telefon numaralarını paylaşma açmaktadır (EU Kids Online, 2010).

Keza, 9-16 yaş grubu çocuklara yönelik başka bir araştırmaya göre, çocukların %44'ü kişisel bilgilerin sosyal paylaşım sitesinde herkese açık kullanılmasını güvenli bulurken, %47'si bu sitelerdeki kişisel bilgilerin gizliliğini korumaya yönelik kuralları bilmediğini, %16'sı ise bu kuralları okuyup anlamadığını belirtmektedir. Ayrıca çocukların %48'i tanımadığı kişiden arkadaşlık teklifi aldığı anda önce profiline bakıp sonra inanırsa kabul ettiğini, %13'ü ise tüm arkadaşlık tekliflerini kabul ettiğini belirtmiştir (TİB ve ODTÜ, 2011).

Diğer yandan, Türkiye aleyhinde faaliyet gösteren “com, org, net” uzantılı binlerce İnternet sitesi ABD, Almanya, Hollanda ve diğer Avrupa ülkeleri üzerinden yayın yapmaktadır. Hatta, bu sitelerde bomba yapımını detaylarıyla anlatan “Teröristin El Kitabı”, “Teröristin Yemek Kitabı” gibi eserler ve bir teröristin bilmesi gereken birçok konuda ayrıntılı bilgiler bulunmaktadır (Bensghir ve Altınok, 2005: 26).

Yine, ülkemizin sık sık siber saldırıların hedefi olduğu görülmektedir. Örneğin, Anonymous ve RedHack gibi gruplar başka ülkelerde olduğu gibi bizim ülkemizde de “siber saldırılar” yapmaktadır. Nitekim, Cumhurbaşkanlığı, TBMM, Başbakanlık, İçişleri/Dışişleri/Ulaştırma/Adalet Bakanlıkları, Genel Kurmay Başkanlığı, MİT, EGM, Yargıtay, YÖK, BTK, TTNET vb. kurum ve kuruluşlar siber saldırılara maruz kalmışlardır. Bu saldırılar sonucu birçok kamu kuruluşumuzun resmi web siteleri hacklenip kullanılamaz hale getirilirken, bazen de kurumlarımızın bilgisayar sistemlerine girerek bir takım gizli bilgilerin ele geçirilmesi mümkün olmuştur.⁸⁰

Siber güvenlik konusuyla ilgili olarak gündeme gelen diğer bir konu ise mahremiyet ihlalleridir. Tüm anayasal ve yasal düzenlemelere rağmen, diğer ülkelerde olduğu

⁸⁰ Bu çerçevede siber saldırılar sonucu MERNİS bilgilerine ulaşıldığı gibi MEB'nın 687 bin öğretmene ait kayıtların tutulduğu İl ve İlçe Milli Eğitim Müdürlükleri Yönetim Bilgi Sistemi'ne girilmiş ve öğretmenlerin isim, soyisim, T.C. kimlik no ve okul isimlerinin bulunduğu bilgiler ünlü paylaşım sitesi Rapidshare'de paylaşma açılmıştır. Benzer şekilde Sinan Berberoğlu liderliğindeki şebekenin, Türkiye genelinde tüm adli kayıtların tutulduğu UYAP sistemine defalarca giriş yaptığı tespit edilmiştir. Keza, Türkiye'de 2000 köle server bulunmaktadır (Alkan, 2012).

gibi ülkemizde de mahremiyet ihlalleri teknolojinin gelişmesi ve İnternetin kullanımının yaygınlaşmasına paralel olarak daha sık gündeme gelmeye başlamıştır. Nitekim, yapılan bir araştırma, görüşlerini İnternet ortamında paylaşmak konusunda Türkiye’deki kullanıcıların %46’sının güven sorunu yaşamadığını, %50’sinin ise bunu güvenli bulmadığını ortaya koymuştur. %31 ise, İnternetin en endişe verici tehlikesinin özel hayatın gizliliğini tehdit ediyor olması olduğunu söylemiştir. Bu oran, Avrupa’da ortaya çıkan rakamların çok çok üstündedir (BBC (08.03.2010b).

Zira, ülkemizde güvenlik gerekçesi ile gündelik yaşamın birçok alanı dijital olarak gözetlenmektedir. Şehirlerde kamusal alanları kuşatan MOBESE kameralar, vatandaşlık numarası ile yapılan işlemler, parmak izi ve iris tarama ile girip çıkılan iş yerleri, biyometrik bilgileri içeren kartların yaygınlaşması gibi uygulamalar düşünülecek olursa, Türkiye’de vatandaş olarak artık oldukça kapsamlı ve entegre bir elektronik veri tabanının içinde dijital bir özne haline geldiğimiz söylenebilir (Alternatif Bilişim Derneği, 2012b).

Benzer gözetleme ve denetim teknolojilerinin İnternet ortamında da kullanıldığı bilinmektedir. İnternet ortamında yapılan her işlemin dijital iz bıraktığı ve izlenebilir ve kaydedilebilir olduğu bilinmektedir. Bu durum, İnternette gerçekleştirilen her tür aktivitenin ve sosyalleşme faaliyetlerinin gerek her an, her yerde, her olan bitenden haberdar olmak isteyen devletler ve istihbarat örgütleri tarafından gerekse de reklam ve pazarlamaya, yani tükettirmeye endeksli ticari şirketler tarafından denetim ve ‘gözetim ağı’na evriltilmesi tehlikesini giderek güçlendirmektedir (Toprak, 2009:13).

3.1.2.3 İnternet Kafeler

TÜİK 2012 verilerine göre, İnternet kullanan bireylerin %16’sı erişimini İnternet kafelerden sağlamıştır. İnternet kafelerde İnternet kullanımı 2005’te %36,6, 2007’de %30,9, 2008’de %24,5, 2009’da 24,1, 2010’da %20, 2011’de %18,7 bulunmuştur (TÜİK, 2012). Yani, zaman içerisinde İnternet kafe kullanımının giderek azaldığı görülmektedir. Bunun yanında, ülkemizdeki 20.765 İnternet kafenin (BTK, 2013: 61) ekonomik büyüklüğü 1.2 milyon dolar olarak hesaplanmaktadır (İİKO, 2012).

Türkiye’de İnternet kafelerin halka açık olması, düşük maliyetli ve kolay ulaşılabilme özelliği; özellikle çocuklar ve gençler için İnternet açığının kapatılması, sayısal uçurumun azaltılması ve kullanımın yaygın hale gelmesine katkı sağlayabilir. Fakat, uygulamada bu mekanlar oyun ve eğlence, arkadaşlarla buluşma ve boş zaman geçirme yeri olarak algılanmakta ve kullanılmaktadır (Taşpınar ve Gümüş, 2003).

Nitekim, araştırmalar bu değerlendirmeleri doğrulamaktadır. Bir araştırmada, kullanıcıların %41,3’ü İnternetle ilk kez İnternet kafede tanıştığını belirtmiştir (Akyay,2004;7). Bir diğerinde, Türkiye’deki İnternet kullanıcısı çocukların %51’inin İnternet kafeleri kullandıkları tespit edilmiştir (EU Kids Online, 2010). Başka bir çalışmada ise, İnternet kafe kullanıcılarının %94,7 gibi büyük bir çoğunluğunun 30 yaş altından; bunların da %14,7’sinin 11-15 yaş grubu çocuklardan oluştuğu ortaya çıkmıştır (Yıldız, 2003: 3). Yine, diğer bir araştırmada, İnternet kafe müşterilerinin %84’ünün lise ve üniversite öğrencileri olduğu görülmüştür. Buna %8’lik ilköğretim öğrencilerini de eklersek oran %92’ye çıkmaktadır. Sivil vatandaşların İnternet kafe kullanımı ise %2 düzeyindedir (Doğu, 2012: 61).

Başka bir araştırmaya göre, erkek çocukların %76,7’si online oyunlara İnternet kafelerden katılmayı tercih etmektedir (Çağıltay vd., 2008: 2520-2529). Ankara’da yapılan bir çalışmada ise, İnternet kafelerin en önemli kullanıcılarının erkek öğrencilerden oluşan çocuklar ve gençler olduğu ve yoğun olarak oyun oynamak ya da sohbet hizmetlerinden yararlanmak amaçlı kullanıldığı sonucuna ulaşılmıştır (Binark ve Sütçü, 2008b).

MEB’nın yapmış olduğu bir çalışmaya göre, öğrencilerin %51,3’ü İnternet kafede 1 saatten az, %42,8’i ise 1-2 saat kaldıklarını ifade etmişlerdir. İnternet kafeye ne zaman gittikleri sorulduğunda %58,1’i hafta sonlarında, %33,9’u okul çıkışında, %9,1’i ise akşam saatlerinde gittiklerini belirtmişlerdir (MEB, 2008: 55-70). Diğer bir araştırmada da İnternet kafelere gelen kullanıcıların %92’sinin 0-2 saat arasında, %7’sinin 2-5 saat arasında ve %1’inin 5 saat üzerinde İnternet kullandığı belirlenmiştir (Doğu, 2012: 61, 63).

İnternet kafelerin yanlış amaçlarla ve bilinçsizce kullanılması özellikle çocukları çeşitli tehlikelere maruz bırakabilmektedir. Bunlar, müstehcenlik, çocuk istismarı, şiddet ve nefret, kumar ve uyuşturucuyu teşvik, siber zorbalık gibi yasadışı ve zararlı İnternet içerikleri olabileceği gibi, bilişim suçları mağduriyeti, yanlış kişilerle arkadaşlık kurma veya zararlı oyunlar ve kontrolsüz İnternet kullanımı ve bağımlılık türü olumsuzluklar da olabilmektedir (Yıldız ve Bölükbaş, 2005).

Buraya kadar değinilen konularda görüldüğü ve tezin onüçüncü alt hipotezinde öngördüğümüz gibi, ülkemiz açısından İnternetin özellikle çocuklar ve gençler üzerinde olmak üzere aile ve toplum için oluşturduğu bir takım riskler ve tehditler bulunmaktadır. Bu riskler ve tehditlerin gerçek boyutları ile ortaya konulması gerekmektedir. Zira İnternetin ülkemiz için oluşturduğu risklerin boyutuna ilişkin elimizde yeterli bilimsel veriler bulunmamaktadır. Ülke genelinde bilişim teknolojileri ve özellikle İnternet kullanımına, bunların etkilerine ve sonuçlarına, bu nedenle oluşan sosyal risklere ve tehditlere ilişkin geniş ve derinlikli alan araştırmalarına ihtiyaç vardır. Bu tür araştırmaların hem zamanla tekrar edilmesi hem de etkin kullanıcıya odaklanan çalışmaların çeşitlendirilmesi gerekmektedir.

3.2 TÜRKİYE’DE İNTERNET İÇERİK DÜZENLEMESİNİN TARİHÇESİ

İnternet içerik düzenlemelerinin bugününü daha iyi anlayabilmek için tarihsel bir perspektife ihtiyaç vardır. Bu nedenle, müstakilen içerik düzenlemesi için çıkarılan 5651 sayılı Yasa’nın öncesinde İnternet konusunda yapılan bilgi toplumu çalışmaları, yasal düzenlemeler, kurumsal yapılar ve uygulamalar, erişim engellemeleri, bu Yasa öncesinde ve yasalaşma sürecinde yaşanan tartışmalar bu çerçevede incelenecektir.

3.2.1 5651 Sayılı Kanun Öncesi

1993 yılında Türkiye’de kullanılmaya başlayan İnternete 2001 yılına kadar önemli bir müdahalede bulunulmamıştır (Akdeniz ve Altıparmak, 2008: 4). Ancak, zaman içinde günlük hayatta ve çalışma hayatında bilgisayar ve İnternet kullanımının yaygınlaşmasıyla, bilgisayarların ve İnternetin suçta araç olarak kullanılmasına

ilişkin olaylar yaşanmaya başlamıştır. Bu tür olayların nitelik ve nicelik olarak suç olgusunda değişikliğe neden olması, bu alanın bir takım yeni hukuki düzenlemelerle disipline edilmesi ihtiyacını ortaya çıkarmıştır. Bu ihtiyaçlar doğrultusunda, İnternet yoluyla oluşan sorunların çözümü için zaman içinde farklı yasal düzenlemeler, kurumsal yapılar ve uygulamalar gündeme gelmiştir. Tüm bu gelişmelerin arka planında dikkate alınması gereken diğer bir mecra da bilgi toplumu çalışmaları ve “e-dönüşüm Türkiye Projesi”dir.

3.2.1.1 Yasal Düzenlemeler

Türkiye’de İnternetin yaygınlaşması ile beliren ihtiyaçların ve oluşan sorunların karşılanması amacıyla başlangıçta mevcut kanunlara çeşitli eklemeler yapılması yolu tercih edilmiştir. İlerleyen zamanlarda konuyla ilgili müstakil yasalar çıkarılması gündeme gelmiştir. İlk olarak, 14.6.1991 tarihinde yürürlükte bulunan Türk Ceza Kanunu (TCK)’na “Bilişim Alanında Suçlar” başlıklı eklenen 525/a,b,c,d maddeleri ile; otomatik işleme tabi tutulmuş sistemden, program, veri ve diğer unsurların ele geçirilmesi, çoğaltılması ve bozulması gibi suçlar düzenlemiştir. Ancak, İnternette işlenen suçlarla ilgili herhangi bir düzenleme yapılmamıştır (Çağlar, 2011:37).

İkinci olarak, 12.6.1995 tarihinde 5846 Sayılı Fikir ve Sanat Eserleri Kanunu (FSEK)’nin 2. maddesinde değişiklik yapılarak, bilgisayar programları da eser olarak kabul edilmiştir. Sonrasında, 3.3.2001 tarihinde FSEK’na Ek 4. maddeyle eser sahipleri ile bağlantılı hak sahiplerinin bu Kanun’da tanınmış haklarının ihlali halinde, başvuruları üzerine servis ve içerik sağlayıcıları tarafından ihlale konu eserlerin içerikten çıkartılması gerektiği yönünde düzenleme yapılmıştır.

21.05.2002 tarihinde, 5680 Sayılı Basın Kanunu’na Ek 9. madde ilave edilerek; yalan haber, hakaret ve benzeri fiillerden doğacak maddi ve manevi zararlarla ilgili hükümleri, bilişim teknolojileri ve İnternet ortamında sayfa açılması veya e-gazete, e-bülten vb. ile yayınlanan her türlü yazı, resim, işaret, sesli veya sessiz görüntü ve benzerleri hakkında da uygulanacağını düzenlemiştir. Böylece, İnternet yayınları da Basın Kanunu kapsamında değerlendirilmeye başlanmıştır.

Fakat, İnternet yayınlarının tek başına Basın Kanunu kapsamında değerlendirilerek sorunların çözülemeye çalışılmasının yeni bir takım sorunlara neden olacağı muhtemeldi. Çünkü “İnternet ortamındaki yayın” kavramı ile Basın Kanunu’nda yer alan “yayın” kavramı birbiriyle örtüşmemekte; İnternet kendisinden önceki kitle iletişim araçlarına benzememekteydi. Zira, İnternetin basılı bir eser olmadığına görülmesi gerekmektedir. Ayrıca, İnternet yayınlarında süreli ve süresiz yayın ayırımı olmaması ve Cumhuriyet Savcılığı’na suretlerinin gönderilememesi de diğer bir sorun kaynağıydı (Günaydın, 2010: 98-99).⁸¹

Nitekim bu ve benzeri nedenlerle aynı yasal değişiklik kapsamı içinde İnternetle ilgili sorunu çözmek üzere RTÜK’nun yetkili kılınmasına karar verilmiştir. Buna göre, 4756 sayılı Kanun ile 3984 Sayılı “Radyo ve Televizyonların Kuruluş ve Yayınları Hakkında Kanun”un 31. maddesinde değişiklik yapılarak; her türlü teknoloji ile ve her tür iletişim ortamında yapılacak yayın ve hizmetlerin usul ve esaslarının, Haberleşme Yüksek Kurulu’nun belirleyeceği strateji çerçevesinde Üst Kurul’ca tespit edilip, Kurul’un onayına sunulacağı ve bu yayın ve hizmetlerin mevzuata uygunluğunun Üst Kurul’ca denetleneceği hükmü getirilmiştir.

Fakat, değişiklikte geçen “Her türlü teknoloji ile ve her tür iletişim ortamında yapılacak yayın ve hizmetler” ifadesi tartışmalara yol açmıştır. Zira, geniş olarak yorumlandığında servis ve içerik sağlayıcıların verdikleri hizmetler ile bireysel iletişim yolları olan mailer ve tüm web sayfalarının da bu kapsama girmesi olasılığı ortaya çıkmıştır. Bu durum, İnternete müdahale yolununun açılmış olduğu değerlendirmesine neden olmuştur (Günaydın, 2010: 101; Öngören, 2006: 26). Bu kabul edilmese bile, en azından İnternet ortamında verilen/verilecek “radyo ve televizyon yayın ve hizmetleri” bu düzenlemeyle RTÜK denetimine girmiş sayılabilecekti (Pekşirin, 2001).

⁸¹ “İnternet ortamındaki yayın” kavramı ile Basın Kanunu’nda yer alan “yayın” kavramı arasındaki farka dikkat çeken bir yazı için bkz. Fikret İlkiz, “**3894 Sayılı Radyo ve Televizyon Kanunları Kuruluş ve Yayınları Hakkında Yasa Tasarısı ve Basın Yasası Değişiklikleri ile İnternet Yayıncılığı Düzenlemesinin Yaratacağı Sorunlar**”, <http://kurul.ubak.gov.tr/m06.php> (17.12.2012)

Bu gelişmeler İnternetle ilgili bazı STK'larınca tepki ile karşılanmış ve tepkilerini söz konusu düzenlemelere karşı ortak bir bildiri yayınlarak göstermişlerdir.⁸² Düzenleme ilginç bir durumun da yaşanmasına neden olmuştur. Zira, devlet tarafından kurulmuş olan İnternet Kurulu'nun üyeleri de bu yasal düzenlemeye karşı olduklarını bir deklarasyon ile duyurmuşlardır (İnternet Kurulu, 2001b).

Bu tepki ve eleştirilerin sadece İnternetle ilgili denetimin RTÜK'e verilmesi ihtimaline karşı olmadığı, İnterneti disiplin altına almaya yönelik her tür düzenleme girişimine karşı olunduğu dikkat çekmektedir. Nitekim bu Yasa kapsamında, gerçek dışı haberlerle hakareti önlemeye matuf olarak yapılan değişikliklerle yalan beyan, hakaret ve benzeri eylemlerden doğan maddi ve manevi tazminat davalarıyla ilgili hükümlerin İnternet'e de uygulanabilecek hale getirilmesi⁸³ dahi eleştiri konusu yapılmıştır. Eleştirilerin gerekçesi ise, bu düzenlemenin asıl amacının, TBMM üyeleri hakkında yapılan eleştirileri, siyasi demeçleri ve muhalefeti susturmak olduğu yönündeki kuşkulardır (Cyber-rights.org, 2002).

Neyse ki, uygulamada 3984 sayılı Yasa'nın 1. maddesinin açıkça RTÜK'nun yetkisini radyo ve televizyon yayınlarının düzenlenmesi ile sınırlı tutmasından dolayı, RTÜK İnternet içeriğine müdahaleyi gündemine almamış; sadece, İnternet yolu ile yapılan radyo ve televizyon yayınlarını görevi kapsamında görmüştür (Öngören, 2006: 26-27).

⁸² Bildiride, İnterneti geleneksel basın-yayın veya medyalarla aynı kategoride değerlendirmenin yanlışlığına; İnternetin birçok boyutu ile hayatın içinde olduğuna, basın ve medya uzantısı olmasının bunlardan sadece bir tanesi olduğuna; İnternetin aynı zamanda bir banka, bir dükkan, bir işyeri, bir kütüphane, bir iletişim aracı veya bunların bir uzantısı olduğuna; bu anlamda kamuya açık bir sosyal ortam olduğuna değinilmektedir. Dolayısı ile, "İnterneti yalnızca en son medya icadı olarak görmenin bu teknolojinin doğası hakkında önemli bir yanılgıya işaret etmektedir" denilmektedir. Bu argumanlardan hareketle asıl olarak, söz konusu Yasa'nın İnterneti kısıtladığı ve yok edeceği görüşüne yer verilmektedir (İnternet Kurulu, 2001a).

⁸³ Genel Kurul'da Hükümet'ten DSP Grubu adına konuşan Emrehan Halıcı düzenlemenin gerekçesini şöyle açıklamaktadır: "Bu yasa Meclisimize ilk geldiği zaman, üzerinde görüştüğümüz madde, Basın Kanunu'nun bütün hükümlerini İnternet için de geçerli kılıyor idi. Ancak, hem kamuoyundan hem de konuyla ilgili kişi ve kurumlardan tepkiler geldi. Biz de bu tepkileri haklı bulduk ve kayıtsız kalmayarak, bir önerge hazırladık ve kuşku duyulan noktaları tamamen ortadan kaldırdık. Maddenin şu anki haliyle, sadece ve sadece Basın Yasası'nın yalan haber, hakaret ve benzeri fiillerden doğacak olan maddî ve manevî zararlarla ilgili hükümleri İnternet için geçerli kılınmaktadır; başka bir hükmü geçerli değildir. Dolayısıyla, yalan haber ve hakarete geçit vermeyen İnternet yayıncılarının bu yasadaki herhangi bir şekilde kuşku duymalarına kesinlikle gerek yoktur. Hiçbir arkadaşımızın da - tahmin etmiyorum ki- yalan haberi ve hakareti burada desteklemesi mümkün değildir." (TBMM, 2002)

12.10.2004 tarihinde 5237 sayılı TCK ile bilişim suçları yeniden ve daha ayrıntılı düzenlenmiştir. Buna göre, Kanun'nun 9. bölümünde “kişisel verilerin kaydedilmesi suçu”, “kişisel verileri hukuka aykırı olarak verme veya ele geçirme suçu”; 10. bölümünde "Bilişim Alanında Suçlar" başlığı altında "bilişim sistemine girme", "sistemi engelleme, bozma, verileri yok etme veya değiştirme", "banka veya kredi kartlarının kötüye kullanılması", "tüzel kişiler hakkında güvenlik tedbiri uygulanması" başlıklı maddelere yer verilmiştir. Ayrıca "nitelikli hırsızlık", "nitelikli dolandırıcılık" maddelerinde yer alan suçların bilişim sistemleri aracılığıyla işlenmesini ağırlaştırıcı neden olarak hükme bağlamıştır.

Ülkemizde bilişim ve İnternet hukuku boyutu ile ilgili diğer bir düzenleme de 4077 sayılı “Tüketicinin Korunması Hakkında Kanun” da değişiklik yapan 23.02.2003 tarihli ve 4822 sayılı Kanun’dur. Bu düzenlemenin 3. maddesiyle mal; “elektronik ortamda kullanılmak üzere hazırlanan yazılım, ses, görüntü ve benzeri gayri maddi malları”da içerecek şekilde tanımlanmış, 9. maddesiyle de mesafeli sözleşmelerin “...görsel, telefon ve elektronik ortamda veya diğer iletişim araçları kullanılarak” gerçekleştirilebileceği, elektronik ortamda yapılan sözleşmelerin teyit işlemlerinin yine elektronik ortamda yapılabileceği hüküm altına alınmıştır.

3.2.1.2 Kurumsal Yapılar

1987 tarihli ve 3348 Sayılı “Ulaştırma Bakanlığı’nın Teşkilat ve Görevleri Hakkında Kanun” gereğince Türkiye’de İnternetten genel anlamda sorumlu Bakanlık, Ulaştırma Bakanlığı’dır. Kanun’la Bakanlığın konuyla ilgili ana hizmet birimi Haberleşme Genel Müdürlüğü olarak belirlenmiştir. Daha sonra 1998 yılında İSS’lar ve Türkiye Bilişim Derneği (TBD)’nin fikri desteği ile özel sektör, üniversiteler, meslek örgütleri, STK’ları ile kamu kesiminden üyelerin katılımıyla Ulaştırma Bakanlığı’na bağlı olarak İnternet Kurulu oluşturulmuştur. Kurulu’n, ana işlevi Bakanlığa İnternet konusunda danışmanlık hizmeti sunmaktı (Akgül, 2001).

İnternetle doğrudan ilgili kurumsal yapı oluşturulması anlamında ilk önemli yasal düzenleme ise 2000 yılında çıkarılan 4502 sayılı Kanun’dur. Bu Kanun’un 22.

maddesi ile İnternet Kurulu'na yasal bir dayanak oluşturulurken,⁸⁴ asıl önemlisi, 2813 sayılı Telsiz Kanunu'nda değişiklik yapılarak Telekomünikasyon Kurumu (TK) kurulmuştur. TK, telekomünikasyon sektörü ile ilgili yetkilendirme, denetleme, teknik düzenlemeye ilişkin görevleri yerine getirmek ve sektördeki serbest rekabeti sağlamak üzere oluşturulmuş, idari ve mali özerkliğe sahip özel bütçeli bağımsız bir kuruluştur ve Ulaştırma Bakanlığı ile ilişkilidir. Böylece TK, izin ve ruhsat, denetim ve düzenleme konularındaki yetkileri nedeniyle İSS'lar ve erişim sağlayıcılar açısından en önemli kuruluş olmuştur (Öngören, 2006: 12).

TK'nun kurulması, IMF ve Dünya Bankası'nın zorlamasıyla o dönem tüm dünyada revaçta olan deregülasyon, özelleştirme ve sektörlerin tam reketbetçi hale getirilmesi için bağımsız üst kurullarca yönetilmesi politikalarının ülkemizdeki uygulamalarından birisidir. Nitekim, Türkiye'de telekomünikasyon sektörünün serbestleşmesine ilişkin faaliyetler 2000 yılında TK'nun kurulması ile hızlanmış ve 2004 yılı başı itibarıyla sektör rekabete açılırken, Türk Telekom A.Ş.'nin %55 hissesi 2005 yılı içerisinde blok satış yoluyla özelleştirilmiştir (DPT, 2006: 13).

TK'nun görevleri genel olarak 4502 sayılı Kanun'da sayılmakla beraber, 15.09.2000 tarihli "Telekomünikasyon Kurumunun Teşkilat ve Görevleri ile Çalışma Esas ve Usulleri Hakkında Yönetmelik" ve 26.08.2004 tarihli "Telekomünikasyon Hizmet ve Altyapılarına İlişkin Yetkilendirme Yönetmeliği" görevleri detaylandırmıştır.

Özellikle 2004 tarihli yönetmelik İnternet için önemlidir. Çünkü, bu yönetmelikte diğer telekomünikasyon hizmetleri ile birlikte "Kablolu Ve Kablosuz İnternet Servis Sağlayıcılığı Hizmeti" de düzenlenmiştir. Yönetmeliğin muhtelif yerlerinde İSS'lara ilişkin yükümlülükler bulunmaktadır. Ancak, Ek-A6'da yer alan düzenleme konumuz açısından önemlidir. Buna göre İSS'lar, kullanıcılarının İnternet üzerindeki yetkisiz ve rahatsız edici girişimlerine meydan verilmemesi yanında, vereceği

⁸⁴ "Madde 22 – 9.4.1987 tarihli ve 3348 sayılı Ulaştırma Bakanlığının Teşkilat ve Görevleri Hakkında Kanuna aşağıdaki ek madde eklenmiştir.

EK MADDE 1. – Bakanlık, teknolojinin getirdiği yeni ulaştırma ve haberleşme hizmetleri ile ilgili olarak oluşturulacak politikaların tespitinde Bakanlık dışından tecrübeli ve yetişkin kişi ve kuruluş temsilcilerinin katıldığı geçici danışma kurulları kurabilir. Bu kurul üyelerinin yol ve konaklama giderleri ile birlikte kurulun diğer faaliyet giderleri Ulaştırma Bakanlığı bütçesinden karşılanır."

hizmete ve sisteminde kullanılacak cihazlara, yetkisiz kişilerin erişimi ve bozucu/değiřtirici müdahalelerini önlemek amacıyla gerekli tedbirleri almakla da yükümlü kılınmıştır. Ayrıca, işletmecilere, her bir kullanıcı için, kullanıcı tarafından sisteme baęlı kalınan süre, trafik miktarı ve trafik yolu bilgilerini en az 6 altı ay süreyle muhafaza etme yükümlülüęü getirilmiştir.

Daha sonra çıkarılan 05.09.2004 tarihli “Telekomünikasyon Kurumu Tarafından İşletmecilere Uygulanacak İdari Para Cezaları İle Dięer Müeyyide ve Tedbirler Hakkında Yönetmelięi” de İSS’lara ilişkin bazı düzenlemeler ihtiva etmektedir. Yönetmelik, bir önceki takvim yılındaki cirosunun %3’üne kadar idari para cezası uygulanacak haller içerisinde İSS’ların haberleşmenin gizlilięine, milli güvenlik ve kamu düzenine zarar verici davranışta bulunması hususunu da saymıştır. Ayrıca, Yönetmelikle “milli güvenliğe aykırı” ve “kamu düzenine aykırı” fiillerin devam etmesi durumunda işletmecinin yetki belgesinin feshine/iptaline kadar giden müeyyideler belirlenmiştir.

Bu kapsamda Yönetmelikte yer alan dięer bir düzenleme de, kamu güvenlik ve istihbarat kurumlarının özel mevzuatları gereęi işletmeciden talep ettięi hususların işletmeciler tarafından yerine getirilmesini öngören yükümlülüktür. Buna göre, yükümlülük yerine getirilmez ise işletmecinin bir önceki takvim yılına ait cirosunun %3’üne kadar idari para cezası uygulanacaktır.

İnterneti, telefon şirketlerini ve dolayısıyla TK’nu ilgilendiren en önemli yasal düzenlemelerden birisi de 2005 tarihli ve 5369 Sayılı “Evrensel Hizmetin Sağlanması Hakkındaki Kanun”dur. Kanun coęrafi konumlarından bağımsız olarak Türkiye Cumhuriyeti sınırları içinde herkes tarafından erişilebilir, önceden belirlenmiş kalitede ve herkesin karşılayabileceęi makul bir bedel karşılığında asgari standartlarda sunulacak olan, İnternet erişimi de dahil elektronik haberleşme hizmetlerini, “evrensel hizmet” olarak tanımlamış ve işletmecilerin, bu Kanun’da belirlenen evrensel hizmeti sağlamakla yükümlü olduęunu düzenlemiştir. Yasa’nın 5. maddesine göre evrensel hizmetin kapsamına temel İnternet hizmetleri de dahildir.

3.2.1.3 Bilgi Toplumu Çalışmaları ve e-Dönüşüm Türkiye Projesi

Türkiye’de 5651 Sayılı Yasa öncesinde İnternetin düzenlenmesi konusuyla ilgili yürütülen çalışmaların diğer bir mecrası ise “bilgi toplumu” çalışmalarıdır. 1990’lı yılların ikinci yarısından itibaren tüm dünyada olduğu gibi Türkiye’de de bilgi toplumu olma yönünde çabaların arttığı, bu amaçla bir takım rapor ve araştırmaların yanı sıra bilgi toplumunun belli unsurlarının koordinasyonuna yönelik çalışmalar yapıldığı görülmektedir. Fakat, ekonomik ve siyasi istikrarsızlık nedeniyle kapsamlı bir yaklaşımla takip edilemeyen bilgi toplumuna yönelik çalışmalar, 2003 yılında ilan edilen e-Dönüşüm Türkiye Projesi ile belirli bir bütünlüğe kavuşturulmuş ve bu alandaki çalışmalara ivme kazandırılmıştır (Bilgitoplumu, 2013a).

27 Şubat 2003 tarihli Başbakanlık Genelgesi ile e-Dönüşüm Türkiye Projesi’nin amaçları, kurumsal yapısı ve uygulama esasları belirlenmiştir. Buna göre Proje’nin koordinasyonu ile Devlet Planlama Teşkilatı Müsteşarlığı (DPT) görevlendirilmiş ve Müsteşarlık bünyesinde Projesi’nin koordinasyonunu yürütmek, kamu kurumlarının bilgi ve iletişim teknolojisi yatırımları arasında eşgüdüm sağlamak ve bilgi toplumu olma yolunda atılması gereken adımlara ilişkin stratejileri belirlemek üzere 2003 yılı Mart ayında Bilgi Toplumu Dairesi (BTD) kurulmuştur. Ayrıca, Proje’nin üst seviyede yönlendirilmesi ve izlenmesi amacıyla ilgili müsteşar yardımcıları ve STK’ların başkanlarından oluşan bir “Danışma Kurulu” oluşturulmuştur.

Genelge’ye göre, e-Dönüşüm Türkiye Projesi’nin başlıca hedefi vatandaşlara daha kaliteli ve hızlı kamu hizmeti sunabilmek amacıyla; katılımcı, şeffaf, etkin ve basit iş süreçlerine sahip olmayı ilke edinmiş bir devlet yapısı oluşturacak koşulların hazırlanmasıdır. Proje’nin “genel olarak demokratikleşme, özel olarak ise kamu yönetimi reformu” bağlamında ele alındığı görülmektedir.

3.2.1.3.1 Kısa Dönem Eylem Planı (2003-2004)

Genelge’de öngörüldüğü gibi, E-Dönüşüm Türkiye Projesi kapsamında ilk olarak çalışma gruplarıyla 2003 yılının Aralık ayına kadar “Kısa Dönem Eylem Planı” hazırlanmıştır. 4 Aralık 2003 tarihli Başbakanlık Genelgesi’yle bu Plan deklare

edilerek uygulamaya konulurken, Proje'nin hayata geçirilmesini sağlamak üzere “e-Dönüşüm Türkiye İcra Kurulu” da oluşturulmuştur (DPT, 2003).⁸⁵

73 eylemden oluşan Plan'da İnternetin düzenlemesine yönelik bazı eylemler de bulunmaktadır. Doğrudan içerik düzenlemesinden bahsedilen 23. Eylemde, “İnternet üzerinde erişim, uygulama, içerik, güvenlik vb. bilgi toplumu hizmetlerini sağlayanların görev, yetki ve sorumlulukları ile denetimlerinin nasıl yapılacağına ilişkin yasa tasarısı taslağı hazırlanması” amacı dile getirilmekte ve bu kapsamda İSS'lara yönelik bir yasal düzenleme yapılması öngörülmektedir (DPT, 2003).

Plan'nda e-devlet uygulamalarının artırılmasına yönelik bazı eylemler yanında, “kolay erişilebilir, daha ucuz, daha hızlı, sürekli ve güvenli İnternet olanağının sağlanması amacıyla düzenlemeler yapılması”, “elektronik imza”, “kişisel verilerin korunması”, “ulusal bilgi güvenliği” kanunlarının çıkartılması, “bilgi ve bilgi teknolojileri alanına özgü suç ve cezaların belirlenmesi için gerekli yasa çalışmalarının yapılması”, “elektronik ortamdaki sözleşmelerin tanınması için yasal düzenlemelerin tamamlanması”, “elektronik ortamda fıkri hakların korunması için yasal çalışmaların yapılması”, “e-ticaretle ilgili mevzuatın hazırlanması”, “telekomünikasyon alanında ikincil düzenlemelerin yapılması”, “evrensel hizmet yönetmeliğinin çıkartılması” gibi İnternetin doğrudan veya dolaylı olarak düzenlenmesini ilgilendiren birçok eyleme de yer verilmiştir (DPT, 2003).

3.2.1.3.2 “Bilgi Toplumuna Dönüşüm Politikası” Belgesi

Kısa Dönem Eylem Planı uygulanırken e-Dönüşüm Türkiye İcra Kurulu, kamu kurum ve kuruluşları ile ilgili STK'ların ortak çalışması ve e-Dönüşüm Türkiye Projesi Danışma Kurulu'nun katkılarıyla hazırlanan “Bilgi Toplumuna Dönüşüm Politikası” belgesini 10 Haziran 2004 tarihinde kabul etmiştir (Bilgitoplumu, 2004).

⁸⁵ İcra Kurulu, bir Başbakan Yardımcısı'nın başkanlığında, Sanayi ve Ticaret Bakanı, Ulaştırma Bakanı, DPT Müsteşarı ve Başbakanlık Başmüşaviri'nden oluşmaktadır. Kurul toplantılarına, Danışma Kurulu Başkanı sıfatıyla DPT Müsteşar Yardımcısı, TÜBİTAK ve TK Başkanı ve Türk Telekom Genel Müdürü ile TOBB, Türkiye Bilişim Vakfı (TBV), TBD ve Türkiye Bilişim Sanayicileri ve İşadamları Derneği (TÜBİSAD) başkanları da katılacaklardır.

Belge’de, Türkiye’nin bilgi toplumuna dönüşümdeki vizyonu, “bilim ve teknoloji üretiminde odak noktası haline gelmiş, bilgi ve teknolojiyi etkin bir araç olarak kullanan, bilgiye dayalı karar alma süreçleriyle daha fazla değer üreten, küresel rekabette başarılı ve refah düzeyi yüksek bir ülke olmak” olduğu belirtilmektedir. Belgeye göre, bu vizyonu gerçekleştirecek amaç ve esaslardan birisi de rekabetçi bilgi ve iletişim teknolojileri piyasasının oluşumudur (Bilgitoplumu, 2004: 1, 4-6).

Belge, belirlenen bu amaçlara ulaşması için iş ortamı ve girişimcilik, ar-ge, yenilikçilik ve sanayi politikaları, bilgi ve iletişim teknolojileri, sosyal dönüşüm ve etkin kamu yönetimi temel politikaları çerçevesinde ihtiyaç duyulan hukuki, teknik ve ekonomik düzenlemeler yapılmasını öngörmektedir (Bilgitoplumu, 2004: 2-4). Belge’de tüm bu amaç ve temel politikaların hayata geçirilmesi de dahil, Türkiye’nin e-Dönüşümüne ilişkin tüm çalışmaların e-Dönüşüm Türkiye Projesi kapsamında yürütüleceği ve bu çalışmaların iyi bir yönetim modeli oluşturularak, ilgili tüm kesimlerin karar alma süreçlerine etkin katılımının sağlanmasıyla gerçekleştirileceği vurgulanmaktadır (Bilgitoplumu, 2004: 7-8).

Görüldüğü gibi “Bilgi Toplumuna Dönüşüm Politikası” belgesi daha çok ekonomik kalkınmışlık, teknolojinin yaygınlaştırılması ve e-devlet uygulamaları ile devletin dönüştürülmesi gibi konuları merkeze almaktadır. İnternetin taşıdığı potansiyel sorunlara sadece bilişim suçları boyutuyla değinilmekte; yasadışı ve zararlı içerikler ve bunlarla mücadele, sosyal maliyetleri gibi hususlar söz konusu edilmemektedir.

3.2.1.3.3 Eylem Planı (2005)

Kısa Dönem Eylem Planı’nın süresi dolduktan sonra, İcra Kurulu’nun kararı ve çalışma gruplarının katılımı ile, orta vadeli “Bilgi Toplumu Stratejisi”nin hazırlanmasına kadar uygulanmak üzere bir yıl süreli 2005 Eylem Planı hazırlanmış ve uygulanmıştır (Bilgitoplumu, 2013b). Yüksek Planlama Kurulu’nun 24.03.2005 tarihli ve 2005/5 Sayılı Kararı ile yürürlüğe giren e-Dönüşüm Türkiye Projesi 2005 Yılı Eylem Planı, 50 eylemden oluşmaktadır (DPT, 2005).

2003-2004 Kısa Dönem Eylem Plan'ından farklı olarak, 2005 Yılı Eylem Planı'nda güvenli İnternet kullanımı konusuna yer verilmiştir. Buna göre, 17. eylem “Güvenli İnternet kullanımı konusunda toplumda farkındalık yaratılması”dır. Eylemin amaç/açıklama kısmında İnternetin güvenli kullanımının yaygınlaştırılması amacıyla bilgilendirme ve bilinçlendirme çalışmalarının yapılacağı belirtilmiştir (DPT, 2005). Böylece güvenli İnternet konusu ilk defa bilgi toplumu belgelerine girmiştir .

Bunun dışında 2005 Yılı Eylem Planı'nda İnternetin düzenlenmesi kapsamında değerlendirilebilecek bazı başka eylemlere de rastlanılmaktadır. Bu çerçevede, Plan'ın 18. eylemde bilişim suçları kanunun çıkartılması, 19. eylemde istenmeyen elektronik iletişim (e-posta, sms vb.) ile mücadele, 5. eylemde kamu kurumları bilgi güvenliği risk analizinin yapılması konularına yer verilmiştir (DPT, 2005).

3.2.1.3.4 Bilgi Toplumu Stratejisi (2006-2010)

2005 Eylem Planı'ndan sonra Bilgi Toplumu Stratejisi ve Eylem Planı hazırlanarak e-Dönüşüm Türkiye İcra Kurulu'na kabul edildikten sonra 2006-2010 döneminde uygulanmak üzere 2006 yılı Temmuz ayında 2006/38 sayılı Yüksek Planlama Kurulu kararı ile yürürlüğe konulmuştur (DPT, 2006a).

Türkiye'nin bilgi ve iletişim teknolojilerinden etkin olarak yararlanması ve bilgi toplumuna dönüşümün gerçekleştirilmesine yönelik olarak orta vadeli strateji ve hedefleri belirlemek üzere hazırlanan Bilgi Toplumu Stratejisi ve eki Eylem Planı'nında; söz konusu belgelerin vatandaşlar, kamu kesimi ve iş dünyası ile STK'ları, kısacası toplumun her kesimi için önümüzdeki 5 yıllık dönemde temel referans belgesi olacağı belirtilmiştir (DPT, 2006a: 2).

Bilgi Toplumu Strateji belgesini konumuz açısından incelersek, en başta vatandaşların bilgi ve iletişim teknolojilerinin ve özellikle bilgisayar ve İnternet kullanımının yaygınlaştırılması, erişim imkanlarının sağlanması ve bu teknolojileri kullanma yeteneğinin kazandırılmasının gereği üzerinde durulduğunu görmekteyiz (DPT, 2006a: 2). Bu çerçevede, yetersiz ve etkinlikten uzak İnternet kullanımı ile ulusal ve uluslararası ölçekte var olan sayısal uçurum sorununun giderilmesine

odaklanılmıştır. Genç nüfus avantajından yararlanılması ve bunları bilgi toplumunun birer ferdi haline getirmesinin öneminden bahsedilmektedir (DPT, 2006a: 7-8).

Belge’de Türkiye’nin bütüncül bir dönüşüm stratejisi izlemesi gerektiğine dikkat çekilirken (DPT, 2006: 9) genel anlamda İnternet içerik düzenlemesini ilgilendiren konuların stratejik önceliklerden “sosyal dönüşüm” başlığı altında yer aldığı görülmektedir. Türkiye’nin bu sosyal dönüşüm sürecinde, “etkin kullanım odaklı” stratejiyi benimsediği belirtilmektedir (DPT, 2006a: 22). “Sosyal dönüşüm” başlığı altında sayısal uçurumun azaltılacağı, İnternet kullanım oranlarının ülke genelinde artırılacağı dile getirilmektedir. Bu amaçla, imkanları kısıtlı olan vatandaşların erişimini sağlamak üzere oluşturulacak kamu İnternet erişim merkezleri (KİEM) kurulacağı; bu mekanlarda vatandaşlara bilgisayar ve İnternet kullanımı konusunda rehberlik ve eğitim hizmetlerinin de verileceği belirtilmektedir (DPT, 2006a: 22).

Belge’de İnternetin düzenlenmesini ilgilendiren konular, bu sosyal dönüşümün hayata geçirilmesinin önündeki engellerin kaldırılması hedefi kapsamında gündeme gelmektedir. Buna göre, bireylerin bu teknolojileri kullanmalarına önemli bir engel teşkil eden güvenlik endişesinin giderilmesi ve güvenli bir İnternet ortamının oluşturulması için gerekli tedbirlerin alınarak kullanımın artırılması yönünde motivasyonun sağlanacağı dile getirilmektedir. Bu çerçevede, gerekli yasal düzenlemelerin yapılacağı belirtilmektedir (DPT, 2006a: 23, 25).

Belge’de aynı konuya stratejik önceliklerden “Kamu yönetiminde modernizasyon” başlığı altında tekrar değinilmektedir. Burada “Hedefler” bahsinde yer alan “Güvenlik ve Kişisel Bilgilerin Mahremiyeti” yan başlığında ülke genelinde ve kamu kurumlarında bilgi sistemleri ile elektronik iletişim ve ağ bağlantılarında güvenliğin ve bilgi güvenliğinin sağlanması ve sürdürülmesi için gerekli organizasyonel ve yasal düzenlemelerin yapılacağı belirtilmektedir (DPT, 2006a: 36). Keza, e-Devlet hizmetlerinin sunumunda, kişisel bilgilerin mahremiyetine saygı gösterileceği ve bu amaçla, kişisel verilerin korunmasına ilişkin yasal düzenleme yapılacağı dile getirilmektedir (DPT, 2006a: 36).

Son olarak, Strateji Belgesi'nin uygulanmasında hedeflere ulaşabilmesi için kamu kurum ve kuruluşları, iş dünyası, STK'ları başta olmak üzere toplumun tüm kesimlerinin Belgeyi benimseyerek ortak hedefler doğrultusunda uyumlu bir biçimde hareket etmelerinin önemi vurgulanmaktadır. Paydaşların sorumluluk/yetki/rollerinin iyi yönetim ilkeleri çerçevesinde tanımlanarak, çalışmaların aktif işbirliği ve etkileşim içinde yürütülmesinin gerekliliği üzerinde durulmaktadır (DPT, 2006a: 44).

Bilgi Toplumu Strateji'nin hayata geçirilmesinde üç kurultan bahsedilmektedir. Bunlardan birincisi olan, e-Dönüşüm Türkiye İcra Kurulu; Strateji'nin uygulanması sürecinde en üst düzeyde politika belirleme ve karar alma, değerlendirme ve yönlendirme organı olarak görev yapacak ve Kurul, bu işlevleri etkin olarak yerine getirmek üzere yeniden yapılandırılacaktır (DPT, 2006a: 44).

İkincisi, “Dönüşüm Liderleri Kurulu”dur ki; tüm kamu kurum ve kuruluşlarında, kuruluşun politika düzeyinde e-dönüşüm çalışmalarını yönlendirmek üzere belirlenecek “dönüşüm liderleri” arasından seçilerek oluşturulacak ve Strateji'nin etkin şekilde hayata geçirilmesi ve kurumlararası işbirliğinin temini için ortak bir platform olacaktır (DPT, 2006a: 44).

Diğer kurul olan “Danışma Kurulu” ise revize edilerek; toplumun tüm kesimlerinin sürece etkin katılım ve desteğini sağlamak ve gerekli dayanışma ve işbirliği ortamını tesis etmek amacıyla STK'lar, üniversiteler ve özel kesim temsilcilerinden oluşturulacaktır. Söz konusu Kurul, Strateji'nin uygulama sürecinde İcra Kurulu'nun faaliyet ve kararlarına yardım ve destek sunacaktır (DPT, 2006a: 44).

Nitekim, 2007/7 sayılı Başbakanlık Genelgesi ile Strateji Belgesi'nde adı geçen “e-Dönüşüm Türkiye İcra Kurulu”, “Dönüşüm Liderleri Kurulu” ve “Danışma Kurulu”na ilişkin kararlar hayata geçirilmiştir. Buna göre, e-Dönüşüm Türkiye İcra Kurulu'nun üyesi Bakan ve üst düzey bürokrat sayısı ile katılımcı kamu ve STK temsilcileri artırılarak, İcra Kurulu'nun yapısı güçlendirilmiştir.⁸⁶ Ayrıca, “e-

⁸⁶ Genelge'yle Kurul toplantılarına katılacaklar şu şekilde oluşturulmuştur: DPT'nin bağlı olduğu Devlet Bakanı, Milli Eğitim Bakanı, Ulaştırma Bakanı, Sanayi ve Ticaret Bakanı, Başbakanlık

Dönüşüm Türkiye Danışma Kurulu” da yeniden yapılandırılmış ve kamu kurumu niteliğindeki meslek kuruluşları, üniversiteler ve STK temsilcilerinden oluşan yeni bir yapıya kavuşturulmuştur.

3.2.1.3.5 Bilgi Toplumu Stratejisi (2006-2010) Eylem Planı

2006-2010 Eylem Planı, 2006-2010 Bilgi Toplumu Stratejisi kapsamında belirlenen stratejik amaç ve hedeflere ulaşılmasını sağlamak üzere hayata geçirilecek faaliyet ve projeleri kapsamaktadır. Bu çerçevede, Türkiye’nin bilgi toplumuna dönüşmesine yönelik olarak hazırlanmış 111 farklı eylemden oluşmaktadır (DPT, 2006b: 1). Plan, İnternet’in düzenlenmesi konusuyla doğrudan ilgili olan “İnternet güvenliği” konusunu Strateji belgesine paralel olarak “sosyal dönüşüm” başlığı altında ele almıştır. Buna göre, 10. eylem olarak “İnternet güvenliği” belirlenmiştir. Bu çerçevede bireylerin bilgi iletişim teknolojilerini kullanımına yönelik motivasyonlarının artırılması amacıyla İnternet ortamını güvenli hale getirecek yasal düzenlemelerin gerçekleştirileceği ve İnternet üzerinde çeşitli denetim ve yasaklar uygulanacağı, ölçülülük kriterlerine bağlı kalınması şartıyla, çocukların zihinsel ve bedensel sağlığının, kişilik haklarının, ailenin ve kamu düzeninin korunmasının sağlanacağı açıklanmıştır (DPT, 2006b: 10).

Böylece, 2005 Eylem Planı’nda “İnternetin güvenli kullanımı” bağlamında bilgi toplumu belgelerine girmeye başlayan İnternet içerik düzenlemesine yönelik ihtiyaç tespitinin ve irade beyanın, 2006-2010 Eylem Planı’nda daha da ileri götürülerek daha vurgulu hale getirildiği ve belirginleştirildiği görülmektedir. Öyle ki, “güvenli İnternet” konsepti içerisinde yasadışı ve zararlı içerikle mücadele kapsamında “gereklilik” ve “ölçülülük” kriterlerine bağlı kalmak şartı ile yasal düzenlemelerin yapılması ve İnternet üzerinde çeşitli denetim ve yasakların uygulanmasının gerekli olduğu açıkça ortaya konulmuştur. Söz konusu Plan, bu gerekliliği makul bir gerekçeye dayandırmaktadır; çocukların, ailenin ve kamu düzeninin korunması

Müsteşarı, İçişleri Bakanlığı Müsteşarı, Maliye Bakanlığı Müsteşarı, DPT Müsteşarı ve bir Başbakanlık Başmüaviri, TÜBİTAK Başkanı, TK Başkanı, KOSGEP Başkanı, Türksat A.Ş Genel Müdürü, Dönüşüm Liderleri Kurulu Başkanı ve e-Dönüşüm Türkiye Danışma Kurulu Başkanı ile TUSİAD, TOBB, TBV, TBD, Yazılım Sanayicileri Derneği ve TÜBİSAD başkanları.

(DPT, 2006b). Nitekim, benzer gerekçelerle ortaya çıkan 5651 Sayılı Yasa, Plan’da yer alan bu 10. eylemin bir ürünü olarak değerlendirilebilir.

Aslında, bahsi geçen Eylem Planı ve dayandığı Strateji’nin bu gerekçelerin de üzerindeki gerekçesi, hareket noktası ve amacı; bilgi toplumuna ulaşmanın ve bu kapsamda İnternet kullanımının yaygınlaştırılmasının önündeki fiziksel ve psikolojik engellerin kaldırılmasıdır. Bu nedenle “güvenli İnternet” eylemi, “sosyal dönüşüm” stratejik önceliği içinde toplumun İnterneti daha fazla kullanma motivasyonlarını artırma bağlamında değerlendirilmiştir. Söz konusu eylemin, Plan’da “Sosyal Dönüşüm” ana başlığı ve “Yüksek Motivasyon ve Zengin İçerik” alt başlığı altında ele alınması bu yaklaşımın bir göstergesidir (DPT, 2006b).

Plan’da bahsi geçenler dışında özellikle İnternetin düzenlenmesi kapsamında değerlendirilebilecek birkaç eylemden daha söz edilebilir. Bunlardan birisi, “kamu yönetiminde modernizasyon” stratejik önceliği içinde ele alınmış bulunan sayısal medyada ve İnternet ortamında sunulan ürünlere ilişkin fikri hakların korunmasıyla ilgili yasal düzenlemelerin yapılmasını öngören 83. Eylemdir (DPT, 2006b: 32).

Aynı stratejik öncelik çerçevesinde benimsenen diğer eylemler ise, “Güvenlik ve Kişisel Bilgilerin Mahremiyeti” alt başlığında yer almaktadır. Buna göre, 87. eylemde; bilgi güvenliği ile ilgili olarak ve kişisel verilerin korunması hakkında yasal düzenlemelerin yapılması, 88. eylemde; siber güvenlik tehditlerini sürekli olarak takip edecek ve tedbirleri koordine edecek “bilgisayar olaylarına acil müdahale merkezi (CERT)” kurulması kararlaştırılmıştır. Ayrıca, Ulusal Bilgi Sistemleri Güvenlik Programı’nın hayata geçirilmesi benimsenmiştir (DPT, 2006b: 33).

Türkiye’nin İnternete bakışını ve İnternet politikalarının ana eksenini oluşturan e-dönüşüm Türkiye Projesi ve bu Proje kapsamında üretilen bilgi toplumu belgeleri genel olarak incelendiğinde; konunun daha ziyade ekonomik kalkınma, refah devleti olma, üretimde ve kullanımda teknolojik gelişmişliği yakalama, e-devlet uygulamaları ile devleti dönüştürme ve hatta demokratikleştirme bağlamında ele alındığı dikkat çekmektedir. Bu nedenle, bilgi toplumuna dönüşme ve bilgi

ekonomisine geçme hedefi büyük bir ideal olarak genellikle pozitif yönleriyle belgelere yansımıştır. Konunun, bilgi toplumuna yöneltilen eleştiriler, bilgi ve iletişim teknolojilerinin ve özellikle İnternetin kendisinin veya yanlış kullanımının neden olduğu sorunlar boyutu çok fazla ön plana çıkartılmamıştır.

Bu yaklaşımın benimsenmesinde, başlangıçta ülkede İnternet kullanımının düşük olmasının ve dolayısıyla İnternetin beraberinde getirdiği güvenlik ve toplumsal sorunlarla henüz fazlasıyla tanışılmamasının etkili olduğu düşünülebilir. Bunun yanında, ülkenin ekonomik, sosyal ve siyasal iç dinamikleri açısından bu tür sorunların dile getirilmesinde bazı riskler görülmüş olabilir. Bu çerçevede, henüz palazlanmakta olan bilişim sektörünün ürkütülmesinden korkulması, teknoloji ve İnternet düşmanı ilan edilme kaygısı gibi birçok sebep akla gelebilir. Nitekim, bu korkuların bir kısmı halen geçerliliğini sürdürmektedir.

Bilgi toplumu belgelerinin temelinde bu eksik yaklaşım göze çarpsa da, “güvenli İnternet” bağlamında yasadışı ve zararlı içerikle mücadeleyi öngören eylemlerin zaman içerisinde bu tür belgelere girmiş olması, sorunların varlığının ve söz konusu eksik yaklaşımın zimmen kabul edilmesinin ifadesi olarak görülebilir.

3.2.1.4 Uygulamalar

Türk Hukukunda, 5651 Sayılı Kanun’dan önce İnternet içeriğine müdahale, İnternet üzerinden işlenen suçların cezalandırılması ve erişim engellemesi uygulamaları farklı kanun hükümlerine dayanılarak gerçekleştirilmiştir. Bu çerçevede, İnternette kaynaklanan veya İnternetin araç olarak kullanılmasıyla meydana gelen ifade suçları, özel hayatın gizliliğini ihlal veya kişilik haklarına saldırılar gibi nedenlerle mahkemelere intikal eden davalar, mevcut yasalarla sonuçlandırılmaya çalışılmıştır.

Başlangıçta bu yaklaşıma göre, mevcut yasaların İnternete uygulanması ile sorunların çözülebileceği düşünülmüştür. Nitekim, 1998-1999’lu yıllarda Eski TCK kapsamında açılmış bir kaç dava, İnternet ortamında yayılan ifade için de ifade suçlarıyla ilgili genel düzenleme sisteminin yeterli olduğu düşüncesinin hakim olduğunu göstermektedir (Akdeniz ve Altıparmak, 2008: 4). Söz konusu davaların

mülga 765 sayılı TCK'nun 159. maddesinin 1. fıkrasına göre açıldığı görülmektedir.⁸⁷

Bu davalardan birisi Emre Ersöz davasıdır. Ersöz hakkında 1998 yılı Haziran ayında TURKNET'in açtığı "Güncel Forum" sayfasına yaptığı yorumdan dolayı "devletin emniyet kuvvetlerini alenen tahkir" suçunu işlemekten dava açılmıştır. Ersöz, yazdıklarının kamuya açık olmadığını, forumun yalnızca İnternet kullanıcılarına açık bir ortam olması nedeniyle kendisinin çevrimiçi yorumlarının aleni sayılamayacağını ileri sürmüştü de 10 ay hapse mahkum edilmiştir (Akdeniz ve Altıparmak, 2008: 5).

Diğer dava ise, 1999 yılında Superonline tarafından açılmış çeşitli forumların yöneticisi Coşkun Ak'ın 40 ay hapse mahkum edildiği davadır. Bu dava da İnternetle ilgili olayların diğer kitle iletişim araçları davaları gibi görüldüğünün bir örneğidir. Türkiye'deki insan hakları ihlallerini eleştiren mesajı forumdan kaldırmayan Coşkun Ak'a mahkeme bu cezayı, Ak'ın görevinin tıpkı bir gazetenin yazı işleri müdürünününe benzediğini belirterek vermiştir (Günaydın, 2010: 140-152).

Bu süreçte 2002 tarihli 4756 Sayılı Yasa kapsamında yalan haber, hakaret ve benzeri fiillerden doğacak maddi ve manevi zararlarla ilgili hükümlerden dolayı bazı tazminat kararları da verilmiştir. Örneğin, Afyon 2. Asliye Hukuk Mahkemesi, "sanliurfa.com" adlı web sitesinde kimliği belirsiz bir kişinin, dönemin Şanlıurfa Valisi hakkında hakaret içeren ifadeler yayınladığı için yer sağlayıcı şirketin Vali'ye 5 milyar TL. tazminat ödemesine hükmetmiştir (Ahi, 2004).

Bununla birlikte, yine aynı dönemde Yargıtay'a intikal etmiş bazı özel hukuk davalarında Yargıtay Hukuk Dairelerinin, İnternet yönetimi ile ilgili bir kanun olmadığı için dava konusu web sayfaların yayından kaldırılması taleplerinin reddedilmesi gerektiğine karar verdiği de görülmüştür. Yargıtay'ın bu tip kararlarının gerekçesinde, aksi durumda yargı kararlarının infaz edilebilirlik açısından sonuçsuz kalmaya mahkum olacağı görüşü etkili olmuştur (Akdeniz ve Altıparmak, 2008: 6).

⁸⁷ Söz konusu fıkra şöyledir: "Türklüğü, Cumhuriyeti, Büyük Millet Meclisini, Hükümetin manevi şahsiyetini, Bakanlıkları, Devletin askeri veya emniyet muhafaza kuvvetlerini veya Adliyenin manevi şahsiyetini alenen tahkir ve tezyif edenler altı aydan üç seneye kadar hapis cezası ile cezalandırılırlar."

Diğer yandan, 5651 Sayılı Yasa'dan önce de farklı yasa hükümlerine göre İnternet içeriğine müdahale edildiği ve birçok sitesinin engellenmiş olduğu görülmektedir. Özellikle zaman içerisinde bilişim suçlarının artması İnternet içeriğine karşı daha katı bir tutum alınmasına sebep olmuştur (Çağlar, 2011: 40). Nitekim, 2000-2004 yılları arasındaki değişik tarihlerde, birçok İnternet sitesinin TSK'ya hakaret, yolsuzluk söylentileri, Türklük karşıtı veya terörist propaganda, hakaret ve kumara ilişkin içerik bulundurdıkları gerekçesiyle mahkeme kararı ile İSS'lar tarafından engellendikleri görülmüştür. Fakat bunlardan sunucuları yurtdışında olan web sitelerinin bir kısmı, yasaklamaya rağmen yayınıni sürdürmeye devam etmiştir.⁸⁸

Bunların dışında MÜYAP, telif hakları bağlamında Türk sanatçıların eserlerinin bulunduğu korsan müzik ve videolar içeren web sitelerine karşı yürüttüğü hukuki mücadele ile birçok sitenin erişiminin engellenmesini sağlamıştır. Bu şekilde erişimi engellenen sitelerin sayısının 2005 yılında 153, 2006 yılında 886 ve 2007 yılında 549 olduğu tespit edilmiştir (Nebil, 2008).

Bunlar dışında farklı yasal düzenlemelerin gerekçe gösterilerek mahkemelerce erişim engelleme kararlarının alındığına da rastlanılmaktadır. Örneğin, Kadıköy 2. Asliye Hukuk Mahkemesi 14 Aralık 2006 tarihinde, Migros Türk T.A.Ş. aleyhinde hukuka aykırı ve tüzel kişiliği tahkir eden ve hakaret içeren iddia ve isnatlarda bulunduğu gerekçesiyle Türk Medeni Kanun'un 24. ve 25. maddeleri ile Hukuk Usulü Muhakemeleri Kanunu'nun 109 ve devamı maddeleri gereğince 30'a yakın web sitesinin kapatılmasına karar vermiştir (Günaydın, 2010: 157-158).

Diğer bir örnekte ise, G.Ö.'nün 2005'de İnternet sitelerinde görüntülerinin yayınlanması ile başlayan sürecin sonunda Kadıköy 1. Asliye Ceza Mahkemesi davayı TCK'nun 134. maddesinde yer alan özel hayatın gizliliğini ihlal suçu kapsamında değerlendirmiş ve yapılan yargılamada G.D. tarafından cep telefonu ile

⁸⁸ Bu sitelerden bazıları şunlardır: "Subay.Net", "ideapolitika.com", "yolsuzluklar.org", "yolsuzluk.com", "yolsuzluk.org", "altinsayfalar.com", "soygun.com", "turkbet.com", "pkk.org", "superbahis.com", "bahismerkezi.com", "cjb.net", "hizb-ut-tahrir.org", "alummah.org", "akademya.org", "cunta.org", "ucbucuk.com", "akparti.gen.tr", "altinrehber.com", "otuken.net", "soyguncular.com", "dindusmanlari.com", "aloihbar.org" (Akdeniz ve Altıparmak, 2008: 8-9).

çekilmiş G.Ö.'ye ait porno görüntülerin mağdurenin katkısı olmadan iradesi dışında kaydedildiği ve yine iradesi dışında ırzına geçildiği sabit görülmüştür. Bu kapsamda Mahkeme, çekilen görüntüleri G.D. ile birlikte İnternet ortamında yayan ve yurtdışı kaynaklı bir siteye koyan S.Y.'yi, özel hayatın gizliliğini ihlal suçundan hapis cezasına mahkum etmiştir (Günaydın, 2010: 158-159).

Erişim engellemeler içerisinde en çok ses getireni ise, 5651 Sayılı Yasa çıkmadan hemen öncesinde 2007 yılı içerisinde mahkemelerin beş ayrı davada YouTube'un erişiminin engellenmesine karar vermeleridir. Bu kararlardan ikisi Atatürk'ü ve diğer kutsal değerleri aşağılamaya, birisi PKK saldırılarını övme ve terör propagandasına, birisi Hırant Dink'in katlini ve katillerini övmeye, sonuncusu ise "soruşturmanın gizliliğini ihlale" ilişkin engellemelerdir (Akdeniz ve Altıparmak, 2008: 31-34).

3.2.2 5651 Sayılı Kanun'un Gelişimi

Çocukların, ailenin ve kamu düzeninin korunması için İnternet ortamında bulunan yasadışı ve zararlı içerikle mücadele edilmesi ve bu konuda yasal düzenleme yapılmasının gerekliliği e-Dönüşüm Türkiye Projesi kapsamında yayınlanan 2006-2010 Bilgi Toplumu Stratejisi Eylem Plan'ında yer almaktaydı. Plan'ın 10. eylemi, "güvenli İnternet" için "gereklilik" ve "ölçülülük" kıstaslarına bağlı kalarak yasal düzenlemelerin yapılmasını ve İnternet üzerinde çeşitli denetim ve yasakların uygulanmasını öngörüyordu.

Ülkenin İnternet politikalarının temel referans belgesi olan söz konusu Eylem Plan'ında yer alan ve hayata geçirilmesi kararı alınan bu eylemi tetikleyen ve daha da hızlı olarak ülke gündemine taşıyan bazı olaylar, 2006-2007 yıllarında vuku bulmuştur. 2006 başında kurulan İstanbul Emniyet Müdürlüğü Asayiş Şubesi'ne bağlı Bilişim Polisi, 2000'lerden beri gelen çeşitli şikayetlere (dolandırıcılık, kişilik haklarına saldırı ya da çocuk pornosu) toplu olarak işlem yapmaya başlamış (Nebil, 2008) ve üst üste gelen operasyonlar İnternetin zarar veren, tehlike ve riskler taşıyan olumsuz yönünün kamuoyu ve karar vericiler tarafından daha iyi görülmesine neden olmuştur.

İnternetin pornografik içeriğe erişimi çok kolay hale getirmesi, yoğun bir şekilde devam eden çocuk pornosu operasyonları, intiharı körükleyen Satanist içerikler, İnternet kafelerde yaşanan olumsuz hadiseler, çocuklarda görülen oyun tutkunluğu, çocukların ve gençlerin İnternet üzerinden yanlış ve zararlı kişilerle ve çevrelerle tanışmaları yönündeki endişeler, konusu hakaret içeren Atatürk'le, milli ve manevi değerlerle ilgili YouTube videolarının ulaşılabilirliğinin getirdiği sorunlara ilişkin şikayetler ve bu konuların sık sık basında yer bulması, İnternet'in düzenlenmesi taleplerini daha yoğun bir şekilde gündeme getirmiştir. Bu talepler, hükümet ve Meclis'i, İnternet içeriğinin düzenlenmesi için yeni bir kanun yapılması amacıyla harekete geçirmiştir (Nebil, 2008; Akdeniz ve Altıparmak, 2008: 10-11).

Bu atmosfer içinde, İnternet içeriğine müdahale amacıyla farklı neden ve yöntemleri öngören iki kanun tasarısı ve bir kanun teklifi hazırlanmıştır. 5651 sayılı Kanun, bu tasarı ve teklifler üzerinde gerçekleşen tartışmalar ve yürütülen çalışmalar ile şekillenerek vücut bulmuş ve bugünkü halini almıştır (Kaya, 2010: 79).

3.2.2.1 Bilişim Ağı Hizmetlerinin Düzenlenmesi Ve Bilişim Suçları Hakkında Kanun Tasarısı

İnternet içeriğinin özel bir kanunla düzenlenmesine yönelik ilk girişim Adalet Bakanlığınca 2006'da gerçekleştirilmiştir (Kaya, 2010:79). Adalet Bakanlığı, İnternet içeriğini düzenlemek ve İnternet suçlarıyla mücadele etmek amacıyla yeni bir kanun taslağı üzerinde çalışmaya başlamıştır. Bu kapsamda hazırlanan taslak, hakkında görüş bildirmesi için üniversiteler, mahkemeler ve ilgili bakanlıklar ve barolar dahil 100'den fazla kurum ve kuruluşa gönderilmesine rağmen yeterince kamuoyu ile paylaşılmadığı gerekçesiyle eleştirilmiştir (Akdeniz ve Altıparmak, 2008: 11).

“Bilişim Ağı Hizmetlerinin Düzenlenmesi ve Bilişim Suçları Hakkında Kanun Tasarısı” başlıklığını taşıyan taslak metinde Kanunun amaç ve kapsamı; içerik sağlayıcı, yer sağlayıcı, erişim sağlayıcı, ortam sağlayıcı ve toplu kullanım sağlayıcıların sorumlulukları ile bilişim sistemi veya bilişim ağı kullanılarak işlenen suçları, bu suçların soruşturulması ve kovuşturulmasına ilişkin esas ve usulleri

düzenlemek olarak belirtilmiştir. Genel gerekçede Tasarı ile, ülkemizde kullanımı giderek yaygınlaşan bilişim ağlarının ortaya çıkartmış olduğu hukuki ve cezai sorunların çözüme kavuşturularak bilişim ağı alanında hukuk sistemimizin AB normları ile uyum sağlanmasının amaçlandığı dile getirilmektedir (Bt-stk.org., 2006).

Taslak, genel olarak iki kısımdan oluşmaktadır. Birinci kısımda içerik, yer, erişim, ortam ve toplu kullanım sağlayıcıların tanımları ile bunların sorumlulukları, yükümlülükleri ve denetimleri yer almaktadır. İkinci kısımda ise, “bilişim sistemlerine ilişkin suçlar”, “bilişim sistemi bağlantılı suçlar”, “içerik bağlantılı suçlar ve idari yaptırımlar” ile “soruşturma ve kovuşturma usulleri” gibi cezai sorumluluklarla ilgili hükümler bulunmaktadır (Bt-stk.org., 2006).

Tasarı’nın hemen 3. maddesinde “Kişilerin ifade ve bilgiye erişim özgürlüğü esastır. Bu özgürlükler ancak kanunla belirtilen hallerde sınırlandırılabilir” denilerek, bu Yasanın omurgasının “ifade özgürlüğü” olduğu beyan edilmiş ve sınırlandırma eğer “yasa” ile yapılmazsa; tüm müdahalelerin bu kanuna aykırı sayılacağı vurgulanmıştır (İlkiz, 2006). Dolayısıyla, AIHS’nin 10. maddesinde öngörülen ifade hürriyetine uygun bir düzenleme yapılmıştır.

Ayrıca, Tasarı’da yer alan “İfade ve bilgiye erişim özgürlüğü”nü düzenleyen 3. madde ile “bilişim ağı üzerinden verilen hizmetlerin, yasaklayıcı uygulamalar yerine, kendi kendini denetim yöntemleri ile düzenlemenin yapılması ve sürdürülmesi” yönteminin daha uygun olacağı benimsenmiştir (Bt-stk.org., 2006).

Benzer bir yaklaşımla tasarının 4. maddesinde “serbestlik ilkesi”ne yer verilmiştir. Buna göre diğer kanun hükümleri saklı kalmak şartı ile; “Bilişim ağı hizmetlerine ilişkin faaliyetler serbesttir. Bu faaliyetlere başlama, yürütme ve sona erdirmeye, izne, bildirime veya başka bir koşula bağlı değildir”. Bu durumda, bilişim hizmetlerinde “yasaklar” yerine, “serbestlik” ve öz denetim tercih edilmiştir (Bt-stk.org., 2006). Bu düzenleme AB e-Ticaret Direktifi 4. maddesi ile uyum gözetilerek hazırlanmıştır.

Taslak, içerik sağlayıcıyı “Bilişim ağı üzerinden kullanıcılara sunulan her türlü bilgi veya veriyi üreten, değiştiren ve sağlayan gerçek veya tüzel kişi” olarak tanımlarken,

genel ilke olarak içerik sağlayıcının kullanıma sunduğu her türlü içerikten sorumlu olduğunu belirtmektedir. Bununla birlikte bağlantı sağladığı, başkalarına ait içerikten sorumlu değildir. Fakat, “sunuş biçiminden, bağlantı sağladığı içeriği benimsediği ve kullanıcının söz konusu içeriğe ulaşmasını amaçladığı açıkça belli ise, genel hükümlere göre sorumludur” (Bt-stk.org., 2006).

Taslağa göre yer sağlayıcı, “Hizmet ve içerikleri barındıran sistemleri sağlayan veya işleten gerçek veya tüzel kişiler”dir. Genel ilke olarak, yer sağlayıcı, barındırdığı içeriği kontrol etmek veya hukuka aykırı bir faaliyetin olup olmadığını araştırmakla yükümlü değildir. Fakat, ceza sorumluluğu ile ilgili hükümler saklı kalmak kaydıyla, bu kanunun 13. ve 29. maddelerinde düzenlenen “düzeltme ve cevap hakkının” ve adli mercilerin talebi gereği haberdar edilmesi ve engelleme yeteneği bulunması durumunda hukuka aykırı içeriğe erişimi engellemek zorundadır (Bt-stk.org., 2006).

Taslağa göre Erişim sağlayıcı ise, “Kullanıcılarına herkese açık bilişim ağına erişim olanağı sağlayan her türlü gerçek veya tüzel kişiler”dir. Genel ilke olarak, erişim sağlayıcı naklettiği içerikleri kontrol etmek veya hukuka aykırı faaliyetleri araştırmakla yükümlü tutulmamıştır. Fakat, bu Kanun hükümlerine uygun olarak haberdar edilmesi ve engelleme yeteneği bulunması durumunda, hukuka aykırı içeriği yayından çıkarmak ve engellemekle, sağladığı hizmetlere ilişkin trafik bilgilerini⁸⁹ doğruluğu ve bütünlüğünü sağlamak şartıyla altı aydan az ve beş yıldan fazla olmamak üzere saklamakla ve faaliyetine son vereceği tarihten en az üç ay önce durumu TK’na, içerik sağlayıcılarına ve müşterilerine bildirmekle ve trafik bilgisi kayıtlarını TK’una teslim etmekle yükümlü kılınmıştır (Bt-stk.org., 2006).

Tasarıda toplu kullanım sağlayıcı “Kişilere belli bir yerde ve belli bir süre bilişim ağını kullanım olanağını sağlayan” olarak tanımlanmıştır. Ticari amaçla toplu kullanım sağlayıcıların denetimi ve ruhsata ilişkin yükümlülükleri mahalli mülki amirliklere verilirken, ruhsatla ilgili bilgi ve belgelerin otuz gün içerisinde mahalli

⁸⁹ Taslakta trafik bilgisi “Bilişim ağı üzerinden gerçekleştirilen her türlü erişime ilişkin olarak taraflara, zamana, süreye, yararlanılan hizmetin türüne, aktarılan veri miktarına ve bağlantı noktalarına ilişkin değerlerden en az birini” ifade eder.

mülki amir tarafından TK'na bildirilmesi istenilmiştir. Ayrıca, toplu kullanım sağlayıcılar, bu kanunun kapsamına giren “içerikle ilgili suçlara” ilişkin içeriğe erişimi önleyici tedbirleri almakla da yükümlü kılınmıştır (Bt-stk.org., 2006).

Taslak, yer ve erişim sağlayıcılara bilişim ağı üzerinde kendi içeriklerinde “gerçek kişi ise; adı ve soyadı, vatandaşlık numarası, tüzel kişi ise; unvanı, vergi kimlik numarası veya sicil numarası, yerleşim adresi, e-posta adresi, sunduğu hizmet bir merciin iznine veya denetimine tabi bir faaliyet çerçevesinde sunuluyor ise yetkili denetim merciine ilişkin bilgiler”in bulundurulması yükümlülüğünü de getirmiştir (Bt-stk.org., 2006).

Tasarıyla içerik, yer, erişim ve toplu kullanım sağlayıcılarına getirilen yükümlülükler ile bu İnternet aktörlerinin kayıt altına alınmaları hedeflenirken, kullanıcılar ve yetkili makamların bunlara kolaylıkla ulaşabilmeleri temin edilmeye çalışılmıştır. Keza, İnterneti mümkün olduğunca kayıt altına alma, İnternet aracılığıyla işlenen suçların takibi, sorumlularının tespiti ve erişim engellemesi tedbirlerinin uygulanması konularında yaşanan sorunların ortadan kaldırılması amaçlanmıştır.

Tasarı, Anayasal bir hak olan “düzeltme ve cevap hakkı”nı İnternet alanı için de düzenlemiştir. 5187 Sayılı Basın Kanunu’nun yazılı basın için, 3984 ve 2954 Sayılı Kanunların radyo ve televizyon yayınları için hükme bağlamış olduğu “düzeltme ve cevap hakkı”, tasarının 13. maddesinde yer almıştır. Daha sonra “uyar-kaldır” uygulamalarının da temelini oluşturacak olan “düzeltme ve cevap hakkı”, bu maddede geniş olarak “hak ihlali” olarak ele alınmış ve “içeriğe erişimin düzeltilmesi ve engellenmesi” başlığı altında düzenlenmiştir (Bt-stk.org., 2006).⁹⁰

⁹⁰ Maddenin düzenlenme biçimi ve madde gerekçesinde yer alan açıklamadan, içerik nedeniyle hakları ihlale uğradığını iddia eden gerçek ve tüzel kişiler için iki aşamalı bir başvuru usulünün öngörüldüğü söylenebilir. Bunlardan ilki, iddia sahiplerinin içerik sağlayıcıya başvurarak içeriğin düzeltilmesini, erişimin engellenmesini veya cevap hakkının yayınlanmasını istemeleridir. Bu aşamada eğer içerik sağlayıcıya erişilemiyorsa yer sağlayıcıya, ona da erişilemiyorsa erişim sağlayıcıya aynı talepleri iletebilirler. Bu talebe en az üç gün içinde cevap verilmesi gerekmektedir. Başvuru sahibinin talebine süresi içinde cevap verilmemesi ya da reddedilmesi halinde, ikinci aşamaya geçilmektedir. Bu durumda başvuru sahibi onbeş gün içinde yerleşim yerinde bulunan sulh ceza mahkemesinden içeriğe erişimin engellenmesi, içeriğin düzeltilmesi veya cevap hakkının

Tasarının ikinci kısmında suç ve cezalar düzenlenmiştir. Bu kapsamda ilk olarak bilişim suçları diyebileceğimiz, “bilişim sistemine girme ve veri elde etme”, “verilere, programların bütünlüğüne veya sistemin çalışmasına müdahale”, “hukuka aykırı donanım veya program”, “bilişim sistemini kullanarak sahtecilik”, “bilişim ortamında yarar sağlamak”, “banka veya kredi kartlarının kötüye kullanılması”, “yanıltarak bilgi toplamak ve taklit yoluyla yanıltmak” suçları ve karşılık gelen cezalar belirlenmiştir (Bt-stk.org., 2006).

İkinci olarak ise, “İçerik Bağlantılı Suçlar ve İdari Yaptırımlar” başlığı altında “çocuk pornografisi bağlantılı suçlar” ve “devletin güvenliğine ve kamu barışına karşı işlenen suçlar” düzenlenmiştir. Tasarıda bu bölümde yer alan içerik bağlantılı suçlarla ilgili düzenlemeler dikkat çekicidir. 23. madde, bilişim ortamında, bir çocuğa veya çocuk gibi görünen veya çocuk olduğu izlenimi veren bir kişiye ait gerçek ya da temsili görüntü, yazı veya sesleri içeren pornografik ürünleri tanıtmak, sunmak, kiraya verme veya satışa arz etmeyi suç saymış ve bu suçları işleyen kişilere altı yıldan oniki yıla kadar hapis ve bin güne kadar adli para cezası öngörmüştür. Suç kapsamına giren bu tür ürünleri, bilişim ortamında kendisi veya başkaları için temin eden veya bulunduran kişilere de iki yıldan beş yıla kadar hapis ve beşbin güne kadar adli para cezası takdir edilmiştir (Bt-stk.org., 2006).

Böylece çocuk pornografisinin İnternet ortamında bulundurulması ve dağıtımını çeşitli yönleriyle suç olarak tanımlanmıştır. Bu konunun TCK’nın 226. maddesinde düzenlenmesine rağmen neden burada da tekrar yer aldığı sorusuna, 23. maddenin gerekçesinde cevap verilmektedir. Buna göre, söz konusu fiillerin, bilişim ortamında üretimi ve dağıtımının çok daha kolay gerçekleşebildiğine dikkat çekilerek, bu nedenle ayrıca çocuk pornografisi ile sınırlı olarak özel bir düzenlemeye madde metninde yer verildiği dile getirilmektedir (Bt-stk.org., 2006).

yayınlanması kararı verilmesini isteyebilir. Sulh ceza hakimi bu istemi üç gün içerisinde duruşma yapmaksızın karara bağlar. Hakimin kararına karşı itiraz yolu açıktır. İtiraz vaki olursa, itiraz mercii üç gün içerisinde itirazı inceleyerek kesin kararı verir. Hakim, erişimin engellenmesi, içeriğin düzeltilmesi veya cevap hakkının yayınlanması kararı verirse; öncelikle içerik sağlayıcı, içerik sağlayıcıya erişilemiyorsa yer sağlayıcı, ona da ulaşılamıyorsa erişim sağlayıcı, bu kararın gereğini en geç kırksekiz saat içinde yerine getirir (Bt-stk.org., 2006).

İçerikle ilgili olarak 24. madde “devletin güvenliğine ve kamu barışına karşı işlenen suçlar” kapsamında bilişim ortamında aleni olarak; TCK’nun ilgili maddelerinde⁹¹ ve 5816 sayılı Atatürk Aleyhine İşlenen Suçlar Hakkında Kanunda yer alan ve bilişim sistemi veya ağıyla işlenen suçlara ilişkin içeriği üreten, tanıtan veya sunanlar hakkında hükmedilecek cezaların yarı oranında arttırılmasını düzenlemiştir. Maddenin gerekçesinde bazı suçların bilişim ortamında işlenmesi halinde, bunların soruşturulmasında/kovuşturulmasında karşılaşılan zorluklar ve bu suçların işlenmesinin diğer basın ve yayın araçlarına göre daha kolay olması nedeniyle özel bir düzenleme yapılması ihtiyacının doğduğundan bahsedilmiştir (Bt-stk.org., 2006).

Keza, Tasarı 26. maddesi ile, tehdit, şantaj, hakaret, kumar veya iftira suçlarının İnternet ortamında işlenmesi durumunda yarı oranında artırılacağını düzenlerken, 29. madde ile, erişim engellenmesi tedbirinin ne şekilde uygulanacağına ilişkin esas ve usullere yer verilmiştir (Bt-stk.org., 2006).⁹²

Tasarının yer, erişim ve içerik sağlayıcıların genel sorumlulukları ve yasadışı ve zararlı içeriklerle ilgili sorumluluklarını düzenleyen maddeleri yanında bir bütün olarak içerik ve bilişim suçlarını düzenleyen diğer maddelerinin, genel olarak AB

⁹¹ Şapka ve Türk Harfleri Kanuna muhalefet (md. 222), göreve ilişkin sırrın açıklanması (md. 258), Cumhurbaşkanına hakaret (md. 299), devletin egemenlik alametlerini aşağılama (md. 300), Türklüğü, Cumhuriyeti, Devletin kurum ve organlarını aşağılama (md. 301), devlete karşı savaşa tahrik (md. 304), yabancı devlet aleyhine asker toplama (md. 306), askeri tesisleri tahrip ve düşman askerî hareketleri yararına anlaşma (md. 307), düşman devlete maddî ve mali yardım (md. 308), TC Hükûmetine karşı silahlı isyan (md. 313), suç için anlaşma (md.316), askerleri itaatsizliğe teşvik (319), Yabancı hizmetine asker yazma, yazılma (md. 320), savaşta yalan haber yayma (md. 323), Devletin güvenliğine ilişkin belgeler (md. 326), Devletin güvenliğine ilişkin bilgileri temin etme (md. 327), Siyasal veya askerî casusluk (md. 328), Devletin güvenliğine ve siyasal yararlarına ilişkin bilgileri açıklama (md. 329), gizli kalması gereken bilgileri açıklama (md. 330), Uluslararası casusluk (md. 331), Devlet sırlarından yararlanma, Devlet hizmetlerinde sadakatsizlik (md. 333), yasaklanan bilgileri temin (334), Yasaklanan bilgilerin casusluk maksadıyla temini (md. 335), Yasaklanan bilgileri açıklama (md. 336), Yasaklanan bilgileri siyasal veya askerî casusluk maksadıyla açıklama (md. 337), Taksir sonucu casusluk fiillerinin işlenmesi (md.338), Devlet güvenliği ile ilgili belgeleri elinde bulundurma (md. 339). (5237 Sayılı TCK, 12.10.2004 tarih ve 25611 Sayılı Resmi Gazete)

⁹² Buna göre, tasarıda sayılan suçların soruşturulmasında veya kovuşturulmasında suç işlendiğine ilişkin kuvvetli şüphe sebeplerinin varlığı halinde, hakim veya gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısının yazılı emriyle erişimin engellenmesine karar verilebilecektir. Fakat, Cumhuriyet savcısı kararını yirmidört saat içinde hakim onayına sunmak ve hakim, kararını en geç yirmidört saat içinde vermek zorundadır. Sürenin dolması veya hakim tarafından aksine karar verilmesi halinde tedbir, Cumhuriyet savcısı tarafından derhal kaldırılır. Bu tedbirlere kovuşturma evresinde mahkemece karar verilebilecektir. Ayrıca, içeriğin engellenmesine ilişkin kararlara karşı ilgililer genel hükümlere göre itiraz edebileceklerdir (Bt-stk.org., 2006).

belgelerinin aynı konuları düzenleyen maddeleri ile paralellik arzedecek şekilde metne döküldüğü görülmektedir (Bt-stk.org., 2006).⁹³

Tasarı, düzenlediği suçların zaten 5237 sayılı TCK'da yer alması ve bazı suçların cezasını orantısız olarak artırması sebebiyle eleştirilmektedir (Akdeniz ve Altıparmak, 2008: 11). Bununla birlikte Tasarıda birçok konu düzenlenmesine rağmen halen bazı giderilmesi gereken yasal boşlukların bulunduğu dikkat çeken fakat genel olarak tasarıyı memnuniyetle karşılayan çevreler de olmuştur (Turkish Daily News, 2007). Hakim, akademisyen ve avukatlardan oluşan bir uzmanlar grubu ise söz konusu suçların Ceza Kanunu içine alınmasının daha uygun olacağı görüşünü dile getirmiştir (TBD, 2006).

Bunun yanında, Taslağın özünde tam bir ceza hukuku metni niteliğinde olduğu, taslağı hazırlayanların asıl amacının İnternet'i düzenlemek için erişimin engellenmesi ya da sansür için kurallar getirmek değil, yeni suçlar ihdas etmek olduğu da belirtilmiştir. Keza, Taslakta dikkat çeken hususlardan birisi de, 5651 Sayılı Kanun'un aksine, idari birimlere erişim engelleme yetkisi vermemiş olmasıdır (Akdeniz ve Altıparmak, 2008: 12).

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

Adalet Bakanlığı'nın kanun tasarısı tartışılırken, 18.12.2006 tarihinde bilişim ağlarının ortaya çıkardığı hukuki sorunları çözme amacıyla hazırlanan "Bilişim Sistemi Üzerinden Suç Teşkil Eden Zararlı Yayınlarla Mücadele Hakkında Kanun Teklifi", İstanbul Milletvekili Gülseren Topuz tarafından TBMM'ye sunulmuştur (TBMM, 2006). Teklif, Adalet Bakanlığı'nın Tasarısı'ndan çok daha kısa ve doğrudan İnternet aktörlerinin ve İnternet kafelerin yükümlülük ve denetimleriyle;

⁹³ Nitekim tasarının genel gerekçesinde, tasarı hazırlanırken 2001 tarihli Avrupa Konseyi Siber Suç Sözleşmesi'nden, AB'nin 2000/31/EG "Bilgi Toplumu Hizmetlerinin, Özellikle Elektronik Ticaretin Ortak Pazardaki Bazı Yönleri Hakkında Direktifi" yanında 1997/66 ile 2002/58 sayılı "Elektronik İletişimde Kişisel Verilerin İzlenmesi ve Gizliliğinin Korunması Yönergesi"nden ve 2000/31 sayılı "E-Ticaret Direktifi" ile 2002/58 sayılı "Elektronik İletişimde Gizliliğinin Korunması Yönergesi"nden yararlanıldığı belirtilmektedir (Bt-stk.org., 2006).

özellikle çocuk istismarı ve şiddet içerikli yayın, sahtecilik ve kumar gibi suçların İnternet üzerinden işlenmesine tedbir almayı amaçlayan bir metin olarak ortaya çıkmıştır. Teklif'in, AB e-Ticaret Direktifi'nin hükümleri gözetilerek hazırlandığı gerekçesinde belirtilmiştir (TBMM, 2006).

Teklif, amaç, kapsam, tanımlar ile İnternet aktörlerinin ve İnternet kafelerin sorumluluk ve denetimleriyle ilgili konularda Adalet Bakanlığı'nın tasarısıyla benzer hükümleri içermektedir. Bilgiye erişim hakkının ve ifade hürriyetinin esas olduğunu ve ancak kanunla sınırlanabileceğini belirten Teklif, İnternet aktörlerini içerik, erişim ve servis sağlayıcılar⁹⁴ olarak tasnif etmiş ve İnternet toplu kullanım sağlayıcılarla birlikte sorumluluklarını ve yükümlülüklerini belirlemiştir (TBMM, 2006).

Teklif'te, Adalet Bakanlığı tasarısından farklı olarak, servis sağlayıcılar için hukuka aykırı olduğunu saptadıkları içerikle ilgili olarak durumu gecikmeksizin yetkili mercilere bildirme yükümlülüğü öngörülmüştür. Ayrıca çocukların cinsel istismarı suçu, şiddet içerikli yayınlara yönelik suçlar, kumar ve sahtecilik suçları yeniden düzenlenmiştir. Buna göre, 7. maddede önceki tasarıdan farklı olarak, “çocuk pornografisi” yerine “çocuk istismarı” ifadesi kullanılmış fakat, suç tanımı olarak önemli bir değişikliğe gidilmemiştir. Sadece, tanıma “çocuk istismarı” yanında, “şiddet içerikli yayınlara yönelik veriler” ögesi de dahil edilmiştir (TBMM, 2006).

Teklif'te “sahtecilik” suçu, 8. maddede düzenlenmiş ve “aykırı bir amaca ulaşmak gayesi ile, bilgisayar sistemine gerçeğe aykırı bilgiler yükleyerek, mevcut verileri değiştirerek veya bunlara yeni şeyler eklemek suretiyle üçüncü kişilerin zararına olacak işlemlerde bulunmak” sahtecilik olarak tanımlanmıştır. Bu suçu işleyenlere iki yıldan dört yıla kadar hapis ve beş yüz güne kadar adli para cezası öngörülmüştür.

Teklif'te “kumar” suçununun düzenlendiği 9. maddeye göre, bilişim ağı üzerinde kumar oynatana iki yıldan dört yıla kadar hapis veya üç yüz günden bin güne kadar

⁹⁴ Teklif'te servis sağlayıcı “Kullanıcıların bilgisayar sistemi aracılığıyla birbirleriyle iletişimini sağlayan özel veya gerçek kişiler ile bu iletişim servisleri ve kullanıcılar için verileri işleme tabi tutan ya da bu verileri depolayan diğer kişiler” olarak tanımlanmıştır. Bu tanım ile erişim sağlayıcılar ile yer sağlayıcıları aynı tanımda birleştirilmekte ve birlikte değerlendirilmektedir (TBMM, 2006).

adli para cezası takdir edilmiştir. Erişim ve içerik sağlayıcıların denetimini düzenleyen 12. maddede ise, önceki Tasarıda olduğu gibi, denetleyici kurum olarak TK kabul edilirken; içerik sağlayıcıların içeriklerinin izlenmesi ve takibi için TK içinde “izleme ve takip komisyonu”nun kurulması önerilmiştir (TBMM, 2006).

“Teklif”te, İnternette suç oluşturan zararlı yayınlarla mücadele için İçişleri Bakanlığı bünyesinde ve ayrıca her vali veya yardımcısının başkanlığında “Zararlı Yayınlarla Mücadele Kurul”u oluşturulması öngörülmüştür. Kurul, bu kanuna göre işlenen aykırılıkları ve suç niteliğindeki hususların takibini yapmaya ve gerektiğinde konuyu TK’na ve yetkili adli mercilere intikal ettirmeye yetkili olacaktır (TBMM, 2006).

Nitelik olarak Adalet Bakanlığı’nın hazırlamış olduğu metinden fazlaca bir farkı bulunmayan bu Teklif, 12.04.2007 tarihinde, TBMM Adalet Komisyonu kararı ile 5651 sayılı Kanun Tasarısının içeriği ile örtüştüğü gerekçesiyle bu Tasarıyla birleştirilmiştir (TBMM, 2007a).

3.2.2.3 5651 Sayılı Kanun’un TBMM Süreci

Bu iki metin dışında Ulaştırma Bakanlığı 2007 yılında bilişim suçlarının önlenmesi amacıyla yeni bir kanun tasarısı üzerinde çalışmaya başlamıştır. İsmi “Elektronik Ortamda İşlenen Suçların Önlenmesi ile 2559 ve 2937 sayılı Kanunlarda Değişiklik Yapılmasına Dair Kanun Tasarısı” olarak belirlenen ve daha sonra 5651 sayılı Kanun’un adını alacak bu metin hazırlandıktan sonra Tasarı olarak 12.02.2007 tarihinde TBMM’ye sunulmuştur (TBMM, 2007b).

3.2.2.3.1 Genel Gerekçe

Tasarının genel gerekçesinde, başlangıçta dünyada olduğu gibi ülkemizde de, İnternetin hızla yaygınlaşması ve buna paralel olarak bu imkanların suiistimal edilerek suçların da hızlı bir şekilde arttığı tespiti yapılmaktadır. Dolayısıyla, artan bu suçlarla mücadele konusunda “etkin ve doğru bir yapılanmayı” mümkün kılacak konuya özel bir yasa çıkartılmasının zorunluluğu dile getirilmektedir (TBMM, 2007b).

Daha sonra, Anayasa'nın "Ailenin korunması" başlıklı 41. maddesine ve "Gençliğin korunması" başlıklı 58. maddesine atıfta bulunarak; 41. maddede geçen "Aile, Türk toplumunun temelidir" ve "Devlet, ailenin huzur ve refahı ile özellikle ananın ve çocukların korunması.. için gerekli tedbirleri alır, teşkilatı kurar" hükmü ile 58. maddedeki "Devlet.. gençlerin müsbet ilmin ışığında, Atatürk ilke ve inkılapları doğrultusunda ve Devletin ülkesi ve milletiyle bölünmez bütünlüğünü ortadan kaldırmayı amaç edinen görüşlere karşı yetişme ve gelişmelerini sağlayıcı tedbirleri alır" ve "Devlet, gençleri alkol düşkünlüğünden, uyuşturucu maddelerden, suçluluk, kumar ve benzeri kötü alışkanlıklardan ve cehaletten korumak için gerekli tedbirleri alır" hükümlerine vurgu yapılmaktadır (TBMM, 2007b).

Hazırlanan bu Tasarı'nın Anayasa'nın söz konusu hükümleri gereğince, aileyi, çocukları ve gençleri İnternet dahil elektronik iletişim araçlarının zararlarından koruma amacına yönelik olduğu; bu kapsamda, uyuşturucu ve uyarıcı madde alışkanlığı, intihara yönlendirme, cinsel istismar, kumar ve benzeri kötü alışkanlıkları teşvik eden İnternet içerikleriyle ilgili gerekli önleyici tedbirlerin alınmasının amaçlandığı belirtilmektedir. Böylece, "elektronik ortamda çocuğa, gençliğe ve aileye yönelik ağır ve vahim nitelikteki saldırıların önlenmesini teminen gereken yasal düzenlemenin yapılması" sağlanmış olacaktır (TBMM, 2007b).

Tasarı ile yeni bilişim suçları kategorisi oluşturulmadığı gibi, suçlara ilişkin cezai ve idari yaptırımlar da getirilmemektedir. Sadece, "TCK'nda yer alan belirli suçların İnternet dahil elektronik ortamda etkilerini sürdürmesinin, idari ve yargısal koruma tedbiri olmak üzere belirlenen iki yöntemle önlenmesi mümkün kılınmaktadır." Bu amaçla, TCK'da yer alan bazı suçların, "elektronik ortamda işlenmesinin içerik, yer ve erişim sağlayıcıları üzerinden önlenmesine ilişkin esas ve usuller belirlenmektedir." Bu yönü ile Tasarı, suçun ve suçlunun gelişen bilişim teknolojilerini kullanarak, Anayasa'nın, özel olarak korunmasını öngördüğü, başta aile, çocuklar ve gençler olmak üzere belirli sosyal kesimlere yönelik suçların kolayca işlenmesini önleyici "özel bir kanun" niteliğindedir (TBMM, 2007b).

Tasarıyla, TK bünyesindeki TİB'na ilave görev ve yetkiler verilerek, belirlenen esas ve usullere göre içerik denetiminin gerçekleştirilmesi öngörülmüştür. Bu kapsamda TİB'na, “elektronik ortamdaki zararlı içeriklerin izlenmesi ve önlem alınması”, “filtreleme görevi”, “bu konuda uluslararası kurum ve kuruluşlarla işbirliği sağlanması”, “şikayet ve talepleri değerlendirmek üzere izleme ve bilgi ihbar merkezi kurulması” gibi önemli yetki ve görevler verilmektedir (TBMM, 2007b).

Genel gerekçede, daha önce yapılan bazı yasal düzenlemelere atıfta bulunularak⁹⁵ bunların bilişim teknolojilerinde yaşanan baş döndürücü gelişmeler nedeni ile İnternet ortamında yapılan ve içerikleri suç teşkil eden yayınların önlenmesinde yetersiz kaldığı, bu konuyla ilgili yasal bir boşluk bulunduğu ve dolayısıyla bir ihtiyacın ortaya çıktığı dile getirilmektedir. Nitekim, Dünyada ve AB ülkelerinde bu ihtiyacı karşılamak için farklı adlarla da olsa genelde bağımsız ya da özerk yapıların oluşturulduğuna dikkat çekilmektedir (TBMM, 2007b).

Gerekçede, elektronik ortamda işlenen suçların hızla artış göstermesi, bu suçların işlenmesindeki kolaylığa karşın ortaya çıkarılmasındaki zorluklar, toplumsal açıdan doğabilecek zararların sonradan telafisinin mümkün olmaması, bu konuda etkin mücadele edecek kurumsal bir yapının acilen oluşturulmasını gerekli kıldığını belirtilmektedir. Keza, ülkemizde İnternet ortamı dahil elektronik ortamda yapılan yayınları teknik açıdan ve bilimsel olarak takip edecek, sorunları tespit edip çözümü için öneriler getirecek; İSS'ları da dahil elektronik haberleşme ve İnternet sektörünü koordine edecek kurumsal bir yapılanmanın kurulmasının zorunlu hale geldiği vurgulanmaktadır (TBMM, 2007b).

Gerekçede, bilişim teknolojileri ve sunduğu hizmetlerin, nitelikleri gereği sadece ulusların milli düzenlerini değil, tüm uluslararası toplumu etkilediği; bu nedenle, diğer ülkelerle ve uluslararası örgütlerle de bu alanda işbirliği ve koordinasyonun

⁹⁵ Atıfta bulunulan kanunlar şunlardır: 5237 sayılı TCK'nun “Bilişim Alanında Suçlar”ı başlığı altındaki 243 ve devamı maddeleri, 07.07.1927 tarih ve 627 sayılı Resmi Gazete’de yayımlanan 1117 sayılı Küçükleri Muzır Nesriyattan Koruma Kanunu, 17.01.1998 tarih ve 23233 sayılı Resmi Gazete’de yayımlanan 4320 sayılı Ailenin Korunmasına Dair Kanun’un ve 15.07.2005 tarih ve 25876 sayılı Resmi Gazete’de yayımlanan 5395 sayılı Çocuk Koruma Kanunu.

önemi hatırlatılmakta ve tasarı ile, TİB'na belirtilen suçlarla mücadelede diğer ülke muadil kuruluşları ve uluslararası örgütlerle gerekli işbirliği ve koordinasyonu sağlama görevinin de verildiği dile getirilmektedir (TBMM, 2007b).

Genel gerekçede, Tasarı'nın gerekliliği için Dünya'daki örneklerle ve AB düzenlemelerine, Anayasal referanslara, toplumsal ihtiyaçlara ve güvenlik endişelerine değinilirken, bilgi toplumu çalışmalarına ve bilgi toplumu belgelerine hiçbir atıf veya referansın yapılmamış olması oldukça ilginçtir. Halbuki, İnterneti ve İnternet politikalarını içine alacak şekilde ülkenin bir bütün olarak bilgi toplumuna dönüşümünü planlayan ve bu yöndeki çalışmalara yön veren "E-Dönüşüm Türkiye Projesi" ve onun bir parçası olarak, Tasarı'nın ortaya çıktığı tarihsel sürece denk düşen "2006-2010 Yılı Bilgi Toplumu Stratejisi ve Eylem Planı" bu Tasarı için belki de en önemli referans kaynağı ve belirleyici unsur olması gerekirdi. Maamafih, Strateji Belgesi'nde ve Eylem Planı'nda Tasarı'ya ilham, dayanak ve kaynaklık edecek epeyce malzeme de bulunmaktadır.

3.2.2.3.2 Adalet Komisyonu Çalışmaları

15.01.2007'de TBMM Adalet Komisyonu'na gönderilen Tasarı, 28.02.2007'de Alt Komisyon'a havale edilmiştir. Tasarıyı değerlendirdiği bir aylık süre zarfında dört toplantı yapan Alt Komisyon, oldukça kısa sayılabilecek bir sürede Tasarı'da usul ve esaslar açısından önemli değişiklikler öngören yeni bir metin ortaya çıkarmış ve raporunu 30.03.2007 tarihinde Adalet Komisyonu'na sunmuştur (TBMM, 2007a).

Adalet Komisyon'u,⁹⁶ Alt Komisyon'dan gelen Raporu görüşmeye başladığı 05.04.2007 tarihli ilk toplantısında, bundan sonraki görüşmelerde Alt Komisyon'un kabul ettiği metnin esas alınmasını kararlaştırmıştır. Buna göre, öncelikle Tasarı'nın

⁹⁶ Komisyon üyeleri ve diğer katılımcılar şöyledir: Milletvekilleri; Köksal TOPTAN (Başkan), Recep ÖZEL (Başkanvekili), Ramazan CAN (Sözcü), Hasan KARA, Fehmi Hüsrev KUTLU, Halil ÖZYOLCU, Haluk İPEK, F. Fikret BALOĞLU, Orhan YILDIZ, Feridun AYVAZOĞLU, Muzaffer KÜLCÜ, Mustafa Nuri AKBULUT, Hakkı KÖYLÜ, Muharrem KILIÇ, Orhan ERASLAN, Ahmet ÇAĞLAYAN, Bekir BOZDAĞ, Ulaştırma Bakanlığı Müsteşarı İbrahim ŞAHİN, Adalet, Ulaştırma, İçişleri ile Maliye bakanlıkları, Yargıtay Cumhuriyet Başsavcılığı, TK, TİB, EGM, Jandarma Genel Komutanlığı, Milli Piyango İdaresi Genel Müdürlüğü temsilcileri ile Prof. Dr. İzzet ÖZGENÇ (TBMM, 2007a).

adı “İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun Tasarısı” olarak değiştirilmiştir. Değişikliğin gerekçesinde, “elektronik ortam” ifadesinin mobil ve sabit telefonlarla birlikte, telsiz, faks, telgraf gibi haberleşme araçları ile radyo ve televizyon gibi yayın araçlarını da kapsadığı; bu durumun yapılamak istenen düzenlemenin “maksadını aşan içeriğe sahip bir metin” ortaya çıkardığı belirtilmiştir. Böylece, Tasarı’nın kapsamı “İnternet“ ile sınırlandırmıştır (TBMM, 2007a).

Tasarı, münhasıran “İnternetin içerik düzenlenmesi“ne yönelik bir metin konseptine dönüştürüldükten sonra metin içinde ekleme-çıkarma şeklinde yapılan değişikliklerle bu konseptte uygunluğun sağlanmaya çalışıldığı görülmektedir. Nitekim, İnternet ortamında yapılan yayınların düzenlenmesi ve bu yayınlarla ilgili olarak sorumluluk rejimini belirlemek amacıyla Tasarıya yeni maddeler eklenmesi ve metnin daha kısa ilk haline göre daha uzun ve detaylı düzenlemelere yer vermesi, bu amaca yönelik değişiklikler olarak değerlendirilebilir.

Bu yaklaşımın izleri Tasarı’nın amaç ve kapsam maddesini düzenleyen 1. maddede yapılan değişiklikte de görülmektedir. Komisyon, “Bu Kanunun amacı, elektronik ortamda işlenen belirli suçların içerik, yer ve erişim sağlayıcıları üzerinden önlenmesine ilişkin esas ve usulleri düzenlemektir” ifadesini, “Bu Kanunun amaç ve kapsamı; içerik sağlayıcı, yer sağlayıcı, erişim sağlayıcı ve toplu kullanım sağlayıcıların yükümlülük ve sorumlulukları ile İnternet ortamında işlenen belirli suçlarla içerik, yer ve erişim sağlayıcıları üzerinden mücadeleye ilişkin esas ve usulleri düzenlemektir“ olarak değiştirmiştir. Böylece, içerik, yer ve erişim sağlayıcıların yanına “toplu kullanım sağlayıcıları“da dahil edilirken, düzenlemenin iki temel amacından birisinin bunlara ait “yükümlülük ve sorumlulukları belirlemek“, diğerinin ise bu aktörler üzerinden “İnternet ortamında işlenen belirli suçların önlenmesine ilişkin esas ve usullerin belirlenmesi“ olduğu vurgulanmıştır (TBMM, 2007a). Burada dikkat çeken bir ayrıntı dah vardır; ilk metinde belirli suçların “önlenmesi“nden bahsedilirken, değişiklikte belirli suçlarla “mücadele“den söz edilmektedir. Sanki bu alandaki düzenleme ve uygulamalar konusunda daha güçlü ve kararlı bir iradenin varlığı vurgulanmak istenmiştir (TBMM, 2007a).

Ayrıca, her iki metinde de “belirli suçlar“ denilerek İnternet ortamında işlenen tüm suçların bu Tasarı kapsamında yer almadığına, bilakis, sadece ilerleyen maddelerde yer alan belirli kategorilerdeki suçların mevzubahis olduğu peşinen beyan edilmektedir. Bu sınırlandırıcı yaklaşım, düzenlemeyi yapan iradenin bu Tasarı’yı bir İnternet içerik düzenlemesi çerçevesi içinde tutmaya çalıştığını da göstermektedir. Adalet Bakanlığı’nın akim kalan önceki Tasarısında bilişim suçlarını da kapsayan tartışmalı bir yaklaşımın benimsenmiş olduğu hatırlanacak olursa, bu Tasarı’da izlenen yolun daha doğru olduğu söylenebilir.

İnternette işlenen belirli suçlarla mücadele edilmesi konusunda içerik, yer ve erişim sağlayıcılarla birlikte “toplu kullanım sağlayıcıları“nın ayrıca telaffuz edilmesi ve Tasarıda yükümlülük, sorumluluk ve denetimleriyle ilgili yeni düzenlemelere konu edilmelerinin, o tarihte sıcak bir gündem maddesi olmalarıyla ilgisi bulunmaktadır. Zira, İnternet kafelerde giderek artan bazı olumsuzlukların ve bu mekanlarda yaşanan ve kamuoyu nezdinde infial uyandıran bazı olayların o günlerde özellikle medyada çokça yer alması, buraların çocuklar ve gençler için daha güvenli ve kontrollü yerler haline getirilmeleri konusunda Hükümeti adım atmaya zorlamıştır.

Tasarı metninde Komisyonunda başka bazı ilaveler ve değişiklikler de yapılmıştır. Bunlardan birisi 2. maddede “İnternet ortamı” ve “Toplu kullanım sağlayıcı” kavramlarının tanımlarında yapılan değişikliktir. Buna göre, “İnternet ortamı” ilk metinde “İnternet sistemi ve İnternet ağından oluşan ortam” olarak tanımlanırken, kabul edilen değişiklikle “Haberleşme ile kişisel veya kurumsal bilgisayar sistemleri dışında kalan ve kamuya açık olan İnternet üzerinde oluşturulan ortam“ olarak tarif edilmiştir. Böylece, İnternet üzerinden yapılan fakat yayın niteliği taşımayan haberleşmeler ile kişisel ve kurumsal bilgisayar sistemleri Tasarı’nın kapsamı dışına alınmıştır. Diğer yandan, ilk metinde “Toplu kullanım sağlayıcı“, “Ticari amaçla kişilere belli bir yerde ve belli bir süre İnternet ağını kullanım olanağı sağlayan” olarak tanımlanırken, değişiklikle “ticari amaçla” ifadesi metinden çıkartılarak ticari olmayan toplu kullanım sağlayıcılar da Tasarı kapsamına alınmıştır (TBMM, 2007a).

Keza, Komisyon Tasarı'ya 3. maddeden sonra gelmek üzere dört yeni madde eklemiştir. Komisyon Raporu'nda, Avrupa Konseyi Siber Suç Sözleşmesi ve Almanya'nın Tele Hizmetler Kanunu hükümlerinden yararlanılarak oluşturulduğu belirtilen bu maddeler sırasıyla içerik sağlayıcıların sorumluluğu, yer, erişim ve toplu kullanım sağlayıcıların yükümlülüğünü düzenlemiştir (TBMM, 2007a).

Tasarı'nın ilk haliyle 3. maddede yer alan fakat, Alt Komisyonca eklenen maddelerle 8. madde olarak teselsül ettirilen "Erişimin engellenmesi kararı ve yerine getirilmesi" başlıklı metin Komisyon'un en çok tartıştığı maddelerden birisini oluşturmuş ve üzerinde bazı değişiklikler yapılmıştır. Komisyon ilk olarak 8. maddenin 1. fıkrasının başlangıç cümlesini değiştirmiştir. Buna göre, ilk hali "Elektronik ortamda yapılan ve içeriği aşağıdaki suçları oluşturan yayınlarla ilgili olarak erişimin engellenmesine karar verilir" iken "İnternet ortamında yapılan ve içeriği aşağıdaki suçları oluşturduğu hususunda yeterli şüphe sebebi bulunan yayınlarla ilgili olarak erişimin engellenmesine karar verilir" ifadesi benimsenmiştir. İlk metindeki "suçları oluşturan" ifadesinin yerine "suçları oluşturduğu hususunda yeterli şüphe sebebi bulunan" ifadesi getirilmiştir (TBMM, 2007a).

İkinci olarak, erişim engellemesi tedbirinin uygulanacağı suçların kapsamında değişiklik yapılmıştır. İktidar ve muhalefet partileri arasındaki en büyük tartışma da sayma yöntemiyle metne dercedilen suç tiplerinin belirlenmesi konusunda olmuştur. Komisyon Raporu'na göre konusu suç oluşturan içeriğe sahip yayınlarla mücadele nin etkinliğini sağlama bakımından ilk metinde katalog içerisinde yer alan suçların sayısı mümkün olduğunca sınırlı tutulmuştur. Komisyon çalışmalarında katalog içerisinde yer alan suçların belirlenmesinde, Anayasa'nın uluslararası sözleşmelerden doğan hükümlerine paralel olarak güvence altına aldığı özellikle düşünceyi açıklama özgürlüğünün kısıtlandığı eleştirilerine maruz kalmamak için gerekli özen gösterilmiştir. Bu nedenle katalog suçlarının kapsamı, İnternet ortamında yapılan, çocukların ve gençlerin olumsuz olarak etkilenebileceği ya da cinsel yönden istismar edilmesiyle oluşturulmuş yayınlarla sınırlı tutulmaya çalışılmıştır. Alt Komisyon bu kapsamda gördüğü için 5237 sayılı TCK'nda yer alan "sağlık için tehlikeli madde temini (md.194)" suçunu da katalog suçlarına eklemiştir (TBMM, 2007a).

Alt Komisyonunda katalog suçların sayısının artırılmasına yönelik girişimler olmuştur. Komisyon'un CHP'li üyelerinin (Feridun Ayvazoğlu ve diğerleri) önerisi ile 5816 sayılı Atatürk Aleyhine İşlenen Suçlar Hakkında Kanun'da yer alan suçlar ile 5237 sayılı TCK'nın 302. maddesinde yer alan Türk Devleti'nin ve ülkenin bölünmez bütünlüğünü bozma suçu ve Anayasa'nın 174. maddesinde güvence altına alınan İnkılap Kanunları'na ve özellikle laiklik ilkesine karşı işlenecek suçların da erişim engelleme sebepleri arasına alınması önerilmiştir (TBMM, 2007a).

Bu önerilerden sadece 5816 sayılı Atatürk Aleyhine İşlenen Suçlar Hakkında Kanun'da yer alan suçlardan bir kısmı İnternet ortamındaki yayın yoluyla da işlenebileceği değerlendirmesiyle kabul edilerek katalog suçları arasına alınmıştır. Bunun dışındaki 302. madde ile İnkılap Kanunları'na ilişkin olan öneriler söz konusu suçların İnternet ortamında yapılan yayınlar yoluyla işlenemeyeceği göz önünde bulundurularak kabul edilmemiştir. Öneri sahibi CHP'li vekiller Komisyon Rapor'unda 8. maddeye ilişkin olarak karşı oy yazısı yazmıştır. Böylece, Komisyon, katalog suçlarının sayısını 6'dan 8'e çıkartmıştır (TBMM, 2007a).

Komisyon aşamasında 8. maddenin 2. fıkrasında yapılan değişikliklerle katalog suçlarına ilişkin bir koruma tedbiri olarak erişimin engellenmesi kararının kimin tarafından ve ne suretle verilebileceği hususunda ayrıntılı düzenleme yapılmıştır. Bu fıkra da en dikkat çekici değişiklik, gecikmesinde sakınca bulunan hallere ilişkin olanıdır. İlk metinde gecikmesinde sakınca bulunan hallerde erişimin, yetkili ve görevli kolluk kuvvetlerinin talebi üzerine veya re'sen, İletişim Başkanlığı'nın yazılı emriyle engellenebileceği öngörülmüştü. Yapılan değişiklikle gecikmesinde sakınca bulunan hallere ilişkin bu kararı Savcılıkların vermesi hükme bağlanmıştır. Savcılık kararına karşı itiraz yolunun açık olduğu da belirtilmiştir (TBMM, 2007a).

Komisyon'un, ilk metinde olmadığı halde Tasarı'ya eklediği başka bir düzenleme ise "İçeriğin yayından çıkarılması ve cevap hakkı" başlığını taşıyan 9. maddedir. Bu şekilde 5187 sayılı Basın Kanun'unun cevap ve düzeltme hakkının kullanılmasına ilişkin hükümleri göz önünde bulundurularak İnternet ortamında yapılan yayınlarla kişilik haklarına saldırıda bulunan kişilere yönelik yeni bir düzenleme yapılmış ve bu

nitelikteki içeriğin yayından çıkarılması ve buna karşı cevap hakkının ne şekilde kullanılabileceğine ilişkin hükümler getirilmiştir (TBMM, 2007a).

Komisyon, bahsi geçen iş ve işlemleri yerine getirmekle görevli kamu kurumunu ve görevlerini belirleyen “İdari yapı ve görevler” başlıklı düzenlemeyi neredeyse ilk hali ile kabul etmiştir. Buna göre TİB, Tasarı’nın 10. maddesiyle, Tasarı’da kendisine tevdi edilmiş tüm görevleri yerine getirmekle memur edilmiş ve bunun için Başkanlığa yeni kadrolar ve mali ayrıcalıklar verilmiştir (TBMM, 2007a).⁹⁷

Komisyon sadece, bu Kanunla oluşturulacak İnternet Kurulu’nu ve bu kurul ile TİB arasındaki ilişkileri düzenleyen 10. maddenin “h” fıkrasını, böyle bir kurula gerek olmadığı ve kurulması öngörülen “Kurul”un daha baştan işlevsiz kalacağı değerlendirmesiyle kabul etmeyerek Tasarı’dan çıkartmıştır (TBMM, 2007a).

3.2.2.3.3 TBMM Müzakereleri

Adalet Komisyon’undan çıkan Tasarı 04.05.2007 tarihli TBMM Genel Kurulu’nda gündeme alınmıştır. Genel kurul aşamasında Tasarı esaslı bir değişikliğe uğramamıştır. Sadece, Komisyon aşamasında metinden çıkartılan “İnternet Kurulu”na ait düzenleme yeniden metne alınmıştır. Tartışmalar daha ziyade 8. maddede yer alan katalog suçlarının hangi suç türlerinden oluşması gerektiği noktasında ve Türkiye’de ve yurtdışında barındırılan içeriklerin kaldırılması veya engellenmesi konularında yoğunlaşmıştır. Ayrıca, 5187 sayılı Basın Kanunu’ndan ilham ile düzenlenen içeriğin yayından çıkarılması ve cevap hakkına ilişkin hükümler de eleştiri konusu olmuştur (TBMM, 2007c: 68-86).

Genel Kurul görüşmelerinde Tasarı hakkında ilk konuşmayı CHP Grubu adına Feridun Ayvazoğlu yapmıştır. Ayvazoğlu, Parti olarak aileyi ve özellikle çocukları İnternetin zararlarından korumaya yönelik bu düzenlemeyi özünde desteklediklerini,

⁹⁷ Şen, ilk hükümet tasarısına göre görevin BTK bünyesinde yeni kurulacak “Bilişim Güvenliği Başkanlığı”na verilmesine rağmen daha sonra TİB’de bunun altyapısının bulunduğu, tekrar bir emek ve masraf yapılmasının doğru olmayacağı düşüncesiyle görevin TİB’inde kurulacak İnternet Dairesi’ne tevdi edildiğini belirtmektedir (Osman N. Şen ile kişisel iletişim, 06.08.2013).

ancak, katalog suçların yetersiz olduğunu, bu suçlar arasına TCK'nun 302. md.'sinde yer alan vatanın toprak bütünlüğünün bölünmesine ilişkin suçlarla, İnkılap Kanunlarına muhalefet suçlarının da eklenmesi gerektiğini belirtmiştir (TBMM, 2007c:70). Ayvazoğlu, yeni katalog suçları önerirken "YouTube" da yer alan ve basına yansıyan Atatürk'e hakaret videolarını ve "Google Earth, Diyarbakır'ı Kuzey Kürdistan'ın başkenti yaptı" şeklindeki haberleri örnek göstermiş ve Google için kullanılan "küstah motor" manşetlerini hatırlatmıştır (TBMM, 2007c: 69).

Daha sonra AK Parti Grubu adına konuşan Gülseren Topuz, düzenlemeye neden ihtiyaç duyulduğunu genel gerekçeden alıntılar yaparak açıkladıktan sonra, Tasarı hakkında ana hatları ile bilgi vermiş ve ülke olarak kamu kurumları, STK'ları, akademisyenler, bilişim çevreleri ve özel sektör kuruluşları ile birlikte, önemli bir problem haline gelmiş bulunan bilişim suçları ve İnternet'in zararlı içeriklerinden ve yayınlardan korunması için önlemler geliştirdiklerini; Hükümet olarak amaçlarının "Temiz İnternet, temiz toplum" olduğunu dile getirmiştir (TBMM, 2007c: 72-74).

Tasarı hakkında şahsı adına söz alan ve CHP milletvekili Mevlüt Aslanoğlu konuşmasına başlarken yaşadığı bir olaydan hareketle İnternet ortamında kişilik haklarına, insan onuruna, şeref ve haysiyetine yapılan saldırılara karşı cezai yaptırımın yetersiz olduğuna vurgu yapmış ve gizli numaradan aramalarla ilgili şikayetleri dile getirmiştir (TBMM, 2007c: 74-75). Böylece Tasarı'nın tümü üzerindeki görüşmeler tamamlanmış ve maddelerinin görüşülmesine geçilmiştir.

Tasarı'nın "amaç ve kapsam" başlıklı 1. maddesiyle ilgili olarak CHP Grubu adına Osman Coşkunoglu söz alarak önce İnternetin öneminden, denetlenmesi ve kontrolündeki teknik zorluklardan, İnterneti kontrol etmeye çalışırken sansüre kapı açılması tehlikesinden, bu alanda yasal düzenlemeler yerine sivil toplumu harekete geçirecek ve eğitimli toplum haline getirecek çalışmalara ağırlık verilmesi gerektiğinden bahsetmiştir. Daha sonra, 2006 yılında Adalet Bakanlığı'nın hazırladığı yasa taslağına atıfta bulunarak, bu Taslağın daha kapsamlı ve STK'larca da üzerinde çalışılan, daha olgun bir metin haline getirildikten sonra, onun yerine bu

kısa ve kamuoyunca yeterince tartışılmamış bir Tasarı'nın Meclis gündemine getirilmesine yönelik eleştirisini dile getirmiştir (TBMM, 2007c: 75-77).

Tasarı'nın 1. maddesi bu konuşmadan sonra oylanmış ve kabul edilmiştir. Tasarı'nın bundan sonra gelen altı maddesi hakkında konuşma talebi olmadığı için maddeler üzerinde oylamaya geçilmiş ve maddeler kabul edilmiştir (TBMM, 2007c: 77-78).

Tasarı'nın katalog suçlarını düzenleyen 8. maddesi üzerinde CHP Grubu adına Coşkunoglu söz alarak, bu maddenin 4. fıkrasıyla TİB'e verilen resen engelleme yetkisini eleştirmiş, bunun sakıncalarından ve bir bütün olarak sitenin kapatılması yerine ilgili içeriğin çıkartılmasını sağlamaya çalışmak gerektiğinden bahsetmiştir. Benzer şekilde, 6. fıkrada yer alan, TİB'nin engellenme kararının konusunu oluşturan yayını yapanların kimliklerinin tespiti halinde Cumhuriyet başsavcılığına suç duyurusunda bulunabilme yetkisini de eleştirmiş ve TİB'na kimlik belirleme yetkisinin verilmesinin sakınca doğuracağını belirtmiştir (TBMM, 2007c: 79-80).

Müzakerenin bu aşamasında CHP'li Ayvazoğlu ve arkadaşlarınca katalog suçlarını düzenleyen 8. maddenin 1. fıkrasına “Devletin birliğini ve ülke bütünlüğünü bozmak (md.302)” ve “Anayasanın 174. md.’sinde belirtilen İnkılap Kanunlarının Korunması kapsamında yer alan suçlar” adıyla iki yeni suç türünün daha eklenmesi için önerge verilmiş ve önerge reddedilmiştir. Ayvazoğlu, önergenin gerekçesinde, bu iki maddenin öneminden bahsederek, Tasarı'nın geneli hakkında yaptığı konuşmada konuyla ilgili dile getirdiği hususları burada tekrarlamıştır (TBMM, 2007c:81).

Tasarının “İçeriğin yayından çıkarılması ve cevap hakkı” maddesi görüşülürken CHP adına konuşan Coşkunoglu, bu maddenin Tasarı'ya Komisyon'da eklendiğini fakat, İnternette işlenen belli suçlar için düzenlen bu yasada bu düzenlemenin yerinin olmadığını savunmuştur. Coşkunoglu, İnternette birisine hakaret etmenin zaten suç olduğunu; suçta cevap ve düzeltme hakkına ihtiyaç duyulmasının mümkün olamayacağını, bu düzenlenmenin İnterneti bu yolla sınırlama ve engelleme yöntemi olarak kullanılabileceği kaygısını dile getirmiştir. Keza, İnternet'in, sadece basın yayın faaliyeti olarak algılanmasının yanlış olacağına; bu nedenle, basın yayın

faaliyeti ile ilgisi olmayan birçok İnternet sitesinde, cevap ve düzeltme metni ile karşılaşılması gibi garip bir durumun ortaya çıkacağı ve basın yayın faaliyeti yapmayan kişilerin, sahibi oldukları İnternet siteleri nedeniyle basın yayın kuruluşlarını ilgilendiren bir sorumluluğa tabi tutulacaklarını ifade etmiştir. Yapılan oylama sonucu 9. madde mevcut hali ile kabul edilmiştir (TBMM, 2007c: 82).

Meclis görüşmelerinde “İdari yapı ve görevler” başlıklı 10. maddenin görüşülmesine geçildiğinde Tasarı’nın ilk metninde bulunup, Adalet Komisyonu’nda çıkartılan İnternet Kurulu’na ilişkin düzenlemenin tekrar metne eklenmesi için önerge verilmiş ve önergeler oylanarak kabul edilmiştir. Böylece izleme, filtreleme ve sakıncalı İnternet içeriğine erişimin engellenmesi konularında politika belirleyecek yeni bir İnternet Kurulu’nun oluşturulmasına karar verilmiş ve 10. maddesinin 5. fıkrasına bu yönde bir hüküm eklenmiştir. Madde üzerinde söz talebi olmadığı için bu yeni hali ile 10. madde oylanarak kabul edilmiştir. Daha sonra Tasarı’nın geri kalan maddeleri ile tümü Genel Kurul’da oylanarak kabul edilmiştir (TBMM, 2007c: 82).

Tasarı’nın Genel Kurulda kabulünden sonra teşekkür konuşması yapan Ulaştırma Bakanı Binali Yıldırım; Yasa’nın İnternet’i cezalandırma değil İnternet yoluyla işlenebilecek, çocuklarımıza, gençlerimize, aile yapımıza yönelik suçların önlenmesini amaçladığını belirtmiş ve İnternet’in milyonlarca yararı karşısında bazı olumsuz yan etkilerini önlemeye yönelik ilk tedbir ve düzenleme olduğunu, bu açıdan Türkiye’nin bu konuda yasal önlem alan altıncı ülke olduğunu dile getirmiştir. Komisyonlarda veya Hükümette hazırlıkları devam eden bilişim suçları, bilişim güvenliği ve verilerin korunmasıyla ilgili üç farklı kanun tasarısının yasalaşması ile bu tedbirlerin tamamlanmış olacağını ifade etmiştir (TBMM, 2007c: 82).

Yıldırım, Tasarı’nın “İçeriğin yayından çıkarılması ve cevap hakkı” başlıklı 9. maddesiyle ilgili olarak, bu maddenin, tüm diğer yayın türlerinde olduğu gibi, İnternet yoluyla yapılan yayında da, yayından mağdur olanın şikayet hakkı olması ve düzeltme talep edebilmesi için Yasa metnine dahil edildiğini belirtmiştir. Bu nedenle bunun bir sansür gibi, engelleme veya İnternetin gelişmesini önlemeye yönelik bir düzenleme olarak görülmemesi gerektiğini dile getirmiştir (TBMM, 2007c: 86).

04.05.2007 tarihli TBMM Genel Kurulu'nda kabul edilen Tasarı, ülkede yaşanan tüm seçim kargaşasına rağmen 5651 sayılı “İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun” olarak, 23.05.2007 tarih ve 26530 sayılı Resmi Gazete’de yayımlanarak yürürlüğe girmiştir. Böylece Türkiye, münhasıran İnternet içeriğinin düzenlenmesini öngören yeni bir kanuna kavuşmuştur.

Tasarı'nın Meclis müzakereleri, Yasanın okunması da dahil, 105 dk. gibi oldukça kısa bir sürede tamamlanmıştır. Görüşmelerde yapılan tüm konuşmaların yer aldığı tutanaklar toplamda 18 sayfaya ulaşabilmiştir. Tutanakların bir kısmını Tasarı'nın bizzat kendi metninin oluşturduğu ve Tasarıyla ilgili söz alan bazı hatiplerin konu dışı konuşmalar da yaptığı dikkate alınırsa,⁹⁸ Tasarı'nın içeriğine ilişkin görüşmelerin gerçekte çok daha kısa olduğu görülmektedir (TBMM, 2007c:68-86).

5651 sayılı Yasa'nın, yasalaşma süreci oldukça hızlı olmuştur. 2007'nin ilk aylarında Ulaştırma Bakanlığınca hazırlanan Tasarı, 12.02.2007'de TBMM'ye sunulmuş, 15.02.2007'de Adalet Komisyonu'na gönderilmiş, 28.02.2007'de Alt Komisyon'a havale edilmiş ve 30.03.2007'de Alt Komisyon'dan çıkmış, 04.05.2007'de Genel Kurul gündemine alınmış ve iki saati bulmayan bir sürede müzakere edilerek kabul edilmiştir. Hazırlıkları ile birlikte yasalaşma sürecinin toplam süresi beş aydır.

Bu nedenle 5651 sayılı Yasa ile ilgili olarak, aceleyle hareket edildiği, bir olubittiye getirildiği; bu yüzden ilgili çevrelerce ve kamuoyunca yeterince tartışılmadığı, tartışılan ve üzerinde az çok uzlaşılan Adalet Bakanlığı Taslağı yerine neden 5651'e kaynaklık oluşturan Yasa Tasarısı'nın tercih edildiği eleştirileri gündeme getirilmektedir. Bu eleştirilerin özellikle sürecin TBMM aşamasına ilişkin kısmı için haklılık payının bulunduğu kabul edilmelidir. Fakat, Yasa'nın fikir olarak ortaya çıkması ve sonrasında yaşananlara ait yukarıda detaylı olarak anlatılan sürecin geneli için bu eleştirilerin büyük oranda geçersiz olduğu iddia edilebilir.

⁹⁸ Örneğin Feridun Ayvazoğlu'nun, CHP Grubu adına Tasarı'nın tümü üzerindeki konuşması tutanaklardan incelendiğinde, konuşmacının toplamda 5,5 sayfa olan konuşma dökümlerinin 3 sayfasının Tasarı dışı güncel politik tartışmalardan oluştuğu görülmektedir (TBMM, 2007c: 68-73).

İlk olarak, İnternet kullanımının özellikle çocuklar ve gençler arasında giderek yaygınlaşmasıyla birlikte, çocuk istismarı ve müstehcenlik gibi zararlı içeriklere erişimin kolaylaşması, İnternet üzerinden işlenen suçların artması ve İnternet kafelerde yaşanan olumsuzluklar 2006 Türkiye'sinde bunlara ilişkin önlem alınmasına yönelik güçlü bir kamuoyu baskısı ve beklentisi oluşturmuştur. Bu durum, ailenin, çocukların ve gençlerin korunması için bu alanda önleyici yasal düzenleme yapılmasını zorunlu kılmıştır. Nitekim, dönemin anamuhalefet partisi olan CHP sözcülerinin de bu girişimi açıkça destekledikleri görülmektedir. bu çerçevede, 2005'ten itibaren İnternet kaynaklı olarak ortaya çıkan olumsuzluklar, bunlara ilişkin neler yapılabileceği, yasal düzenleme ihtiyacı, bu düzenlemenin şekli, kapsamı, konuları, nasıl yapılacağı gibi hususlar Türkiye'nin ve konunun tarafı olan herkesin gündeminde yer almış ve tartışılmıştır.

İkinci olarak, bu dönemsel şartlar altında söz konusu ihtiyacı karşılamak için yasal düzenlemeye temel teşkil eden üç farklı metin ortaya çıkmıştır. Bunlardan ilki, Adalet Bakanlığı'nın hazırladığı fakat üniversiteler, mahkemeler, ilgili bakanlıklar, barolar ve konuyla ilgili STK'larla paylaştığı ve tartışmaya açarak son şeklini verdiği, içerisinde hem bilişim suçlarına hem de zararlı içeriklere ilişkin düzenlemelerin bulunduğu tasarıdır. Bu tasarıda zararlı içerikle ilgili olarak sadece çocuk pornografisi ile devletin güvenliğine ve kamu barışına karşı işlenen suçlara ilişkin içerikler metinde yer almıştır.

Konumuz açısından asıl dikkat edilmesi gereken husus ise, tasarıdaki içerik, yer, erişim ve toplu kullanım sağlayıcıların sorumluluklarına ilişkin yapılan düzenlemeler ile içeriklere ilişkin “düzeltme ve cevap hakkı” getiren hükümlerdir. Konunun tarafı olan kişi ve kuruluşlarca tartışılarak ve üzerinde çalışılarak oluşturulan Adalet Bakanlığı tasarısında bu iki konuya ilişkin yapılan düzenlemeler büyük oranda 5651 sayılı Yasa'ya taşınmıştır. Zira, söz konusu Yasa'nın katalog suçları ve idari yapıyı düzenleyen bölümleri haricindeki kısımları genel olarak Adalet Bakanlığı'nın taslağından meydana getirilmiştir. Yani, her ne kadar 5651 sayılı Yasa çok fazla tartışılmadan hızlı bir şekilde yasalaşmış olsa da, Yasa'ya kaynaklık yapan metin

tartışılmış ve belli bir uzlaşa ile oluşturulmuştur. Dolayısıyla, 5651 sayılı Yasa'nın kamuoyunca yeterince tartışılmadığı eleştirisi çokta haklı gözükmemektedir.

Eleştirilere ilişkin diğer bir nokta ise, konunun bilgi toplumu çalışmaları ve bu bağlamda e-Dönüşüm Türkiye Projesi'yle ilgili olan yönüdür. Daha önce de belirtildiği gibi, 5651 sayılı Yasa'nın köklerini, bu Proje kapsamında oluşturulan 2006-2010 Bilgi Toplumu Strateji Belgesi ve Eylem Planı'nda bulmak mümkündür. İnternetin içerik ve kullanım güvenliğine ilişkin boyutları da dahil, ülkenin İnternet politikalarının temel referans belgesi olan bu metinlerde, güvenli bir İnternet ortamının oluşturulması için gerekli tedbirlerin alınması ve İnternet üzerinde çeşitli denetim ve yasakların düzenlenmesinin gerekliliği yer almıştır.

Bu belgelerin hazırlanmasında görev alan e-Dönüşüm İcra Kurulu ve Danışma Kurulu'nda konuyla ilgili STK'larının, sektör temsilcilerinin ve akademisyenlerin bulunduğu bilinmektedir. O halde bahsi geçen konuların bu platformlarda konuşulup tartışıldıktan sonra bu belgelere geçirildiği söylenilebilir. Yani, Yasa'da bulunan düzenlemelere ilişkin hususların çok önceden tartışma alanına girmiş, tartışılmış ve çözüm noktasında belli bir karara varılarak bu temel referans belgelerine girmiş olduğunu iddia etmek yanlış olmayacaktır.

Eleştirilere ilişkin son bir nokta ise, Adalet Bakanlığı yerine neden Ulaştırma Bakanlığı Taslağının tercih edildiğiyle ilgilidir. Adalet Bakanlığı Tasarısının görüşüldüğü Komisyon çalışmalarına bir yıl süreyle katılan Şen, Ulaştırma Bakanlığı teklifinin yasalaşmasında; tasarının bilişim suçlarını kapsayan geniş kapsamlı bir metin olması nedeniyle Adalet Bakanlığı Komisyon çalışmalarının uzaması, konuyla ilgili infial uyandıran bazı olayların arka arkaya gelmesi dolayısıyla Başbakan'ın bir an önce sonuç alınmasını istemesinin etkili olduğunu belirtmektedir. Keza, Ulaştırma Bakanı'nın bu alanla ilgilenmesi, konuya sahip çıkması ve pratikliğinin de önemli bir faktör olduğunu dile getirmektedir (Osman N. Şen ile kişisel iletişim, 06.08.2013).

Tüm bu değerlendirmeler, 5651 sayılı Yasa konularının, düzenleme çalışmalarının ve bu çalışmalarla ortaya çıkan metinlerin bir süredir tartışıldığını ve çözüme ilişkin

olarak belirli tedbirlerde anlaşma sağlandığını göstermektedir. Bu bağlamda bahsi geçen Yasa'nın, tam istenildiği gibi olmasa da, büyük oranda tüm bu tartışma ve çalışmaların bir sonucu olarak ortaya çıktığı söylenebilir. Yani, Yasa üç-beş ay gibi kısa bir süre içerisinde ortaya çıkıp karar verilerek sonuçlandırılmış olsa da, öncesi ve arkaplanı vardır.

Fakat, Tasarı metni belirginleştikten sonra, özellikle katalog suçları, öngörülen idari yapı ve erişim engellemeye ilişkin usul ve esaslarla ilgili olan maddelerin kamuoyunca daha geniş bir zaman diliminde tartışılması, tüm tarafların görüş ve önerilerinin alınmasını sağlayacak mekanizmaların işletilerek en geniş uzlaşısı ile TBMM Genel Kurulu'na getirilmesinin daha doğru ve sağlıklı olacağı da açıktır.

3.3 5651 SAYILI KANUN VE TİB SONRASI

Türkiye'nin İnternet tarihinde 5651 sayılı Kanun bir milat sayılabilir. İçerik düzenlemesi konusuna özgü olarak hazırlanan bu Kanun getirdiği yeni hükümler, yasadışı içerik olarak tanımladığı katalog suçları, Kanun'a dayalı olarak çıkarılan yönetmelikler ve tüm bunların uygulamaları ile bu uygulamaların içinde yer alan ilgili kamu kurumları açısından yeni bir dönemi başlatmıştır.

3.3.1 5651 Sayılı Kanun Sonrası Oluşan Hukuki Çerçeve

5651 sayılı Kanun getirdiği hükümler ve yapılan ikincil düzenlemeler Türkiye'de İnternet içerik düzenlemesiyle ilgili yeni bir hukuksal çerçeve oluşmuştur. Aynı zamanda İnternet aktörlerine ilişkin özel düzenleme olma özelliğini de taşıyan 5651 sayılı Kanun, konusu suç teşkil eden yayınlarla mücadelede İnternet aktörlerinin belirlenmesi yoluna gitmiş ve bu aktörlere getirilen yükümlülükler ile mücadele yöntemini belirlemiştir. Kanun, bu kapsamda söz konusu İnternet aktörleri ile işbirliğini öngörürken, İnternet hizmetlerinin kalitesinin arttırılmasını da hedeflemektedir (İnternet Daire Başkanlığı, 2008: 11,15). Bu hukuksal çerçevenin daha iyi anlaşılması için 5651 sayılı Kanun'un, katalog suçlarının ve konuyla ilgili söz konusu ikincil düzenlemelerin detaylı olarak incelenmesi gerekmektedir.

3.3.1.1 5651 Sayılı Kanun'un Getirdiği Hükümler

5651 sayılı Kanun; Anayasa'nın, özel olarak korunmasını öngördüğü, başta aile, çocuklar ve gençler olmak üzere belirli sosyal kesimlere yönelik suçların kolayca işlenmesini önleyici özel bir düzenleme mahiyetindedir. Kanun ile yeni bilişim suçları türleri oluşturulmamakta, yeni cezai ve idari yaptırımlar getirilmemektedir. Keza düzenleme ile, TCK ve bir özel yasada yer alan belirli suçların İnternet ortamındaki olumsuz etkilerinin önlenmesi için idari ve yargısal koruma tedbiri olarak iki çeşit yöntem öngörülmektedir. Kanun ile içerik denetiminin nasıl ve hangi kurum tarafından yapılacağına ilişkin düzenlemeler yapılmıştır.

5651 sayılı Kanun biri geçici olmak üzere 14 maddeden oluşmaktadır. Kanun'un "amacı ve kapsamı" 1. maddede; içerik, yer, erişim ve toplu kullanım sağlayıcıların yükümlülük ve sorumluluklarını düzenlemek ve bahse konu sağlayıcılar marifetiyle İnternet ortamında işlenen belirli suçlarla mücadelenin esas ve usullerini belirlemek olarak ifade edilmiştir.

Kanun'un "Tanımlar" alt başlığını taşıyan 2. maddesi; içerik, yer, erişim ve toplu kullanım sağlayıcılar ile trafik bilgisi, bilgi, izleme, erişim, veri, İnternet ortamı ve İnternet ortamında yapılan yayın gibi Yasa metninde geçen kavramların tanımlamalarına yer vermiştir.

Kanun'un "Bilgilendirme yükümlülüğü" alt başlığını taşıyan 3. maddesi ile içerik, yer, erişim ve toplu kullanım sağlayıcılarına bilgilendirme yükümlülüğü getirilmiştir. Buna göre, içerik, yer ve erişim sağlayıcılar, yönetmelikle belirlenecek olan esas ve usuller çerçevesinde tanıtıcı bilgilerini kendilerine ait İnternet ortamında kullanıcıların ulaşabileceği şekilde ve güncel olarak bulundurmakla yükümlü tutulmuşlardır. 3. maddenin 2. fıkrası, bu yükümlülüğü yerine getirmeyenlere ilişkin olarak TİB tarafından ikibin Yeni Türk Lirasından onbin Yeni Türk Lirasına kadar idari para cezası verilebilmesini öngörmüştür.

Kanun'a göre içerik sağlayıcı "İnternet ortamı üzerinden kullanıcılara sunulan her türlü bilgi veya veriyi üreten, değiştiren ve sağlayan gerçek veya tüzel kişiler"dir. 4.

madde, içerik sağlayıcının “kullanıma sunduğu her türlü içerikten sorumlu olduğunu”, fakat “bağlantı sağladığı başkasına ait içerikten” sorumlu tutulamayacağını düzenlemiştir. Ancak, “sunuş biçiminden, bağlantı sağladığı içeriği benimsediği ve kullanıcının söz konusu içeriğe ulaşmasını amaçladığı açıkça belli ise, genel hükümlere göre sorumludur”.

Kanun’da “Hizmet ve içerikleri barındıran sistemleri sağlayan veya işleten gerçek veya tüzel kişileri” ifade eden yer sağlayıcıların yükümlülükleri 5. maddede düzenlenmiştir. Buna göre, yer sağlayıcıların “yer sağladığı içeriği kontrol etmek” veya “hukuka aykırı bir faaliyetin söz konusu olup olmadığını araştırmakla” yükümlü olmadıkları belirtilmiştir. Fakat, yer sağladıkları hukuka aykırı içerikten, “Erişimin engellenmesi kararı ve yerine getirilmesi” konusunu düzenleyen 8. ve “İçeriğin yayından çıkarılması ve cevap hakkı” konusunu düzenleyen 9. maddelere göre “haberdar edilmeleri halinde” ve “teknik olarak imkan bulunduğu ölçüde” yayından kaldırmakla yükümlüdürler.

Kanun’da “Kullanıcılarına İnternet ortamına erişim olanağı sağlayan her türlü gerçek veya tüzel kişiler” olarak tanımlanan erişim sağlayıcıların yükümlülükleri 6. maddede belirlenmiştir. Buna göre, erişim sağlayıcının erişim sağladığı içerikten dolayı, sadece bu sıfatı nedeniyle sorumlu tutulamayacağı hükme bağlanmıştır. Dolayısıyla, erişim sağlayıcı kendisinin aracılığıyla erişilen içeriklerin “hukuka aykırı olup olmadıklarını” ve “sorumluluğu gerektirip gerektirmediğini” kontrol etmekle yükümlü değildir. Fakat, herhangi bir kullanıcısının yayınladığı hukuka aykırı içerikten, bu Kanun’da yer alan hükümlere uygun olarak haberdar edilmesi durumunda ve teknik olarak engelleme imkanı bulunduğu ölçüde erişimi engellemekle yükümlüdür.

Bunun yanında erişim sağlayıcı, sağladığı hizmetlere ilişkin olarak; yönetmelikte belirtilen trafik bilgilerini⁹⁹ yine yönetmelikle altı aydan az ve iki yıldan fazla

⁹⁹ Tanımlar kısmında belirtildiğine göre trafik bilgisi “İnternet ortamında gerçekleştirilen her türlü erişime ilişkin olarak taraflar, zaman, süre, yararlanılan hizmetin türü, aktarılan veri miktarı ve bağlantı noktaları gibi değerleri” ifade etmektedir.

olmayacak şekilde belirlenecek süre kadar saklamakla ve bu bilgilerin “doğruluğunu, bütünlüğünü ve gizliliğini sağlamakla” yükümlüdür. Ayrıca, faaliyetine son vereceği tarihten en az üç ay önce durumu TK’na, içerik sağlayıcılarına ve müşterilerine bildirmekle ve trafik bilgilerine ilişkin kayıtları yönetmelikte belirlenecek usul ve esaslara göre bu Kurum’a teslim etmekle yükümlüdür. Trafik bilgilerini belirtilen şekilde saklamakla ilgili yükümlülüklerini veya faaliyetine son vermesi durumundaki yükümlülüklerden birisini yerine getirmeyen erişim sağlayıcısı, TİB tarafından onbin Yeni Türk Lirasından ellibin YTL’ye kadar idari para cezası ile cezalandırılır.

Kanun’da “Kişilere belli bir yerde ve belli bir süre İnternet ortamı kullanım olanağı sağlayan”ları ifade eden toplu kullanım sağlayıcıların yükümlülükleri 7. madde ile düzenlenmiştir. Kanun’da toplu kullanım sağlayıcıların “ticari olanlar” ve “ticari olmayanlar” şeklinde ikili bir ayrıma tabi tutularak yükümlülüklerinin farklılaştırıldığı görülmektedir. Buna göre ticari amaçla toplu kullanım sağlayıcıların denetimi mahalli mülki amirler tarafından yapılırken, aynı maddeden izin belgesi almaları yükümlülüğü getirilmiştir. Ayrıca, izne ilişkin bilgilerin otuz gün içinde mahalli mülki amir tarafından TK’na bildirilmesi de hükme bağlanırken, izin belgesinin verilmesine ve denetime ilişkin usul ve esasların yönetmelikle düzenleneceği belirtilmiştir. Keza, belirtilen yükümlülüklerini yerine getirmeyen ticari amaçla toplu kullanım sağlayıcılara, mahalli mülki amir tarafından üçbin Yeni Türk Lirasından onbeşbin Yeni Türk Lirasına kadar idari para cezası verilebilecektir. Kanun’a göre, ticari amaçla olup olmadığına bakılmaksızın tüm toplu kullanım sağlayıcıların, “konusu suç oluşturan içeriklere erişimi önleyici tedbirleri alma” yükümlülüğü bulunmaktadır.

Kanun’da 8. madde “Erişimin engellenmesi kararı ve yerine getirilmesi” başlığını taşımaktadır. Bu maddenin 1. fıkrasında katalog suçlar belirlenmiştir. Buna göre, “İnternet ortamında yapılan ve içeriği aşağıdaki suçları oluşturduğu hususunda yeterli şüphe sebebi bulunan yayınlarla ilgili olarak erişimin engellenmesine karar verilir” denilerek bu suçlar sayılmıştır. Söz konusu suçlar, 5237 sayılı TCK’nda yer alan “İntihara yönlendirme (madde 84)”, “Çocukların cinsel istismarı (madde 103, birinci fıkra)”, “Uyuşturucu veya uyarıcı madde kullanılmasını kolaylaştırma (madde

190)”, “Sağlık için tehlikeli madde temini (madde 194)”, “Müstehcenlik (madde 226)”, “Fuhuş (madde 227)”, “Kumar oynanması için yer ve imkan sağlama (madde 228)” ve “5816 sayılı Atatürk Aleyhine İşlenen Suçlar Hakkında Kanun’da yer alan suçlar” olarak belirlenmiştir.

8. maddenin sonraki kısmında ise erişim engellemesi kararının alınması ve yerine getirilmesi ile ilgili usul ve esaslar düzenlenmiştir. 2. fıkraya göre, erişimin engellenmesi kararı, “soruşturma evresinde hakim, kovuşturma evresinde mahkeme” tarafından verilir. Ayrıca, soruşturma safhasında, “gecikmesinde sakınca bulunan hallerde” Cumhuriyet savcısı tarafından da erişimin engellenmesi kararı verilebilir. Bu durumda Cumhuriyet savcısı kararını yirmidört saat içinde hakim onayına sunar. Hakim ise, kararını en geç yirmidört saat içinde verir. Bu süre içinde karar onaylanmazsa tedbir, Cumhuriyet savcısı tarafından derhal kaldırılır. Koruma tedbiri olarak verilen erişimin engellenmesi kararına karşı, Ceza Muhakemesi Kanunu hükümlerine göre itiraz edilebilir. 3. fıkra hakim, mahkeme veya Cumhuriyet savcısı tarafından verilen erişimin engellenmesi kararının birer örneğinin, gereği yapılmak üzere TİB’na gönderileceği belirtilmektedir.

4. fıkra, katalog suçlarını oluşturan yayınların içerik veya yer sağlayıcısının yurt dışında bulunması halinde Başkanlığa erişimin engellenmesi kararını re’sen verebilme yetkisi tanımaktadır. Yasa, içerik veya yer sağlayıcısı yurt içinde bulunsan bile, içeriği çocukların cinsel istismarı ve müstehcenlik suçlarını oluşturan yayınlara ilişkin olarak da Başkanlığa aynı yetkiyi vermiştir. Bu karar, erişim sağlayıcısına bildirilerek gereğinin yerine getirilmesi istenir. 5. fıkraya göre, “erişimin engellenmesi kararının gereği, derhal ve en geç kararın bildirilmesi anından itibaren yirmidört saat içinde” yerine getirilir.

6. fıkra, Başkanlık tarafından verilen erişimin engellenmesi kararının konusunu oluşturan yayınları yapanların kimliklerinin belirlenmesi durumunda, Başkanlık tarafından, Cumhuriyet başsavcılığına suç duyurusunda bulunacağı hükmünü getirmektedir. 7. fıkra, soruşturma sonucunda kovuşturmaya yer olmadığı kararı verilmesi durumunda, 8. fıkra kovuşturma evresinde beraat kararı verilmesi halinde,

erişimin engellenmesi kararının kendiliğinden hükümsüz kalacağını düzenlemiştir. Keza, her iki durumda da kararın bir örneğinin TİB’na göndermesi gerekmektedir.

9. fıkra, konusu katalog suçlarını oluşturan içeriğin yayından çıkarılması halinde; erişimin engellenmesi kararının, soruşturma evresinde Cumhuriyet savcısı, kovuşturma evresinde mahkeme tarafından kaldırılmasını hükme bağlamıştır. 10. fıkra, koruma tedbiri olarak verilen erişimin engellenmesi kararının gereğini yerine getirmeyen yer veya erişim sağlayıcılarının sorumlularına, “fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde”, altı aydan iki yıla kadar hapis cezası öngörmektedir.

11. fıkra, idari tedbir olarak verilen erişimin engellenmesi kararının yerine getirilmemesi halinde, TİB tarafından erişim sağlayıcısına, onbin Yeni Türk Lirasından yüzbin Yeni Türk Lirasına kadar idari para cezası verilmesini; idari para cezasının verilmesine rağmen yirmidört saat içinde kararın yerine getirilmemesi halinde ise TİB’in talebi üzerine TK tarafından yetkilendirmenin iptaline karar verilmesini hüküm altına almıştır.

12. fıkraya göre, bu Kanun’da tanımlanan kabahatler dolayısıyla TİB veya TK tarafından verilen idari para cezalarına ilişkin kararlara karşı, 2577 sayılı İdari Yargılama Usulü Kanunu hükümlerine göre kanun yoluna başvurulabilir. Ayrıca, daha sonra çıkarılan 5809 sayılı Elektronik Haberleşme Kanunu’nun 67. maddesine göre, işlemlerin yürütülmesi için Başkanlığa gönderilen hakim ve mahkeme kararlarına 5271 sayılı Ceza Muhakemesi Kanunu hükümlerine göre Başkanlıkça itiraz edilebileceği hükmü getirilmiştir.

Kanun’un 9. maddesi “İçeriğin yayından çıkarılması ve cevap hakkı” başlığını taşımaktadır. 9. madde 1. fıkrasıyla, içerik nedeniyle haklarının ihlal edildiğini iddia eden kişilere, içerik sağlayıcısına, ulaşamaması halinde yer sağlayıcısına başvurarak kendisine ilişkin içeriğin yayından çıkarılmasını ve yayındaki kapsamından fazla olmamak üzere hazırladığı cevabı bir hafta süreyle İnternet ortamında yayımlanmasını isteyebilme hakkı getirmektedir. Bunun yanında içerik veya yer

sağlayıcıya bu tip talepleri ulaştığı tarihten itibaren iki gün içinde yerine getirme zorunluluğu getirmiştir. Bu sürede yerine getirilmeyen talep reddedilmiş sayılır.

2. fıkra talebin reddedilmiş sayılması halini düzenlemektedir. Buna göre, talebi reddedilmiş sayılan kişi, onbeş gün içinde yerleşim yeri sulh ceza mahkemesine başvurarak, içeriğin yayından çıkarılmasına ve yayındaki kapsamından fazla olmamak üzere hazırladığı cevabın bir hafta süreyle İnternet ortamında yayımlanmasına karar verilmesini isteyebilir. Bu durumda sulh ceza hakimi bu talebi üç gün içinde duruşma yapmaksızın karara bağlar. Sulh ceza hakiminin kararına karşı Ceza Muhakemesi Kanunu hükümlerine göre itiraz yolu açıktır.

3. fıkra, sulh ceza hakiminin kesinleşen kararının, 1. fıkraya göre yapılan başvuruyu yerine getirmeyen içerik veya yer sağlayıcısına tebliğinden itibaren iki gün içinde içeriğin yayından çıkarılarak hazırlanan cevabın yayımlanmasını düzenlemektedir. 4. fıkra ise, sulh ceza hakiminin kararını bu maddede belirtilen şartlara uygun olarak ve süresinde yerine getirmeyen sorumlu kişiler için altı aydan iki yıla kadar hapis cezası öngörmektedir. Ayrıca, içerik veya yer sağlayıcının tüzel kişi olması durumunda, bu fıkra hükmünün yayın sorumlusu hakkında uygulanacağı belirtilmiştir.

Kanun'un 10. maddesi ise, Kanun'la sınırları çizilen içerik düzenlemesiyle ilgili idari yapıyı, sorumlu kamu kurumunu ve görevlerini belirlemektedir. Buna göre, 1. fıkra ile bu konuda Kanun'la verilen görevleri yerine getirmek üzere, TK bünyesinde bulunan TİB görevlendirilmiştir. 2. fıkra ile de TİB'na görevlerini yerine getirmede kullanacağı yeni personel kadroları ihdas edilmiştir.

3. fıkra ile TİB'na görevlerine ilişkin olarak yapacağı mal veya hizmet alımlarında bazı ayrıcalıklar getirilmiştir. Buna göre, her türlü mal ve hizmet alımlarında, ceza ve ihalelerden yasaklama işleri hariç, 4734 sayılı Kamu İhale Kanunu ile 4735 sayılı Kamu İhale Sözleşmeleri Kanunu hükümlerinden muafiyet tanınmıştır.

4. fıkra'da Başkanlığın görev ve yetkileri sayılmıştır. Buna göre, Kanun'larla verilen diğer yetki ve görevleri saklı kalmak şartıyla, Başkanlığın bu Kanun kapsamındaki görev ve yetkileri şöyle sıralanmıştır:

- a) Bakanlık, kolluk kuvvetleri, ilgili kamu kurum ve kuruluşları ile içerik, yer ve erişim sağlayıcılar ve ilgili STK'ları arasında koordinasyon oluşturarak, İnternet ortamında katalog suçlarını oluşturan içeriğe sahip faaliyet ve yayınları önlemeye yönelik çalışmalar yapmak. Bu amaçla, gerektiğinde, her türlü giderleri TK'nca karşılanacak çalışma kurulları oluşturmak.
- b) İnternet ortamında yapılan yayınların içeriklerini izleyerek, katalog suçların işlendiğinin tespit edilmesi halinde, bu yayınlara erişimin engellenmesi için bu Kanun'da öngörülen gerekli tedbirleri almak.
- c) İnternet ortamında yapılan yayınların içeriklerinin izlenmesinin hangi seviye, zaman ve şekilde yapılacağını belirlemek.
- ç) TK'ca işletmecilerin yetkilendirilmeleri ile mülki idare amirlerince ticari amaçlı toplu kullanım sağlayıcılara verilecek izin belgelerinde filtreleme ve bloke etmede kullanılacak sistemlere, yapılacak düzenlemelere ilişkin usul ve esasları belirlemek.
- d) İnternet ortamındaki yayınların izlenmesi suretiyle katalog suçların işlenmesini önlemek için izleme ve bilgi ihbar merkezi dahil, gerekli her türlü teknik altyapıyı kurmak veya kurdurmak, bu altyapıyı işletmek veya işletilmesini sağlamak.
- e) İnternet ortamında herkese açık çeşitli servislerde yapılacak filtreleme, perdeleme ve izleme esaslarına göre donanım üretilmesi veya yazılım yapılmasına yönelik asgari kriterleri belirlemek.
- f) Bilişim ve İnternet alanındaki uluslararası kurum ve kuruluşlarla işbirliği ve koordinasyonu sağlamak.
- g) Katalog suçların, İnternet ortamında işlenmesini konu alan her türlü temsili görüntü, yazı veya sesleri içeren ürünlerin tanıtımı, ülkeye sokulması, bulundurulması, kiraya verilmesi veya satışının önlenmesini temin etmek için yetkili ve görevli kolluk kuvvetleri ile soruşturma mercilerine, teknik imkanları dahilinde gereken her türlü yardımda bulunmak ve koordinasyonu sağlamak.

Kanun'da 10. maddenin 5. fıkrası ile, yeni İnternet Kurulu'na ilişkin düzenlemeler yapılmıştır. Buna göre, Ulaştırma Bakanlığı'nın 3348 sayılı Kanunun ek 1. maddesi uyarınca, Adalet Bakanlığı, İçişleri Bakanlığı, çocuk, kadın ve aileden sorumlu Devlet Bakanlığı ile Kurum ve ihtiyaç duyulan diğer bakanlık, kamu kurum ve kuruluşları ile İSS'lar ve ilgili STK'ları arasından seçilecek bir temsilcinin katılımıyla bir İnternet Kurulu oluşturulması öngörülmüştür. Başkanlığa bu Kurul ile gerekli "işbirliği ve koordinasyonu sağlama"; bu Kurul'ca "izleme, filtreleme ve engelleme yapılacak içeriği haiz yayınların tespiti ve benzeri konularda yapılacak öneriler ile ilgili gerekli her türlü tedbir veya kararları alma" görevi verilmiştir.

Kanun'un 11. maddesi, Kanun'da belirtilen konuların uygulamasına ilişkin yönetmeliklerin çıkartılmasıyla ilgili düzenlemeleri içermektedir. Daha sonra 05.11.2008 tarihli 5809 sayılı Elektronik Haberleşme Kanunu'nun 67. maddesiyle 5651 sayılı Kanun'a bazı ek maddeler ilave edilmiştir. Bu yeni düzenlemeler genel olarak yeni personel kadrosu ihdasları ile personel alımı ve ataması, yeni kadro unvanları ve tahsisleri, mevcut ve yeni personel için kariyerlik sisteminin düzenlenmesi gibi personel iş ve işlemlerine dair konulara ilişkindir.

3.3.1.2 Katalog Suçlarına İlişkin Yasalar

5651 sayılı Kanun'un "Erişimin engellenmesi kararı ve yerine getirilmesi" başlığını taşıyan 8. maddesinin 1. fıkrasında katalog suçlar belirlenmiştir. Bu bölümde söz konusu Katalog suçların temelini oluşturan yasaların kapsamına değinilecektir.

3.3.1.2.1 İntihara Yönlendirme

İntihara yönlendirme suçu katalog suçları arasında yer almaktadır. 5651 sayılı Yasa'ya göre, 5237 sayılı TCK'nın 84. maddesinde yer alan intihara yönlendirme suçunun İnternet ortamında yapılan yayınlarla oluştuğu yönünde yeterli şüphe bulunması durumunda erişim engellenmesi kararı verilebilecektir.

Kişinin kasıtlı olarak hayatına son vermesi olarak tanımlanabilecek intiharın, "özendirilmesi" fiillerinin başka bir insanın hayatına saldırı niteliği taşıdığı kabul

edildiğinden, bu tür fiillerin cezasız kalmaması amacıyla, intihara yönlendirme şeklinde müstakil bir suç oluşturulmuş ve bu suç, 5237 sayılı TCK'nın 84. maddesinde yaptırıma bağlanmıştır (Kaya, 2010: 88).

Buna göre, bu maddenin 1. fıkrası ile başkasını intihara azmettiren, teşvik eden, baskasının intihar kararını kuvvetlendiren ya da baskasının intiharına herhangi bir şekilde yardım eden kişiler için iki yıldan beş yıla kadar hapis cezası öngörülmüştür. 2. fıkra, İntiharın gerçekleşmesi durumunda müeyyideyi ağırlaştırmış ve dört yıldan on yıla kadar hapis cezasına çıkarmıştır. 3. fıkra, bu fiile alenen teşvik eden kişiye ise, üç yıldan sekiz yıla kadar hapis cezası verileceğini hüküme bağlamıştır. Son fıkraya göre ise, işlediği fiilin anlam ve sonuçlarını algılama yeteneği gelişmemiş olan veya ortadan kaldırılan kişileri intihara yönlendirenlerle cebir veya tehdit kullanmak suretiyle kişileri intihara mecbur edenler, kasten adam öldürme suçundan sorumlu tutulurlar. Keza, bu hükümlere paralel olarak, 5187 sayılı Basın Kanunu'nun 20. maddesi intihar olayları hakkında haber vermenin sınırlarını aşan ve okuyucuyu bu tür fiillere özendirecek nitelikte yazı ve resim yayınlanmasını yasaklamıştır.

Birçok devlet intiharın önlenmesi ve özellikle gençliğin korunması için çeşitli düzenlemeler yapmakta ve bu tür içeriklerle mücadele etmektedir. Nitekim, Japonya ve Güney Kore, Gençlik Yasa'larında intihara yardım ve teşvik etmeyi zararlı içerik olarak kabul etmiş ve ülkelerinde erişim engelleme uygulamalarının temel gerekçelerinden birisi yapmıştır (Internet Hotline Centre Japan, 2013; OpenNet, 06.08.2012). Benzer şekilde, İtalya'da intihara yönlendirme, satanizm için insan ya da hayvan kurban etmek türü içerikler yasadışı olarak kabul edilmiştir (114.it, 2012; Stop-it, 2012). Yine, Rusya'da Roskomnadzor Kurumu'na içlerinde intihara teşvik içeriklerinin de dahil olduğu bazı içerikleri mahkeme kararı olmaksızın kara listeye alma ve erişimi engelleme yetkisi verilmiştir (Hürriyet, 01.11.2012). Keza, Bulgaristan intihar ve kendine zarar verme içeriklerini yasadışı kabul etmiş ve yasaklamıştır (Web112.net, 2010). Bu kapsamda, ikisi de INHOPE üyesi olan Almanya'daki Jugendschutz İhbar Merkezi ile Yunanistan'daki Safeline İnternet İhbar Merkezi, ülkede zararlı görüldüğü için intihara teşvik içerikleriyle ilgili ihbarları kabul etmektedirler (Jugendschutzlandesstellen.de, 2012; Safeline.gr, 2013).

İntihara yönlendirme suçuyla ilgili İnternet içeriğinin engellenmesini öngören 5651 sayılı Kanun'un 8. maddesi de bu doğrultuda hazırlanmıştır. Bu hüküm, gençliğin korunması için gereken tedbirleri alması için devlete sorumluluk yükleyen Anayasanın 58. maddesine dayanmaktadır (Kaya, 2010: 89-90).

3.3.1.2.2 Çocukların Cinsel İstismarı

Çocukların cinsel istismarı suçu da katalog suçları arasında yer almaktadır. Ailenin ve çocukların korunması temel amacıyla hazırlanan 5651 sayılı Kanun, bu suçu bir erişim engelleme sebebi olarak kabul etmiştir. Buna göre, 5237 sayılı TCK'nın 103. maddesinin 1. fıkrasında düzenlenen çocukların cinsel istismarı suçunun İnternet ortamında yapılan yayınlarla oluştuğu yönünde yeterli şüphe bulunması durumunda erişim engellenmesi kararı verilir.

5237 sayılı TCK'nın 6. maddesinde “çocuk”, “henüz on sekiz yaşını doldurmamış” kişi olarak tanımlanmıştır. 102. madde, erişkin kişilere karşı işlenen “cinsel davranışlarla bir kimsenin vücut dokunulmazlığını ihlal”i “cinsel saldırı”, 103. madde çocuklara karşı işlenen ihlalleri çocukların zayıflıklarını göz önüne bulundurarak “cinsel istismar” olarak nitelendirmiştir. Dolayısıyla, çocukların cinsel istismar suçunun oluşması için her durumda, mağdurun 18 yaşından küçük olması gerekmektedir. Aksi durumda çocukluk niteliği yitirileceği için “cinsel saldırı” suçu gündeme gelecektir. 103. madde çocuğu cinsel yönden istismar eden kişilere üç yıldan sekiz yıla kadar hapis cezası öngörmüştür.

103. madde cinsel istismar suçunu ikiye ayırarak düzenlemiştir. Birincisi, 15 yaşını tamamlamamış veya tamamlamış olmakla birlikte bu davranışların hukuki anlam ve sonuçlarını algılaya yeteneği gelişmemiş olan çocuklara karşı gerçekleştirilen her türlü cinsel davranıştır. Burada mağdur çocuğun rıza göstermesi veya fiillerin cinsel ilişki aşamasına varmamış olması suçun oluşmasını önlememektedir. İkincisi ise, 15 yaşını tamamlamış mağdur çocuğun cebir, tehdit, hile veya iradeyi etkileyen başkaca bir sebeple iradesinin zayıflatılarak cinsel davranışların gerçekleştirilmiş olmasıdır. İki durumda da, suçun oluşması için cinsel davranışın objektif olarak şehevi nitelikte

bulunması yeterli olup, failin şehvi arzularını fiilen tatmin edip etmemesinin ve failin veya mağdurun cinsiyetinin önemi bulunmamaktadır (Kaya, 2010: 92-93).

Çocuk istismarı ve çocuk pornografisi ile mücadele genel olarak tüm ülkelerin benimsediği bir konudur. Nitekim her iki konu da uluslararası sözleşmelere konu olmuştur. Bu bağlamda, çocukların korunmasına ilişkin temel uluslararası metin olan BM Çocuk Haklarına Dair Sözleşme Türkiye tarafından 14.09.1990 tarihinde imzalamış ve 27.01.1995 tarihinde yürürlüğe girmiştir. Buna göre, 18 yaşının altındaki tüm bireyler çocuk olarak kabul edilmektedir. Sözleşme, çocukların her türlü istismardan ve sömürüden korunma hakkını tanımış ve Sözleşme'yi kabul eden devletleri bunu sağlamaları için çocukların menfaatine en uygun yasal, idari, sosyal ve eğitimsel tedbirleri almakla yükümlü kılmıştır.

Bilahere çocukların cinsel istismarı ve sömürülmesi konusunda daha etkin olunması için BM, 25.05.2000 tarihinde Çocuk Haklarına Dair Sözleşmeye Ek Çocuk Satışı, Çocuk Fahişeliği ve Çocuk Pornografisi İle İlgili İhtiyari Protokol'ü kabul etmiştir. Türkiye bu Protokolü 08.09.2000 tarihinde imzalamış ve 28.06.2002 tarihinde yürürlüğe sokmuştur. Protokolün temel amacı çocuk satışı, çocuk fahişeliği ve çocuk pornografisini önlemektir. Bu çerçevede, Protokolü kabul eden devletlerin bu fiilleri iç hukuklarında suç olarak kabul etmeleri gerekmekte ve bu suçların tanımı, uluslararası işbirliği, devletlerin yargılama yetkisi, suçluların iadesi ve ceza yargılamasına ilişkin temel ilkeler gibi konuları düzenlemektedir.

Protokol, ülkemiz iç hukuku ve özellikle 5651 sayılı Kanun'un uygulaması açısından önem taşımaktadır. Bu bağlamda, çocuk pornografisi çocuğun cinsel amaçlı istismarı ve bunun ses, görüntü ve yazı ile temsil edilmesi şeklinde iki farklı suçu ortaya çıkarmaktadır. 5237 sayılı TCK'nın 103. maddesi çocuğun cinsel amaçlı istismarı fiilleriyle mücadeleye, 5651 sayılı Yasa da bu hükmün erişim engelleme sebebi olarak sayılması ile temsil sorunuyla mücadeleye hizmet etmektedir (Kaya, 2010:96).

3.3.1.2.3 Uyuşturucu veya Uyarıcı Madde Kullanılmasını Kolaylaştırma

Aileyi ve çocukları İnternetin zararlı içeriğinden korumak amacı ile çıkarılan 5651 sayılı Yasa kapsamında katalog suçlarından birisini de “uyuşturucu veya uyarıcı madde kullanılmasını kolaylaştırma” oluşturmaktadır. Buna göre, TCK’nın 190. maddesinde düzenlenen bu suçun İnternet ortamında yapılan yayınlarla oluştuğu yönünde yeterli şüphe bulunması durumunda erişim engellenmesi kararı verilebilir.

TCK’nın “Kamunun Sağlığına Karşı Suçlar” başlıklı Üçüncü Bölümü’nde 188. madde ile “Uyuşturucu veya uyarıcı madde imal ve ticareti”, 190. madde ile “Uyuşturucu veya uyarıcı madde kullanımını kolaylaştırma” ve 191. madde ile de “Kullanmak için uyuşturucu veya uyarıcı madde satın almak, kabul etmek veya bulundurmak” fiilleri suç olarak düzenlenmiştir.

TCK, uyuşturucu maddelerin neler olduğunu tanımlanmadığı gibi, bunların teker teker sayılması yoluna da gitmemiştir. Hangi maddelerin uyuşturucu madde sayılması gerektiği hususunun belirlenmesi Bakanlar Kurulu Kararnamesine bırakılmıştır. Böylece zaman içinde yeni ortaya çıkan ve uyuşturucu etkisi yapan maddelerin yaptırım dışı kalmasının önlenmesi hedeflenmiştir (TBMM, 2004).

Uyuşturucu veya uyarıcı madde kullanılmasını kolaylaştırmaktan kasıt, bu maddeleri kullanmak isteyen kişilerin bunlara ulaşmasını çabuklaştırmak ve bunu güvenilir hale getirmektir (Özmen, 2009: 51). TCK 190. md. bu fiilin üç şekilde işlenebileceğini belirleyerek cezai müeyyideye bağlamıştır. Buna göre, şu üç “kullanımı kolaylaştırmak” fiilini işleyen kişiye iki yıldan beş yıla kadar hapis cezası verilir: a) Uyuşturucu kullanımı için özel yer, donanım veya malzeme sağlamak, b) Uyuşturucu veya uyarıcı madde kullananların yakalanmalarını zorlaştırıcı önlemler almak, c) Uyuşturucu veya uyarıcı madde kullanma yöntemleri konusunda bilgi vermek.

Bu fiillerden “kullanma yöntemleri konusunda başkalarına bilgi vermek”ten maksatın, uyuşturucu veya uyarıcı maddenin nasıl kullanıma hazır hale getirileceği ya da ne şekilde vücuda zerk edileceği konusunda bilgi sağlamaktır. Yine, söz konusu maddelerin ne şekilde kullanılarak daha etkili olacağına yönelik bilgi vermek ya da tavsiyede bulunmak da bu kapsamda değerlendirilebilir (Özmen, 2009: 52).

TCK 190. madde, “özendirme” fiilini suç olarak düzenlemiştir. Özendirmekten kast, uyuşturucu ya da uyarıcı maddenin kullanılması konusunda muhatapları teşvik etmek, onları isteklendirmek ya da bu davranışta bulunmaları yönünde kışkırtmaktır (Özmen, 2009: 52). Düzenlemede, “özendirme” fiilinin “alenen özendirme” ve “bu nitelikte yayın yapma” olarak iki farklı şekilde işlenmesi mümkün görülmüş ve bu iki fiili işleyen kişiler için iki yıldan beş yıla kadar hapis cezası öngörülmüştür.

Bu kapsamda söz konusu maddenin özellikle “kullanılmasını kolaylaştırmak” fiillerinden “kullanma yöntemleri konusunda başkalarına bilgi vermek” ve “özendirme” fiillerinin İnternet ortamındaki yayınlarla işlenmesi mümkündür.

Uyuşturucuyla mücadele konusunda devletlerarası işbirliği sağlamak amacıyla kurulan en önemli iki kuruluş Interpol ve BM’e bağlı Uluslararası Narkotik Kontrol Kurulu (INCB) dur. INCB, uyuşturucu dahil olmak üzere her türlü yasadışı kimyasalın ve ilacın İnternet üzerinden satılmasını önlemek amacıyla; devletlerin bunu önlemek için gerekli mevzuat değişikliklerini yapmasını ve ülke çapında faaliyet gösteren servis sağlayıcıların bu tür içeriği barındırmasının engellenmesi önerilerinin de içerisinde yer aldığı tavsiye kararlar yayınlamıştır (INCB, 2009).

Nitekim, dünyada bir çok ülke bu konuda tedbir almaktadır. Avustralya’da ACMA, uyuşturucu kullanımını özendiren içeriklerle mücadele etmektedir. Bu kapsamda, bu tür içerikler yurtiçinde barındırılıyor ise adli tedbirler ve uyar-kaldır yöntemi ile, yurtdışı kaynaklı ise ulusal filtre listesine alınarak engellenmektedir (Deibert vd., 168-169). Keza, Rusya’da Roskomnadzor Kurumu’una mahkeme kararı olmaksızın intihara yönlendirme içeriklerini kara listeye alma ve engelleme yetkisi verilmiştir (Hürriyet, 01.11.2012). Yine, Japonya’da uyuşturucu, uyarıcı zararlı maddelerin ekiminin, üretiminin, yapılmasının ve kullanımının anlatılması, kullanımının teşvik edilmesi veya reklamı ya da psikoaktif ilaçları kullanmaya teşvik etmek ve reklamını yapmak “yasadışı” kabul edilmiştir (Internet Hotline Centre Japan, 2013).

Benzer şekilde İtalya, Güney Kore, Bulgaristan, Suudi Arabistan ve İran’da uyuşturucu kullanımını teşvik etmek yasadışı olarak kabul edilen İnternet içerik

türlerindendir (114.it, 2012; Web112.net, 2010; Singo, 2013b; Internet.sa, 2013a). Ayrıca, Hollanda'daki Meldpunt Kinderporno ve İspanya'daki Protegeles İnternet İhbar Merkezleri uyuşturucu kullanmaya teşvik konusunda ihbarları kabul etmekte ve bunlarla ilgili yardım hizmeti vermektedir (Meldknop.nl, 2013; Protegeles, 2013).

3.3.1.2.4 Sağlık İçin Tehlikeli Madde Temini

Anayasa'nın 58. maddesi devleti gençliği alkol düşkünlüğünden ve benzeri kötü alışkanlıklardan korumak için gerekli tedbirleri almakla yükümlü kılmaktadır. Bu yükümlülüğün bir gereği olarak 5237 sayılı TCK'nun 194. maddesi sağlık için tehlike oluşturabilecek maddelerin çocuklara, akıl hastalarına veya uçucu madde kullananlara verilmesini veya bu tür kişilerin tüketimine sunulmasını suç kabul etmiştir. Bu suçu işleyenler için altı aydan bir yıla kadar hapis cezası öngörülmüştür. 5651 sayılı Kanun da, bu suç türünü katalog suçları arasına almış ve İnternet ortamında yapılan yayınlarla bu suçun oluştuğu yönünde yeterli şüphe bulunması durumunda bu içeriklere erişim engelleme kararı verilebileceğini hükme bağlamıştır.

Maddenin metninde çocuklara veya akıl hastalarına sağlık için tehlikeli olabilecek maddelerin verilmesi suç olarak tanımlanmıştır. Madde gerekçesinde bağımlılık yapan uyuşturucu veya uyarıcı maddelere ilişkin TCK'da özel hükümler bulunduğu için söz konusu maddelerin bu maddenin kapsamı dışında kaldığı belirtilmiştir. Dolayısıyla alkollü içki ve tütün mamülleri yanında, insanda bağımlılık yaratması ve sağlık için tehlikeli olması nedeniyle tiner gibi kimyasal maddeler de bu suçun kapsamındadır (TBMM, 2004). Her ne kadar suçun konusunu bu maddelerin oluşturduğu gerekçede yazılsa da, Yasa'da tehlikeli maddenin tanımına açıkça yer verilmemiş olması suçta ve cezada kanunilik ilkesine ters düştüğü gerekçesiyle eleştirilmektedir (Kaya, 2010: 101-102).

Yasa maddesine göre suç, sağlık için tehlikeli olabilecek maddelerin çocuklara veya akıl hastalarına verilmesiyle ve tüketimlerine sunulmasıyla oluşmaktadır. Bu bakımdan, söz konusu suça teşebbüs de tamamlanmış suç gibi cezalandırılmayı gerektirmektedir. Keza, çocukların yanı sıra, 18 yaşını doldurmuş olsa da, akıl hastası olan veya uçucu madde kullanan kişiler de bu suçun mağduru olabilirler (TBMM, 2004).

3.3.1.2.5 Müstehcenlik

5651 sayılı Kanun'un ailenin, çocukların ve gençlerin korunması saikiyle katalog suçları içerisine aldığı diğer bir suç türü de TCK'nın 226. maddesinde yer alan "müstehcenlik" suçudur. 226. madde "müstehcenlik" başlığını taşımaktadır. Madde metninde, müstehcenlik ve çocukların bu tür zararlı yayınlara karşı korunmasına ilişkin hükümler ayrıntılı olarak düzenlenmiştir. Madde gerekçesinde bu madde oluşturulurken müstehcenlik kavramının içeriğinin belirlenmesinde; "toplumda egemen olan değer ölçüleri" ve "toplumun sahip bulunduğu ortak edep (ar ve haya) duygularının, edep törelerinin ihlali, incitilmesi ve her ne suretle olursa olsun edep ve ahlak temizliğine alenen saldırı niteliği taşıyan hareketler, tutum ve davranışlar ve takınılan durumların" gözönüne alındığı belirtilmektedir. Böylece, toplum kültürünün önemli bir kısmını oluşturan iffet, ar ve haya duygularının, toplumun ortak edep ve ahlak temizliğinin korunması amaçlanmakta ve bu değerlere saldırı niteliği taşıyan hareketler yasaklanmaktadır (TBMM, 2004).

226. maddenin 1. fıkrası çocukların müstehcen içeriğe erişimi ile ilgili konuları düzenlemiştir. Buna göre, doğrudan veya dolaylı olarak çocuklara görüntü, yazı veya sözler içeren ürünler vasıtasıyla müstehcen içeriğe erişimi sağlayan şu fiillere altı aydan iki yıla kadar hapis ve adli para cezası öngörülmüştür: a) Bir çocuğa müstehcen görüntü, yazı veya sözleri içeren ürünleri veren ya da bunların içeriğini gösteren, okuyan, okutan veya dinleten, b) Bunların içeriklerini çocukların girebileceği veya görebileceği yerlerde ya da alenen gösteren, görülebilecek şekilde sergileyen, okuyan, okutan, söyleyen, söyleten, c) Bu ürünleri, içeriğine vakıf olunabilecek şekilde satışa veya kiraya sunan, d) Bu ürünleri, bunların satışına mahsus alışveriş yerleri dışında, satışa sunan, satan veya kiraya veren, e) Bu ürünleri, diğer mal veya hizmet satışları yanında veya dolayısıyla bedelsiz olarak veren veya dağıtan, f) Bu ürünlerin reklamını yapan.

2. fıkra müstehcen içeriğin basın ve yayın yoluyla yayını veya yayınına aracılık edilmesini cezayı ağırlaştırıcı bir neden olarak kabul etmiş ve cezayı altı aydan üç yıla kadar hapis ve beşbin güne kadar adli para cezasına çıkartmıştır.

3. fıkra ise, müstehcenliğe karşı çocukları korumaya yönelik iki ayrı suç tanımına yer vermiştir. Bunlardan birincisi, müstehcen görüntü, yazı veya sözleri içeren ürünlerin üretiminde çocukların kullanılması suretiyle oluşmaktadır ki, bunun cezası beş yıldan on yıla kadar hapis ve beşbin güne kadar adli para cezasıdır. İkincisi ise, bu ürünlerin ülkeye sokulması, çoğaltılması, satışa arzı, satışı, nakli, depolanması, ihracı, bulundurulması ya da başkalarının kullanımına sunulması fiillerinden birinin işlenmesiyle oluşmaktadır. Bu fiillerin cezası da iki yıldan beş yıla kadar hapis ve beşbin güne kadar adli para cezasıdır.

4. fıkra, şiddet kullanılarak, hayvanlarla, ölmüş insan bedeni üzerinde veya doğal olmayan yoldan yapılan cinsel davranışlara ilişkin yazı, ses veya görüntüleri içeren ürünlerin üretilmesi, ülkeye sokulması, satışa sunulması, satışı, nakli, depolanması, başkalarının kullanımına sunulması veya bulundurulması fiillerini suç saymış ve bir yıldan dört yıla kadar hapis ve beşbin güne kadar adli para cezası öngörmüştür.

5. fıkra ise, 3. ve 4. fıkralarda belirtilen ve müstehcenlik bakımından mutlak yasak kapsamına giren ürünlerin içeriğinin basın ve yayın yolu ile yayınlanması, yayınlanmasına aracılık edilmesi ya da çocukların görmesinin, dinlemesinin veya okumasının sağlanmasını ayrı bir suç olarak belirlemiş ve altı yıldan on yıla kadar hapis ve beşbin güne kadar adli para cezası öngörmüştür.

7. fıkra, bilimsel eserleri müstehcenlik suçu kapsamı dışında tutmuştur. Bu nedenle cinsel bir eğitim kılavuzu, ya da cinselliğin antropolojik, sosyolojik, tıbbi veya tarihi yönlerini içeren her türlü içerik müstehcenlik suçunun kapsamı dışındadır (Kaya, 2010: 105). Sanatsal ve edebi değeri olan eserler için ise, her koşulda müstehcen içeriğe sahip ürünlerin üretilmesinde çocukların kullanılmasını yasaklayan 3. fıkradaki hükme riayet edilmesi ve çocukların bu tür eserlere ulaşmasının engellenmesi şartıyla bu eserlerin Yasa kapsamı dışında tutulacağını düzenlemiştir.

Bu durumda 226. maddenin müstehcenliği “mutlak olarak yasak müstehcenlik” ve “nispi olarak yasak müstehcenlik” olmak üzere ikiye ayırdığı görülmektedir. Buna göre, “mutlak olarak yasak müstehcenlik” maddenin 3., 4. ve 5. fıkralarında yer

verilen hususlar ve doğal olmayan yollardan yapılan cinsel ilişkiyi ifade eden müstehcenliktir ve mutlak olarak yetişkin-çocuk ayrımı yapılmaksızın herkes bakımından yasaklanmıştır. Buradaki müstehcenliğin, hiçbir şekilde toplumun genel ahlakı ile bağdaştırılması mümkün değildir (Özbek, 2009: 27-28).

“Nispi olarak yasak müstehcenlik” ise, maddenin 1. ve 2. fıkralarında yer alan müstehcenliktir. Burada çocukların müstehcen ürüne ulaşmasını sağlayanları cezalandırarak çocukları koruma altına alma ve genel olarak müstehcen ürünün belirli şekillerde satışını yasaklama söz konusudur. Buradaki esas unsuru müstehcen içeriğe çocukların ulaşip ulaşamaması oluşturmaktadır (Özbek, 2009: 27-28).

Bu düzenlemeye göre, “mutlak olarak yasak müstehcenlik” dışındaki müstehcen ürünlerin, çocukların ulaşmasını engellemek şartıyla, satışına mahsus alışveriş yerlerinde satılması veya kiraya verilmesi serbesttir. Bu durumda bu kapsama, belirtilen şartlar dahilinde sadece müstehcen içerik bulunduran ve tamamen müstehcen ürünlere ilişkin ücret karşılığı hizmet veren İnternet sitelerinin de girdiği söylenebilir. O halde, çocukların Kanun’un izin verdiği bu tür sitelere girmesini önlemek maksadıyla İnternet sitesinin giriş sayfasında herhangi bir müstehcen içerik bulundurmaksızın, siteye 18 yaşından küçüklerin giremeyeceğine dair bir uyarı yazısının konması ve 18 yaşından küçüklerin erişimine engel olacak yaş doğrulama sistemlerinin kullanılması gerekmektedir. Aksi halde, bu İnternet sitelerinin 5651 sayılı Kanun’un 8. maddesine göre engellenmesi gerekmektedir (Atamer, 2008).

226. madde, metninde geçen “müstehcenlik” ve madde gerekçesinde geçen “genel ahlak” kavramını tanımlamadığı ve “sanatsal ve edebi değeri olan eserler”in nasıl belirleneceğine ilişkin net bir kıstas belirtmediği için eleştirilmektedir. Kanun’un amacına uygun bir şekilde uygulanabilmesi için bu göreceli kavramların açıklanması gerektiği vurgulanmaktadır (Kaya, 2010: 105-106). Nitekim, müstehcenlik kavramının zamana, kişilere ve yere bağlı olarak değişen bir kavram olduğu; müstehcenlik anlayışının da toplumdan topluma değiştiği gibi, aynı toplum içinde zaman içerisinde değişikliğe uğradığı bilinmektedir (Özel, 2007).

Müstehcen kelimesi “Hücnnet” kelimesinden türemiştir. “Hücnnet”in sözlük anlamı “soysuzluk, karışıklık, bayağılık, aşağılık, kötü davranış”tır. Müstehcen kelimesi ise, "ayıp, terbiyesizce, iğrenç, açık-saçık, edepsizcesine, edebe aykırı, yakışıksız" anlamlarına gelmektedir. Öte yandan müstehcenlik tanımı içinde yer alan edep kelimesi “terbiye, güzel ahlak, iyi davranış, incelik, kibarlık, utanma, örtülmesi gerekli ayıp yerler” gibi anlamlara gelmektedir. Bu da müstehcenlik ile ahlak kavramları arasındaki ilişkiyi ortaya koymaktadır. Ahlak denildiğinde ise, kelimenin en dar anlamıyla, “neyin doğru veya yanlış sayıldığı ya da sayılması gerektiği” anlaşılmaktadır (Özbek, 2009: 15-16).

“Genel ahlak” kavramı ise Anayasa Mahkemesi kararlarında “belli bir zamanda, belli bir toplumun büyük çoğunluğunca benimsenmiş, kolayca anlaşılan ahlak kurallarının bütünü” olarak tarif edilmiştir (Anayasa Mahkemesi Kararı, 1964, 2012). Bu tarif genel ahlakın sınırlarını kesin olarak çizmemekte ve somut olayın özelliklerine göre bir değerlendirme yapılmasını tavsiye etmektedir (Kaya, 2010: 106).

Anayasa Mahkemesi’nin bu tarif ile belli bir anda ve belli bir toplumda bireylerce benimsenen etik düşüncelerin asgarisine, yani ilk bakışta gözlenebilen temel değerlere dikkat çektiği belirtilmektedir. Ayrıca, Yüksek Mahkeme’nin toplum yapısının manevi yönünü ve etik çatısını belirleyen genel ahlak kavramını daha açık bir kavram olan kamu düzenine yaklaştırarak belirsizliği önlemek istediği vurgulanmaktadır. Dolayısıyla, “genel ahlak”ın, belli bir anda ve belli bir toplumda benimsenen etik düşüncelerin asgarisi olduğu söylenebilir. Bu nedenle devlet ancak, belli bir zamanda sosyal dengelerin bu kurallara dayandığını dikkate almak suretiyle bunlara uyulmasını isteyebilir (Bulut, 2013).

Konuyla ilgili olarak, müstehcenlikle birlikte tartışılan iki kavram “erotizm” ve “pornografi”dir. Doktrinde, bu iki kavramın müstehcenliğin iki ayrı türü olduğu belirtilmekle birlikte (Yürüşen, 2001: 23), her ikisinin tanımının da en az müstehcenliğin tanımı kadar muğlak olduğu da dile getirilmektedir (Dülger, 2007: 1522). “Erotik” kelimesi Fransızca “Eros” kelimesinden gelmekte ve sözlük anlamı itibariyle “Aşkla ilgili olan, aşkı anlatan, kösnül, erosal, şehevi, şehvani”dir (Bulut,

2013). Bu yönüyle erotik aktivitelerin, cinsel ilişkinin ön aşamalarını ve ilişkiye geçişin ritüel davranışlarını kapsadığı; cinsel ilişkiyi dolaylı bir şekilde ve bedensel çıplaklığı sanatsal estetik anlayışı içinde gösterdiği kabul edilmektedir (Özbek, 2009: 19). Buna göre “erotizm”, şiddet içermeyen, aşağılayıcı olmayan ve rızaya dayalı cinsel aktivitelerin sözlü ya da görsel temsili olarak tanımlanmakta (Yürüşen, 2001: 25); cinsellik içermesine rağmen cinsel uyarılının ön plana çıkarılmadığı ve cinsel organların görünmediği içerikler olarak tarif edilmektedir (Kaya, 2010: 107).

Pornografi kelimesi ise “Açık saçık yayın veya resim, edebe aykırı kitap veya resim” olarak tarif edilmektedir (Bulut, 2013). Eski Yunandan gelen ve kelime anlamı olarak “müstehcen şey” demek olan pornografide cinselliğin yapılmasından daha öte onun yayını ön plandadır. Dolayısıyla, pornografi toplumda kabul gören seks veya ahlaki davranış ölçütlerine karşı saldırı ya da aykırı bir hareket tarzıdır. Pornografide insan diğer tüm ilişkileri ve duyguları bir yana bırakılmak suretiyle cinsel bir objeye indirgenmekte; cinsel hareketleri estetikten uzak, kaba ve kışkırtıcı bir şekilde ön plana çıkartılmaktadır. Tüm çabası büyük oranda cinsel nesnelere olan şehvetli ilgiyi ortaya çıkarmak olan, hatta bazen iğrençlik duyguları uyandıracak tarzda, bunları olabildiğince açık-seçik olarak gösteren içerikler pornografiktir (Özbek, 2009: 19).

Aralarında var olduğu kabul edilen bu farktan hareketle, erotik içeriğin sanatsal veya edebi başkaca bir değerinin bulunduğu savıyla bir ifade biçimi ve tezahürü olarak korunması gerektiği ileri sürülmektedir. Fakat pornografi, ifade hürriyeti kapsamında korunmasını gerekli kılacak meşru bir ifade içermemesi nedeniyle korunmaya değer görülmemektedir. Nitekim, pornografinin kadını nesneleştirme ve kadın/erkek ilişkisini tek yönlü bir erkek egemenliğine dönüştürmesi, şiddet ve aşağılama içermesi (Yürüşen, 2001: 26) nedenleriyle korunması gereken bir değer olarak görülemeyeceği genel olarak kabul edilmektedir (Kaya, 2010: 108).

TCK’nın müstehcenlikle ilgili maddelerinin uygulamasında da benzer bir ayrıma gidilmeye çalışıldığı görülmektedir. Keza, Yargıtay’ın da “cezalandırılabilir olanın erotik değil, pornografik ya da müstehcen olandır” yaklaşımını benimsediğine ilişkin kararları vardır. O halde Türk Ceza Hukuku yönünden müstehcenlikle pornografinin

aynı anlama geldiği ve genel olarak pornografi suç sayılırken, erotik yayınların suç kapsamında görülmediği söylenebilir (Özbek, 2009: 22-23; Özel, 2007).

Diğer yandan, bir yayının erotik mi pornografik mi olduğunun ayırımının yapılmasında da zorluklar bulunmaktadır. Adli makamlar bu konuda tereddüde düşerlerse 1117 sayılı Küçükleri Muzır Neşriyattan Koruma Kanunu hükümlerine göre resmi bilirkişilik yapmakla görevlendirilen Başbakanlık Küçükleri Muzır Neşriyattan Koruma Kurulu'na müracaat edilmektedir.

Yargıtay'ın değişik kararları Mahkeme'nin her zaman özel olarak erotik ile müstehcenlik kavramları arasındaki fark ya da farkları ortaya koyma yoluna gitmediğini, bu kavramları genellikle birlikte değerlendirmekte olduğunu gösterse de (Yargıtay Kararı, 1999, 2001, 2010); müstehcenlik ile erotik ve pornografik içeriklerle ilgili kararlarında bilinen en önemli kıstasın söz konusu içeriğin kişilerin tenasül uzvunu gösterip göstermediği noktasında belirlediğini söyleyebiliriz. Yargıtay genellikle içtihatlarında yayın içeriklerinde kişilerin tenasül uzvunun yer almasını müstehcenlik suçunun oluşmasının gerekçesi saymaktadır (Özel, 2007).

Fakat, Yargıtay'ın her zaman bu kıstası dikkate aldığı söylenemez. Örneğin, Yargıtay 7. Ceza Dairesi, bir davada tenasül uzvunun görünmediği bir kadın resmine ilişkin olarak resmin küçüklerin maneviyatı üzerinde olumsuz etki oluşturacağı gerekçesiyle müstehcenlik suçunun oluştuğuna karar vermiştir (Yargıtay Kararı, 1993). Buradan da anlaşılacağı üzere, tenasül uzuvları görünen kadın veya erkek içeriklerinin yayınlanması söz konusu yayını müstehcenlik kapsamına kesin olarak sokmaktadır. Lakin, her ne kadar genital organlar görünmese de, somut olay bir bütün olarak değerlendirildiğinde amacın müstehcenlik olduğu kanısına varılır ise müstehcenlik vardır denilebilmektedir (Altınay, 2011: 23).

Bunun dışında, genel olarak Yargıtay kararları değerlendirildiğinde; görünüm ve kompozisyon itibarıyla ar ve haya hislerini rencide eder nitelikte olan, özellikle cinsel arzuların istismarı veya cinsel duyguları tahrik gayesiyle yapılan veya küçüklerin maneviyatı üzerinde muzır tesir yapacak mahiyette bulunan içerikler müstehcen veya

pornografik kabul edilmektedir (Özel, 2006). Dolayısıyla, bu kriterler çerçevesinde her yayını kendi şartları içinde ve sanığın saiki de dikkate alınarak incelemek gerekmektedir (Özel, 2007).

Görüldüğü gibi, müstehcenlik her ne kadar muğlak ve ucu açık bir kavram gibi görünse de; hem mülga 765 sayılı hem de 5237 sayılı yeni TCK'nunda yer alması nedeniyle, uzun yıllardır adli mercilerin vermiş olduğu kararlar doğrultusunda içtihatlar yerleşmiştir. Başka bir ifadeyle, müstehcenlik tanımında ceza hukuku açısından çok büyük bir belirsizlik bulunmamaktadır (Altınay, 2011: 25).

İnternette yer alan müstehcen veya pornografik içeriğin mücadeleye konu edilmesi tüm dünyada giderek yaygınlaşan bir uygulamadır. Bu konuda, her tür yetişkin pornografisine ait içeriğin çocukların erişiminin önüne geçilmesine yönelik boyutu, çocukların korunması adına neredeyse tüm ülkelerde öncelikli mücadele alanlarından birisidir. Nitekim, AB, yetişkin pornografisi, ırkçılık ve şiddet gibi içeriklerden çocukların korunmasını içerik politikasının önemli konularından birisi yaparken, ABD'de, çocukların korunması amacıyla kütüphaneler ve devlet okullarının filtreleme yazılımlarını kullanmalarını zorunlu tutan CIPA, bu yönde yapılmış bir düzenlemedir (FCC, 2001). Keza, ABD'de Ceza ve Ceza Usul Kanunu'nun çocukların istismarının önlenmesine ilişkin 2256 Nolu maddesi içerik sağlayıcıların müstehcen içeriğe ilişkin yaş doğrulaması gibi sistemleri kullanmasını zorunlu kılmaktadır (Onecl, 2011).

Benzer şekilde, 1994 tarihli Yeni Fransız Ceza Yasası şiddet ve pornografi içeren ya da insan onurunu ağır bir şekilde rencide eden bir içeriğin, hangi araçla olursa olsun çocuklar tarafından erişilebilir kılınmasına 3 yıl hapis ve 500 bin Frank para cezası öngörmüştür (Legifrance, 1994). Yine, Almanya'da Gençlik Koruma Yasası ile çocuklar ve gençlerin korunması için yasadışı ve zararlı görülen müstehcenlik, ırkçılık, şiddet ve vahşet içeren elektronik yayınlara önlem alınmasına yönelik hükümler getirilmiş ve elektronik yayın materyallerinin içeriklerine göre yaş gruplarının gözetilerek kategorize edilmesi ve etiketlenmesi konusunu düzenlemiştir (Gesetze-im-internet.de, 2002). Rusya Federal Yasası'da çocukların sağlık, ahlaki ve

ruhsal gelişimine zarar veren şiddet, zulüm ve pornografi içeriklerine karşı önlem alınmasını düzenlemiştir (Friendly Runet Foundation, 2013a).

Diğer yandan, genel olarak yetişkin pornografisi içeriklerine yönelik olarak da giderek birçok ülke tarafından tavrı alındığı görülmektedir. Bunların bir kısmı sadece ekstrem yetişkin pornografisine karşı tedbir geliştirmektedir. Örneğin, Avustralya ACMA'nın oluşturduğu kara liste ile hayvanlarla cinsel ilişki, aşırı şiddet ve tecavüz gibi aşırı pornografik içeriklere erişim engellemesi uygulamaktadır (Deibert vd., 2008: 168-169). Yine, İngiltere, Ceza Adaleti Göçmen Yasası ile extreme yetişkin pornografisi bulundurmaya suç kabul edilerek, iki yıla kadar hapis ve para cezası öngörmüştür (Cyberlaw, 2008).

Keza, İngiltere'de IWF'nin extreme pornografik içerikle mücadele etmek amacıyla oluşturduğu kara listeler, tüm İSS'lere, mobil operatörlere, arama motorlarına gönderilmekte ve bunlar tarafından erişimleri engellenmektedir (TİB, 2008; Nebil, 2009). Almanya İnternette yer alan ekstrem yetişkin pornografisine ait içeriklerle mücadelesini bu tür içeriği “yasak yayın” kapsamında değerlendiren Alman Ceza Yasası ile yürütmektedir (Gesetze-im-internet.de, 2011). Almanya'da Federal Hükümet, pornografi, şiddet ve neo-Nazi aktivitelerine yönelik yasadışı web sitelerini içeren kara liste sağlamaktadır (Nebil, 2009).

Bazı ülkeler ise, her tür müstehcen ve pornografik İnternet içeriği ile mücadele etmektedir. Örneğin, Japonya akademik ve tıbbi amaçlar hariç olmak üzere cinsel organları açıkça veya açığa yakın bir şekilde gösteren müstehcen materyallerin hepsini “yasadışı” olarak kabul etmiştir (Internet Hotline Centre Japan, 2013). Güney Kore, de Bilgi ve İletişim Ağı Kullanımı ve Bilgi Koruma Teşvik Yasası ile müstehcenliği “yasadışı içerik” kapsamına alarak ülkede erişim engelleme uygulamalarının temel gerekçelerinden birisi yapmıştır (OpenNet, 06.08.2012). Keza, Singapur, Yayıncılık Yasası ile her tür çıplaklık veya bir cinsel organın tasviriyle, kişi veya kişileri açık bir cinsel ilişki içerisinde gösteren içerikleri yasaklı yayınlardan saymıştır (MDA, 1997). Bunlar dışında, Çin, Suudi Arabistan ve İran gibi ülkeler baştan beri her tür pornografik içerik ile mücadele etmektedir.

3.3.1.2.6 Fuhuş

5651 sayılı Kanun, ailenin, çocukların ve gençliğin korunması amacına uygun olarak kişilerin ve özellikle çocukların fuhşa teşvik edilmesini katalog suçları kapsamına almış ve bu fiilleri suç olarak düzenleyen 5237 sayılı TCK'nın 227. maddesine aykırılık oluşturan içeriğin erişiminin engellemesini kabul etmiştir.

5237 sayılı TCK'nın 227. maddesi, çocukların ve yetişkinlerin fuhşunu benzer hükümlerle ancak farklı ağırlıkta cezai yaptırımlarla düzenlemiştir. Maddenin 1. fıkrası, çocuğun fuhşa teşvik edilmesi, fuhuş yolunun kolaylaştırılması, bu maksatla tedarik veya barındırma yapılması ya da çocuğun fuhşuna aracılık edilmesi fiillerine dört yıldan on yıla kadar hapis ve beşbin güne kadar adli para cezası öngörmüştür. Ayrıca, bu suçun işlenmesine yönelik her türlü hazırlık hareketinin de tamamlanmış suç gibi cezalandırılacağına hükmetmiştir.

2. fıkra, yetişkinlerin fuhşa teşvik edilmesine, kolaylaştırılmasına, aracılık edilmesine veya yer temin edilmesine iki yıldan dört yıla kadar hapis ve üçbin güne kadar adli para cezası öngörürken, fuhşa sürüklenen kişinin kazancından yararlanarak kısmen veya tamamen geçim sağlanmasını da fuhşa teşvik kapsamına almıştır.

4. fıkra, cebir veya tehdit kullanarak, hile ile ya da çaresizliğinden yararlanarak bir kimseyi fuhşa sevk eden veya fuhuş yapmasını sağlayan kişi hakkında yukarıdaki fıkralara göre verilecek cezanın yarısından iki katına kadar artırılacağını; 5. fıkra, söz konusu suçların eş, üstsoy, kayın üstsoy, kardeş, evlat edinen, vasi, eğitici, öğretici, bakıcı, koruma ve gözetim yükümlülüğü bulunan diğer kişiler tarafından ya da kamu görevi veya hizmet ilişkisinin sağladığı nüfuzun kötüye kullanılmasıyla işlenmesi halinde, verilecek cezanın yarı oranında artırılmasını hüküm altına almıştır. 6. fıkra, bu suçların, örgüt faaliyeti çerçevesinde işlenmesi halinde, yukarıdaki fıkralara göre verilecek cezaları yarı oranında artırmaktadır. 227. maddede düzenlenen çocukları ve yetişkinleri fuhşa teşvik etme, bunun yolunu kolaylaştırma ve aracılık etme fiillerinin İnternet ortamında yapılan yayınlarla işlenmesi mümkündür.

227. maddenin gerekçesinde söz konusu düzenlemeler yapılırken, Türkiye'nin fuhuşla mücadele ile ilgili olarak milletlerarası sözleşmelerden kaynaklanan yükümlülüklerinin göz önünde bulundurulduğu dile getirilmektedir. Zira, söz konusu sözleşmeler, taraf olan ülkelere fuhuşun önlenmesi için mücadele edilmesi konusunda bir çok yükümlülükler getirmektedir (TBMM, 2004).

Dünyada da İnternetin fuhuşa aracılık yapılmasını önlemek için içeriğe müdahalede bulunan ülkeler vardır. Örneğin Japonya fuhuş yapmak veya yaptırmak, fuhuşu teşvik etmek veya fuhuşun önlenmesine yönelik yasalara aykırı reklamlarla ilgili içerikleri “yasadışı” kabul etmiştir (Internet Hotline Centre Japan, 2013). Keza, Singapur Yayıncılık Yasası, İnternetin “fuhuş” için kullanılmasını yasadışı olarak tanımlamış ve İSS’ların sundukları hizmetlerde bu tür içeriklerle ilgili gereken tedbirleri almalarını zorunlu kılmıştır (MDA, 2004).

3.3.1.2.7 Kumar Oynanması İçin Yer ve İmkan Sağlama

5651 sayılı Kanun, 5237 sayılı TCK’nın 228. maddesinde yer alan kumar oynanması için yer ve imkan sağlama suçunu katalog suçlarından birisi olarak kabul etmiş ve bu suçun İnternette yapılan yayınlarla oluştuğu yönünde yeterli şüphe bulunması durumunda bu tür içeriğin engellenmesi kararının verilebilmesini hükme bağlamıştır.

Türk hukukunda 5326 sayılı Kabahatler Kanunu’nun 34. maddesine göre kumar oynamak “kabahat”, TCK’nun 228. maddesine göre kumar oynatmak ve bu doğrultuda yer ve imkan sağlamak ise suç olarak kabul edilmiştir. Kumar, 5237 sayılı TCK’nun 228. maddesinde “kazanç amacıyla icra edilen ve kar ve zararı talihe bağlı olan oyunlar” olarak tanımlanmıştır. Buna göre bir oyunun kumar sayılması için oyunun “kazanç kastı ile icra edilmesi” ve “kar ve zararın talihe bağlı olması” koşulları aranacaktır. Bu tanıma göre, Türkiye’de kumarhanelerin faaliyet göstermesi yasaklanırken; kazanç kastı olmaksızın, dostlar arasında eğlenmek üzere oyun oynanmasına imkan sağlanması bu suçun kapsamı dışında kalmıştır (TBMM, 2004). Yasa, söz konusu fiili işlemenin cezasını bir yıla kadar hapis ve adli para cezası

olarak belirlemiştir. Çocukların kumar oynaması için yer ve imkan sağlanması ise verilecek cezanın bir katı oranında artırılmasını öngörmektedir.

Maddenin gerekçesinde bu suça ilişkin düzenlemenin, kumarın sosyal bakımdan ortaya koyduğu büyük tehlike ve doğurması olası faciaların göz önüne alınarak hazırlandığı ve söz konusu suçun oluşabilmesi için, aleniyet şartının aranmadığı belirtilmektedir. Düzenlemeye göre suç başkalarının kumar oynayabilmesi için yer veya başka suretle imkan sağlandığı anda oluşmaktadır (TBMM, 2004).

228. maddenin 2. fıkrası, çocukların kumar oynaması için yer ve imkan sağlanmasını ağırlaştırıcı bir sebep olarak kabul edilmiştir. Fakat, online kumar oynanan sitelerin ziyaretçi yaşlarının tespit edilememesi bu hükmün uygulanmasını zorlaştırmaktadır. Zira, birçok web sitesinin ana sayfalarında yer alan yaş doğrulama sistemleri yanlış bilgiler verilerek aşılabilmektedir. Bu nedenle, çocukların kumar oynaması için yer ve imkan sağlanıp sağlanmadığının tespiti oldukça zordur (Kaya, 2010: 114).

Diğer yandan, 5651 sayılı Kanun ilk yürürlüğe girdiği dönemlerde bu suça ilişkin engelleme nedeni fazla dikkat çekmezken; online kumar sitelerinde dolaşan paranın miktarının artması ve bu sitelere yönelik başta Milli Piyango İdaresi olmak üzere kamu otoritelerinin denetimlerini artırması sonucunda TİB'in bu suça yönelik çalışmaları hız kazanmıştır (Kaya, 2010: 114).

Nitekim, dünyada da birçok ülke online kumar konusunda düzenlemeler yapmakta ve bu tür içeriğe müdahale etmektedir. ABD'de, İnternette Kumarın Yasaklanması Yasası, kumar ve şans oyunlarının, İnternet üzerinden oynanmasını yasaklayarak, bunu yapanlara 2 yıla kadar hapis ile 10 bin \$ para cezası getirmiştir (LOC, 1997). Avustralya'da ACMA yasal olmayan kumar içeriğiyle mücadele etmektedir (ACMA, 2012h). Fransa, Kumar ve Online Kumar Yasasıyla ARJEL'e yasadışı kumar sitelerine karşı önlem alma ve İSS'lara başvurarak mahkeme kararı olmaksızın bu sitelerin engellenmesini talep etme yetkisi vermiştir (ARJEL, 2012).

Keza, Güney Kore, Bilgi ve İletişim Ağı Kullanımı ve Bilgi Koruma Teşvik Yasası ile kumara teşvik konusunu “yasadışı içerik” olarak kabul etmiş ve KCSC'yi bu tür

içeriğin önlenmesi konusunda yetkili kılmıştır (ICEC, 2013b). Singapur da, Yayıncılık Yasası ile İSS'ların sundukları hizmetlerin loto, at yarışı, her türlü şans oyunu için kullanılmaması yönünde gereken tedbirleri almaları konusunda İSS'ları yükümlü kılmıştır (MDA, 2004). Bunlar dışında, Çin'in yanında Suudi Arabistan ve İran gibi birçok İslam ülkesi bu konudaki içeriklerle mücadele etmektedir.

3.3.1.2.8 Sabit İhtimalli Veya Müşterek Bahis Oynatılması

5651 sayılı Kanun'un ilk metninde olmamakla birlikte, 5237 sayılı TCK'nın 228. maddesinde yer alan kumar oynanması için yer ve imkan sağlama suçunun konsepti içinde, 2008 yılında 7258 sayılı Futbol Müsabakalarında Müşterek Bahisler Tertibi Hakkında Kanun'da yapılan bir değişiklik ile İnternet ortamında yasadışı olarak "sabit ihtimalli veya müşterek bahis oynatılması"¹⁰⁰ ve bu amaçla yer ve imkan sağlanması suç olarak kabul edilmiş ve bu tür siteler için erişimin engellenmesi hükümlerinin uygulanacağı düzenlenmiştir. Böylece, başka bir yasal düzenleme vesilesi ile yeni bir katalog suçu ihdas edilmiştir.

23.1.2008 tarihli 5728 sayılı Yasa ile 7258 sayılı Yasanın 5. md.'sinde yapılan değişiklikle, izinsiz olarak spor müsabakaları ile ilgili sabit ihtimalli veya müşterek bahis oynatılması ve bu amaçla yer ve imkan sağlanması suç kabul edilmiş ve bu fiile aykırı hareket edenler için bir yıldan üç yıla kadar hapis ve onbin güne kadar adli para cezası öngörülmüştür. Böylece bu düzenleme ile kumar oynanması için yer ve imkan sağlamayı suç sayan TCK'nın 228. md. ile uyumlu hale getirilmiştir.

7258 sayılı Yasa, bu tür oyunların İnternet üzerinden oynatılmasına ilişkin özel bir hüküm de getirmiştir. Bu doğrultuda, yurt dışında oynatılan her tür bahis ve şans

¹⁰⁰ 5738 sayılı Spor Müsabakalarına Dayalı Sabit İhtimalli ve Müşterek Bahis Oyunlarının Özel Hukuk Tüzel Kişilerine Yapıtılması Hakkında Kanun "sabit ihtimalli ve müşterek bahis oyunları"nı tanımlamaktadır. Buna göre, sabit ihtimalli bahis oyunlarını, "yurt içinde ve yurt dışında tertiplenen spor müsabakalarına ait sonuçların veya etkinliklerin tahmin edilmesi esasına göre oynatılan ve iştirak edenler arasından doğru tahmin edenlere, önceden belirlenen bahis oranlarıyla ikramiye kazandıran oyunlar" olarak tanımlamıştır. Müşterek bahis oyunları ise, "yurt içinde ve yurt dışında tertiplenen spor müsabakalarına ait sonuçların tahmin edilmesi üzerine oynatılan, hasılatın önceden belirlenen ikramiye yüzdesinin, doğru sonucu tahmin eden iştirakçiler arasında paylaştırıldığı bahis oyunları" şeklinde tanımlamıştır. (27/02/2008 tarihli ve 26800 sayılı Resmi Gazete.)

oyununun İnternet yoluyla ve başka bir şekilde erişim sağlanarak Türkiye’de oynanmasına imkan sağlanmasını suç kabul etmiş ve bu suça iki yıldan beş yıla kadar hapis cezası öngörmüştür. Bununla bağlantılı olarak Yasa, tanımlanan suçlarla ilgili olarak, 5651 sayılı Yasa’nın erişimin engellenmesine ilişkin hükümlerinin uygulanacağını belirterek katalog suçlarına yeni bir suç türü daha eklemiştir.

Bu düzenlemeye paralel olarak, “her türlü bahis veya şans oyunları ile bağlantılı olarak para nakline aracılık eden” kişiler için bir yıldan üç yıla kadar hapis ve beşbin güne kadar adli para cezası; “kişileri, reklam vermek ve sair surette, her türlü bahis veya şans oyunlarını oynamaya teşvik edenler” için de altı aydan iki yıla kadar hapis ve üçbin güne kadar adli para cezası belirlenmiştir. Online bahis oynatanların reklamlarını genellikle İnternet ortamı üzerinden gerçekleştirdikleri ve hatta yeni bağımlılar oluşturmak için web siteleri üzerinden eğitim dahi verdikleri göz önünde bulundurulursa (Kaya, 2010: 115-116), bu düzenleme bir bütün olarak yasadışı bahis ve şans oyunları ile mücadelenin tamamlayıcı bir unsuru olarak kabul edilebilir.

Yabancı bahis sitelerinin erişimlerini engelleme bir diğer sebebinin yasal bahis sitelerinin kullanımını teşvik etmek ve bu şekilde elde edilen geliri vergilendirmek olduğu da ileri sürülmektedir (Kaya, 2010: 116). Nitekim, Maliye Bakanlığı talih oyunlarının kanun dışı olarak sanal ortam üzerinden oynatılmasının takibi, denetlenmesi ve ilan ve reklamlarının önlenmesi amacıyla “Sanal Ortamda Oynatılan Talih Oyunları Hakkında Yönetmelik”i hazırlayarak yürürlüğe koymuştur. Yönetmelik bilgisayar, İnternet, interaktif televizyon, cep telefonu ve benzeri tüm bilişim ortamlarında oynatılan talih oyunlarının denetlenmesini kapsamaktadır.

Türkiye’nin dışında, başka ülkelerde de bu konuda İnternet içeriğine yönelik kısıtlamalar getirilmektedir. Örneğin, Avustralya’da ACMA, yasaklanmış olan telefon bahisçiliği, izinsiz at yarışları bahisleri, diğer müsabakaların müsabakadan önce oynanan bahisleri, reklam ve malların tanıtımı amaçlı promosyon çekilişleri ve çekiliş hizmetlerine ilişkin şikayetleri kabul etmektedir (ACMA, 2012f).

3.3.1.2.9 Atatürk Aleyhine İşlenen Suçlar

Katalog suçlarından birisi de Atatürk aleyhine işlenen suçlarla ilgilidir. Buna göre, 5816 sayılı Atatürk Aleyhine İşlenen Suçlar Hakkında Kanun'da yer alan suçların İnternet ortamında yapılan yayınlarla oluştuğu yönünde yeterli şüphe bulunması durumunda söz konusu içeriğe erişim engellenmesi uygulanabilecektir.

5816 sayılı Kanun'un 1. maddesi "Atatürk'ün hatırasına alenen hakaret edilmesi veya sövülmesi" ile "Atatürk'ü temsil eden heykel, büst veya abidelerin veya Atatürk'ün kabrinin tahrip edilmesi, kırılması, bozulması veya kirletilmesi" olmak üzere iki farklı suça yer vermiştir. Kanun'da bunlardan birincisi için bir yıldan üç yıla, ikincisi için ise bir yıldan beş yıla kadar hapis cezası öngörülmüştür. 1. maddede ayrıca, bu iki suçu işlemeye başkalarını teşvik eden kimselerin asıl fail gibi cezalandırılacağı belirtilmiştir. Kanun 2. maddesi ise, söz konusu suçların iki veya daha fazla kişi tarafından toplu olarak veya umumi ya da umuma açık yerlerde veya basın vasıtasıyla işlenmesini ağırlatıcı neden olarak kabul etmiş ve bu durumda cezayı yarı nispetinde artırmıştır. Bu suçlardan sadece "Atatürk'ün hatırasına alenen hakaret veya sövme" suçunun İnternet ortamında yapılan yayınlarla işlenmesi mümkün olduğu için 5651 sayılı Kanun'un kapsamına bu tür suçlar girmiştir.

5651 sayılı Yasa genel bir yaklaşım olarak hakaret suçu gibi kişilik haklarına saldırı türü suçları bir erişim engelleme sebebi olarak kabul etmemiş, ortaya çıkabilecek mağduriyetleri gidermek için özel bir mekanizma olarak "yayından çıkarma ve cevap hakkı" düzenlemesini getirmiştir. "Atatürk'ün hatırasına alenen hakaret veya sövme" suçu bu genel kurala bir istisna olarak düzenlenmiştir (Kaya, 2010: 117).

5651 sayılı Kanun'un temel amacının ailenin, çocukların ve gençlerin korunması olduğu hatırlanırsa, Kanun'da bu amaç dışında yer alan tek ideolojik engelleme sebebinin 5816 sayılı Kanun'dan kaynaklanan engellemelerle ilgili olduğu görülecektir (Kaya, 2010: 117; Akdeniz ve Altıparmak, 2008: 57). Nitekim, erişim engellemelerine ilişkin en yoğun tartışmalar da bu konuda yaşanmıştır. Fakat, şunu da belirtmek gerekir ki, tarihi kişiliklerin ceza kanunlarıyla korunmaması gerektiğine yönelik görüşler olmasına rağmen, AİHM'in Türkiye'nin bu yaklaşımını haklı bulan kararları da bulunmaktadır (Akdeniz ve Altıparmak, 2008: 57).

Son olarak, 5651 sayılı Kanun ve bahsi geçen katalog suçları dışında olsa da, erişim engelleme ve bu çerçevede TİB ile ilgili olduğu için değinilmesi gereken diğer bir yasal düzenleme 633 Sayılı Diyanet İşleri Başkanlığı (DİB) Kuruluş ve Görevleri Hakkında Kanun'undur. Bu Kanun'da 1.7.2010 tarihli 6002 sayılı “Diyanet İşleri Başkanlığı Kuruluş Ve Görevleri Hakkında Kanun İle Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun”la yapılan değişiklik erişim engellemesi ve TİB’e ilişkin bazı düzenlemeler getirmiştir.

Bu çerçevede, Kanun’un 6. maddesi, Kurul’un görevleri arasında “hatalı ve noksan olarak basıldığı veya yayımlandığı Kurul tarafından tespit edilen mushaf ve cüzler ile sesli ve görüntülü Kur’an-ı Kerim yayınlarının” DİB’nin müracaatı üzerine, yayının yapıldığı yer sulh hukuk mahkemesi kararı ile toplatılıp imha edileceğini düzenledikten sonra, bu kapsama giren yayının İnternet ortamında yapılması haline ilişkin hükümler getirmiştir.

Buna göre, DİB’nin müracaatı üzerine, sulh hukuk mahkemesi bu yayınlara ilişkin olarak erişimin engellenmesi kararı verir ve bu kararın bir örneği gereği yapılmak üzere TİB’na gönderilir. Sulh hukuk mahkemesinin verdiği kararlara ve DİB’nin talebinin reddine dair kararlarına karşı iki hafta içinde asliye hukuk mahkemesine itiraz edilebilir. İtiraz üzerine verilen karar kesindir. Toplatma ve imha kararına veya erişimin engellenmesi kararına itiraz edilmiş olması, karara konu teşkil eden yayınların toplatılmasına ve erişimin engellenmesine engel teşkil etmez.

Görüldüğü gibi 5651 sayılı Kanun katalog suçları diye bilinen belirli suç tiplerine ait içeriklerle mücadeleyi benimsemiş olmakla birlikte, zaman içerisinde değişik ihtiyaçlardan ve gerekçelerden dolayı yeni erişim engellemesi sebepleri ortaya çıkmakta ve farklı yasal düzenlemeler söz konusu olmaktadır.

3.3.1.3 İkincil Düzenlemeler

5651 sayılı Kanun’un uygulamasını göstermek amacıyla ikincil düzenlemeler yapılmıştır. Bu çerçevede üç farklı yönetmelik hazırlanarak yürürlüğe konulmuştur.

Ayrıca, bazı yönetmeliklerde İnternet içerik düzenlemesini ilgilendiren bir takım hükümler bulunmaktadır.

3.3.1.3.1 Erişim Sağlayıcılara ve Yer Sağlayıcılara Faaliyet Belgesi Verilmesine İlişkin Usul ve Esaslar Hakkında Yönetmelik

24.10.2007 tarihli “Telekomünikasyon Kurumu Tarafından Erişim Sağlayıcılara ve Yer Sağlayıcılara Faaliyet Belgesi Verilmesine İlişkin Usul ve Esaslar Hakkında Yönetmelik”, 5651 sayılı Kanun’un erişim ve yer sağlayıcılar konusunda TİB’na vermiş olduğu görev ve yetkilere dayanılarak hazırlanmıştır. Yönetmeliğin hazırlanma amacı, erişim ve yer sağlayıcıları kayıt altına alarak yasadışı ve zararlı içerik ile mücadelede kontrol edilebilir ve denetlenebilir bir zemin oluşturmaktır.

Nitekim, Yönetmeliğin 4 ile 7. maddesi arasında, Türkiye’de erişim ve yer sağlayıcı olmak isteyenlerin TK’ndan faaliyet belgesi almakla yükümlülüğü belirtilmekte ve yer sağlayıcı faaliyet belgesi almaksızın bu faaliyette bulunanların İnternet erişim hizmetinin, TİB kararıyla ilgili erişim sağlayıcı tarafından durdurulacağı ilan edilmektedir. Ayrıca, erişim sağlayıcı faaliyet belgesinin, geçerliliğinin TK tarafından yetkilendirildiği süre kadar; yer sağlayıcı faaliyet belgesinin geçerliliğinin beş yıl olacağı hüküm altına alınmaktadır. Keza TK, erişim sağlayıcıları ve yer sağlayıcılarının listesini, Kurum’un İnternet sitesinde güncel olarak ilan edecektir.

Yönetmeliğin 8.-13. maddelerinde, başvuru sahibinde bulunması gereken şartlar, başvuru ve faaliyet belgesi verilmesi usulü, faaliyet belgesinin devri, yenilenmesi, sona ermesi gibi hususlar düzenlenmiştir. Faaliyetini sona erdiren erişim sağlayıcılara, diğer bazı yükümlülükler yanında, İnternet ortamında gerçekleştirilen her türlü erişim hizmetine ilişkin olarak son bir yıla ait “erişim sağlayıcı trafik bilgileri”ni¹⁰¹ TK’na teslim etme yükümlülüğü de getirilmiştir.

¹⁰¹ Yönetmelikte erişim sağlayıcı trafik bilgisi, “İnternet ortamına erişime ilişkin olarak abonenin adı, adı ve soyadı, adresi, telefon numarası, abone başlangıç tarihi, abone iptal tarihi, sisteme bağlantı tarih ve saat bilgisi, sistemden çıkış tarih ve saat bilgisi, ilgili bağlantı için verilen IP adresi ve bağlantı noktaları gibi bilgileri”ni ifade etmektedir.

Yönetmeliğin 14.-17. maddelerinde “Erişim ve Yer Sağlayıcıların Yükümlülükleri” düzenlenmiştir. Buna göre, yer ve erişim sağlayıcılar belirtilen şu tanıtıcı bilgileri, kullanıcıların ana sayfadan doğrudan ulaşabileceği şekilde iletişim başlığı altında, doğru eksiksiz ve güncel olarak bulundurmakla yükümlü kılınmıştır: a) Gerçek kişi ise; adı ve soyadı, tüzel kişi ise unvanı ve sorumlu kişiler, vergi kimlik numarası veya ticaret sicil numarası, b) Yerleşim yeri, tüzel kişi ise merkezinin bulunduğu yer, c) Elektronik iletişim adresi ve telefon numarası, ç) Sunduğu hizmet bir merciin iznine veya denetimine tabi bir faaliyet çerçevesinde yapıyor ise yetkili denetim merciine ilişkin bilgiler. Ayrıca, yer sağlayıcı faaliyetini sona erdirmek istediğinde TK’na yapacağı bildirimi müteakip, hizmetlerine son vereceğini kullanıcıların ulaşacağı şekilde ana sayfasından duyuracaktır.

Yönetmeliğin 15. maddesiyle, erişim sağlayıcının, Yasa’da yer alan erişimi engelleme yükümlülüğü tekrar edildikten sonra devamında erişim sağlayıcılara; erişim sağlayıcı trafik bilgisini bir yıl saklamak, bu bilgilerin doğruluğunu, bütünlüğünü oluşan verilerin dosya bütünlük değerlerini (hash)¹⁰² zaman damgası ile birlikte muhafaza ve gizliliğini temin etmek, Başkanlığın görevlerini yerine getirebilmesi için yapacağı trafik izlemesinde gerekli yardım ve desteği sağlamak, faaliyet belgesinde yer alan Başkanlığın uygun gördüğü bilgileri talep edildiğinde bildirmek ve ticari amaçla İnternet toplu kullanım sağlayıcılar¹⁰³ için belirli bir IP bloğundan sabit IP adres planlaması yapmak ve bu bloktan IP adresi vermek¹⁰⁴ yükümlülüğü getirilmiştir.

¹⁰² Yönetmelikte “dosya bütünlük değeri”nin, “Bir bilgisayar dosyasının içindeki bütün verilerin matematiksel bir işlemle geçirilmesi sonucu elde edilen ve dosyanın içerisindeki verilerde bir değişiklik yapıp yapılmadığını kontrol için kullanılan dosyanın özünü belirten değeri” ifade ettiği belirtilmektedir.

¹⁰³ Yönetmelikte “Ticari amaçla İnternet toplu kullanım sağlayıcı”nın “İnternet salonu ve benzeri umuma açık yerlerde belirli bir ücret karşılığı internet toplu kullanım sağlayıcılığı hizmeti veren veya bununla beraber bilgisayarlarda bilgi ve beceri artırıcı veya zeka geliştirici nitelikteki oyunların oynatılmasına imkân sağlayan” ifade ettiği belirtilmektedir.

¹⁰⁴ Yönetmelikte “IP Adresi”nin “Belirli bir ağa bağlı cihazların birbirini tanımak, birbirleriyle iletişim kurmak ve veri alışverişinde bulunmak için kullandıkları İnternet Protokolü standartlarına göre verilen adresi”; “Sabit IP Adresi”nin ise “Belirli bir ağa bağlı cihazların ağ üzerinden birbirleriyle iletişim kurmak ve birbirlerine veri alışverişinde bulunmak için kullandıkları, zamana, oturuma göre değişmeyen ve sistem yöneticisi tarafından belirlenip tanımlanan ve değiştirilebilen IP adresini” ifade ettiği belirtilmektedir.

15. maddenin akabinde erişim sağlayıcıların faaliyetine son verme durumundaki yükümlülükleri belirlenmiştir. Buna göre, erişim sağlayıcıların faaliyetine son vereceği tarihten en az üç ay önce, durumu TK'na, içerik sağlayıcılarına ve müşterilerine bildirmekle, TK'na bildirilen kapanma tarihinden geriye doğru bir yıllık süredeki trafik bilgilerine ilişkin bütün kayıtları metin dosyası olarak, log formatlarını açıklamalarıyla birlikte, abone kütük bilgilerini TİB'na cd, dvd gibi optik medya ortamında teslim etmekle yükümlü kılınmıştır.

Ayrıca erişim sağlayıcı, faaliyete başlamasından itibaren her ay düzenli olarak, her erişim yöntemine ilişkin kullanacağı erişim numaralarını ve toptan hizmet verdiği abonelere ilişkin bilgileri Başkanlığa göndermekle ve Başkanlık ile aralarındaki bağlantıdan erişimi engellenecek adreslere ilişkin gönderilecek bilgileri kendi sistemlerinde derhal uygulanabilmesi için, gerekli olan donanım ve yazılımı kurarak lazım olan düzenlemeleri yapmakla yükümlü tutulmuştur.

Yine, Yönetmeliğin 15. maddesiyle erişim sağlayıcıya, verdiği hizmeti kullananlara ilişkin bilgilerin başkaları tarafından elde edilmesini ilgili mevzuatta belirlenen esas ve usullere uygun olarak engelleme yükümlülüğü getirilirken, erişim sağlayıcıların, kendisi aracılığıyla erişilen içeriklerin hukuka aykırı olup olmadığını ve sorumluluğu gerektirip gerektirmediğini kontrol etmekle yükümlü olmadıkları vurgulanmıştır.

16. madde ise, yer sağlayıcıların yükümlülüklerine açıklık getirmektedir. Buna göre, yer sağlayıcının, barındırdığı hukuka aykırı içeriği yayından kaldırmakla yükümlü olduğu tekrar edilmiş ve yer sağlayıcının trafik bilgisini¹⁰⁵ altı ay saklamakla, bu bilgilerin doğruluğunu, bütünlüğünü oluşturan verilerin dosya bütünlük değerlerini (hash) zaman damgası ile birlikte saklamak ve gizliliğini temin etmekle yükümlü olduğu belirtilirken, yer sağladığı içeriği kontrol etmek veya hukuka aykırı bir faaliyetin var olup olmadığını araştırmakla yükümlü olmadığı vurgulanmıştır.

¹⁰⁵ Yönetmelikte “yer sağlayıcı trafik bilgisi”nin “İnternet ortamındaki her türlü yer sağlamaya ilişkin olarak; kaynak IP adresi, hedef IP adresi, bağlantı tarih-saat bilgisi, istenen sayfa adresi, işlem bilgisi (GET, POST komut detayları) ve sonuç bilgisi gibi bilgileri” ifade ettiği belirtilmektedir.

Yönetmeliğin 17. maddesinde ise, erişim ve yer sağlayıcıların bilgilerini güncelleme yükümlülükleri düzenlenmiş ve meydana gelen değişiklikleri en geç bir ay içerisinde TK'na bildirmekle yükümlü oldukları hatırlatılmıştır. 18 ve 19. madde erişim ve yer sağlayıcılara uygulanacak yaptırımları ele almıştır. Buna göre, 18. madde; 14. maddedeki bilgilendirme yükümlülüğünü yerine getirmeyen erişim veya yer sağlayıcıya TİB'nca ikibin YTL'sından onbin YTL'na kadar idari para cezası verileceğini öngörmüştür. Keza, Yönetmeliğin 15. maddesinde belirtilen trafik bilgilerinin saklanması ve gizliliğinin sağlanması ile faaliyetine son vermeye ilişkin yükümlülüklerden birini yerine getirmeyen erişim sağlayıcısına, Başkanlıkça onbin YTL'sından ellibin YTL'na kadar idari para cezası verilmesi hükme bağlanmıştır.

19. maddede ise yer ve erişim sağlayıcıların faaliyet belgelerinin iptali konusu ele alınmıştır. Buna göre, Türkiye'de bulunan yer sağlayıcısının bu Yönetmelikteki yükümlülüklerini yerine getirmemesi halinde faaliyet belgesinin TK tarafından iptal edilebileceği; bu durumda, TİB kararıyla ilgili yer sağlayıcının almakta olduğu İnternet erişim hizmetinin erişim sağlayıcı tarafından durdurulacağı belirtilmiştir.

Erişim sağlayıcı işletmecilere ilişkin olarak ise, işletmecinin erişim sağlayıcılığı faaliyet belgesinin 5651 sayılı Kanun ve ilgili mevzuat hükümlerine göre iptali halinde, bu işletmecinin Kablolı ve Kablosuz İSS olması halinde, bu telekomünikasyon hizmeti sunumuna yönelik genel izninin¹⁰⁶ TK tarafından iptal edileceği düzenlenmiştir. İşletmecinin, bunun dışında bir telekomünikasyon hizmeti sunumuna yönelik yetkilendirme ile erişim sağlayıcılığı hizmeti sunuyor olması halinde ise, yetkilendirmesi kapsamındaki erişim sağlayıcılığı hizmetleri askıya alınacaktır. Bu durumda işletmecinin erişim sağlayıcı faaliyetlerini derhal durdurma yükümlülüğü vardır. Bunun yanında, erişim sağlayıcılığı faaliyet belgesinin iptali, yeniden telekomünikasyon hizmetleri sunumuna yönelik yetkilendirme ve faaliyet belgesi başvurusu yapılmasına engel değildir.

¹⁰⁶ Yönetmelikte “genel izin”, “Bir telekomünikasyon hizmetinin yürütülmesi için, Kurum tarafından işletmecileri belirli genel şartlara ve Kurum nezdinde kayıt yaptırılmasına tabi olarak yetkilendiren genel düzenleyici işlemi” ifade etmektedir.

Mevcut yer veya erişim sağlayıcıların faaliyet belgesi alma durumları Geçici Madde 1’de düzenlenmiştir. Buna göre, bu durumda olanlar için, TK tarafından, telekomünikasyon yoluyla iletişim konusunda yetkilendirmesi olup olmadığına bakılmaksızın, yer veya erişim sağlayıcı olarak faaliyet icra etmesi amacıyla bir faaliyet belgesi düzenleneceği öngörülmüştür.

Görüldüğü gibi, çıkarılan bu Yönetmelikle katalog suçları ile belirlenmiş olan zararlı içeriklerle mücadele konusunda Türkiye’deki erişim ve yer sağlayıcılarının kayıt altına alınarak disipline edilmeleri, kontrol ve denetimlerinin sağlanmasına ilişkin önemli bir adım atılmıştır.

3.3.1.3.2 İnternet Toplu Kullanım Sağlayıcıları Hakkında Yönetmelik

01.11.2007 tarihli “İnternet Toplu Kullanım Sağlayıcıları Hakkında Yönetmelik”, İnternet toplu kullanım sağlayıcılarının yükümlülükleri ve sorumlulukları ile denetimlerine ilişkin esas ve usulleri düzenlemek amacıyla, 5651 sayılı Kanuna dayanılarak hazırlanmıştır.

Yönetmeliğin 4 ile 9. maddeleri arasında ticari nitelikte olsun veya olmasın tüm İnternet toplu kullanım sağlayıcılarının yükümlülükleri belirlenmiştir. Buna göre, 4. maddede ticari olmayan İnternet toplu kullanım sağlayıcılarına, “konusu suç oluşturan içeriklere erişimi önleyici tedbirleri almak” yükümlülüğü yanında, yine bu kapsamda bir tedbir olarak nitelendirilebilecek “iç IP Dağıtım Loglarını¹⁰⁷ elektronik ortamda kendi sistemlerine kaydetmek” yükümlülüğü de getirilmiştir.

Yönetmeliğin 5. maddesinde ise, İnternet kafe olarak bilinen ticari amaçla İnternet toplu kullanım sağlayıcılarının yükümlülükleri belirlenmiştir. Bu kapsamda İnternet kafelerin yükümlülükleri şunlardır: a) Mülki idare amirinden izin belgesi almak, b) Konusu suç oluşturan içeriklere erişimi önleyici tedbirleri almak, c) TİB tarafından onaylanan içerik filtreleme yazılımını kullanmak, ç) Erişim sağlayıcılardan sabit IP

¹⁰⁷ Yönetmelikte “İç IP Dağıtım Logları”, “Kendi iç ağlarında dağıtılan IP adres bilgilerini, kullanıma başlama ve bitiş tarih ve saatini ve bu IP adreslerini kullanan bilgisayarların tekil ağ cihaz numarasını (MAC adresi) gösteren bilgileri” ifade etmektedir.

almak ve kullanmak, d) İç IP Dağıtım Loglarını elektronik ortamda kendi sistemlerine kaydetmek ve TİB tarafından 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 saklamak.

Yönetmelikte İnternet kafelerin işyeri olarak açılmasıyla ilgili hükümler 6. maddede, izin alınmadan açılan işyerleri konusu 7. maddede, izin belgesi sahipliği ve sorumlu müdür belirlenmesi 8. maddede yer almaktadır. İnternet kafelerde uyulması gereken kurallar 9. maddede,¹⁰⁸ İnternet kafelerin denetlenme usul ve esasları¹⁰⁹ ile bunlara uygulanacak idari para cezaları ise, 10. ve 11. maddelerde düzenlenmiştir.¹¹⁰ Yönetmeliğin 12. maddesinde İnternet kafelere verilen izinler ve faaliyetlerinin sona ermesine ilişkin bilgilerin 30 gün içinde mülki idare amiri tarafından TİB'na bildirilmesi öngörülmüştür. 13. maddede ise, TİB'nın, Kanunla verilen görevleri dolayısıyla gerekli gördüğü bilgileri doğrudan İnternet kafelerden veya mülki idare amirliklerinden talep edebilmesi mümkün kılınmıştır. Ayrıca, İnternet kafelerin TİB'nın taleplerini derhal yerine getireceği belirtilmiştir.

¹⁰⁸ Söz konusu kurallar şunlardır: a) 12 yaşından küçükler ancak, yanlarında veli veya vasileriyle işyerlerine girebilirler, b) 15 yaşından küçükler yanlarında veli veya vasileri olmadan saat 20.00'den sonra işyerlerine alınmazlar, c) Tütün ve tütün mamulleri içilemez, ç) İşyerlerinde 1117 sayılı Küçükleri Muzır Neşriyattan Koruma Kanununa aykırı hareket edilemez, d) İşyerlerinde 4250 sayılı İspirto ve İspirtolu İçkiler İhisi Kanununun 19. maddesi gereğince alkollü içecek satılması, bulundurulması veya sunulması yasaktır, e) İşyerlerinde 5846 sayılı Fikir ve Sanat Eserleri Kanunu kapsamında korunan hakların ihlal edilmesinin önlenmesi için gerekli tedbirler alınır, f) İşyerlerinde elektronik ve mekanik oyun alet ve makineleri bulunamaz, g) İşyerlerindeki bilgisayarlarda uyuşturucu veya uyarıcı madde alışkanlığı, intihara yönlendirme, cinsel istismar, müstehcenlik, fuhuş, şiddet, kumar ve benzeri kötü alışkanlıkları teşvik eden ve 18 yaşından küçüklerin psikolojik ve fizyolojik gelişimine olumsuz etkisi olabilecek oyunlar oynatılamaz, ğ) İşyerlerine giren ve çıkanların tespiti amacıyla gerekli kamera kayıt sistemi kurulur. Bu sistem aracılığıyla elde edilen kayıtlar yedi gün süreyle saklanır ve bu kayıtlar yetkili makamlar haricindeki kişi ve kuruluşlara verilemez.

¹⁰⁹ 10. maddeye göre, İnternet kafeler 5. maddede yer alan izin belgesi alma, konusu suç oluşturan içeriklere erişimi önleyici tedbirler alma, içerik filtreleme yazılımı kullanma, sabit IP alma ve kullanma, iç IP loglarını tutma ve saklama gibi konularla; 9. maddede yer alan işyerlerinde uyulması gereken kurallar konusunda mülki idare amirlikleri tarafından denetlenir. Bunun dışında genel güvenlik ve asayiş yönünden ise kolluk tarafından denetlenir ve tespit edilen mevzuata aykırı hususlar mülki idare amirliklerine gereği yapılmak üzere bildirilir.

¹¹⁰ 11. maddede, 5. maddedeki yükümlülüklerle aykırı hareket ettiği belirlenen İnternet kafelere, mülki idare amiri tarafından üçbin YTL onbeşbin YTL'ye kadar idari para cezası verilebileceği belirtilirken, 9. maddede belirtilen kurallara uymayanlara, mülki idare amiri tarafından 2559 sayılı Polis Vazife ve Salahiyet Kanunu'nun 6. maddesinin 1. fıkrasının (d) bendi uyarınca idari para cezası verileceği ifade edilmiştir. Ayrıca, idari para cezalarının, 5326 sayılı Kabahatler Kanunu'nda belirtilen usul ve esaslara göre uygulanacağı hatırlatılmıştır.

Böylece, 5651 sayılı Kanun'un ortaya çıkmasının en önemli sebeplerinden birisini oluşturan İnternet kafelere hem hukuki bir statü kazandırılırken hem de, biraz karışık bir yapı öngörmekle birlikte, denetim ve kontrol altına alınmalarıyla ilgili önemli bir düzenleme gerçekleştirilmiştir.

3.3.1.3.3 İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik

30.11.2007 tarihli “İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik”, 5651 sayılı Kanun’a dayanılarak yapılmış bir düzenlemedir.

Yönetmeliğin 4. maddesinde İnternet yayınlarının şu ilkelere uygun olması gerektiğine dikkat çekilmiştir: a) İnsan onuruna, temel hak ve hürriyetlere saygılı olmalıdır, b) Gençlerin ve çocukların fiziksel, zihinsel ve ahlaki gelişimini zedeleyecek türden içeriklere yer vermemelidir, c) Ailenin huzur ve refahını sağlayan hususlara zarar verecek nitelikte olmamalıdır, ç) Kişileri, uyuşturucu madde bağımlılığı, fuhuş, müstehcenlik ve kumar gibi kötü alışkanlıklara teşvik edici olmamalıdır. Ayrıca, herkesin kendisine yönelik haklarını ihlal eden İnternet yayınlarının içeriklerinden dolayı cevap ve düzeltme hakkı bulunmalıdır.

Yönetmeliğin 5.-9. maddelerinde içerik, yer ve erişim sağlayıcılarının Kanun’da genel olarak belirlenen yükümlülük ve sorumlulukları her biri için ayrı ayrı detaylandırılarak açıklanmıştır. Bu bağlamda ilk olarak her üç aktörün bilgilendirmeye ilişkin ortak yükümlülüklerinin neleri kapsadığı sayma yöntemiyle belirlenmiştir. İlk çıkarılan Yönetmeliğin 14. maddesinde erişim ve yer sağlayıcılar için sayılmış olan bilgilendirme yükümlülüğü bu Yönetmelikte 5. madde metnine aynen alınmış ve bu yükümlülüğe ticari veya ekonomik amaçlı içerik sağlayıcılar da dahil edilmiştir. İlave olarak bilgilendirme yükümlülüğü kapsamında ticari veya ekonomik amaçlı içerik sağlayıcılara, yer sağlayıcıya ilişkin tanıtıcı bilgileri, doğru, eksiksiz ve güncel olarak ana sayfasında bulundurma yükümlülüğü getirilmiştir.

6. maddede, içerik sağlayıcının İnternet ortamında kullanıma sunduğu içeriğe ilişkin sorumluluğu, Kanun'da yer aldığı şekli ile aynen tekrar etmiştir. Yönetmeliğin 7. maddesi yer, 8. maddesi erişim sağlayıcıların yükümlülüklerini konu edinmiştir. Keza, 7. madde ilk çıkarılan Yönetmeliğin 16. maddesinin, 8. madde de 15. maddesinin birebir aynısı olarak düzenlenmiştir. Sadece, erişim sağlayıcılara ayrıca, kullanıcılarına vekil sunucu hizmeti sunuyor ise; vekil sunucu trafik bilgisini bir yıl saklamak, bu bilgilerin doğruluğunu, bütünlüğünü oluşan verilerin dosya bütünlük değerlerini zaman damgası ile birlikte muhafaza etmek ve gizliliğini temin etmek yükümlülüğü de getirilmiştir.¹¹¹

Benzer şekilde idari para cezalarını düzenleyen Yönetmeliğin 9. maddesinde bahsi geçen hükümler, erişim ve yer sağlayıcılar için daha önce ilk çıkarılan Yönetmelikteki 18. maddede yapılan düzenlemelerin aynısıdır. İlave olarak sadece bilgilendirme yükümlülüğünü yerine getirmeyen içerik sağlayıcıları için de ikibin YTL'ndan onbin YTL'na kadar idari para cezası verilmesi öngörülmüştür. Keza, içeriğin yayından çıkarılması ve cevap hakkını düzenleyen Yönetmeliğin 10. ve 11. maddesi de, Kanun'un 9. maddesindeki düzenlemenin bir benzeridir.

Yönetmeliğin 12. maddesi Yasa'da geçen katalog suçlarını tekrar ederken, "Koruma tedbiri olarak erişimin engellenmesi kararı" başlıklı 13. madde, Kanun'un 8. madde 2. fıkrasındaki metnin bir benzeri olarak düzenlenmiştir. Yine, Yönetmelikte "İdari tedbir olarak erişimin engellenmesi kararı" başlıklı 14. madde de, Kanun'un 8. maddesi 4. fıkrasındaki düzenlemeyi aynen almış fakat, devamında ilave olarak idari tedbir kararının hakim onayına sunulması konusu metne dercedilmiştir.

Buna göre, re'sen verilen erişim engelleme kararlarından yurtdışı kaynaklı olanlara ilişkin herhangi bir işlem yapılmaz iken, içerik veya yer sağlayıcının yurt içinde

¹¹¹ Yönetmelikte "vekil sunucu trafik bilgisi", "İnternet ortamında erişim sağlayıcı tarafından kullanılan vekil sunucu hizmetine ilişkin talebi yapan kaynak IP adresi ve port numarası, erişim talep edilen hedef IP adresi ve port numarası, protokol tipi, URL adresi, bağlantı tarih ve saati ile bağlantı kesilme tarih ve saati bilgisi gibi bilgileri"; "dosya bütünlük değeri", "Bir bilgisayar dosyasının içindeki bütün verilerin matematiksel bir işleminden geçirilmesi sonucu elde edilen ve dosyanın içerisindeki verilerde bir değişiklik yapıp yapılmadığını kontrol için kullanılan dosyanın özünü belirten değeri" ifade etmektedir.

bulunması durumunda bu kararın, yirmidört saat içinde hakimın onayına sunulması ve hakimın kararını en geç yirmidört saat içinde vermesi öngörölmüştür. Bu süre içinde kararın onaylanmaması halinde idari tedbir kararı, Başkanlık tarafından derhal kaldırılır ve erişim sağlayıcılara bildirilerek gereğinin yerine getirilmesi istenir.

14. maddenin devamında yer alan TİB tarafından verilen erişimin engellenmesi kararının konusunu oluşturan yayını yapanların kimliklerinin belirlenmesi halinde, Cumhuriyet başsavcılığına suç duyurusunda bulunulacağına ilişkin düzenleme de Kanun 8. maddesinin 4. fıkrasından aynen alınmıştır. Sadece bu düzenlemeye TİB'nın, suç duyurusuna esas teşkil edecek verilerin elde edilebilmesi için kamu kurum ve kuruluşlarından bilgi ve belge talep edebileceği hükmü eklemiştir.

Yönetmelikte, Kanun'da yer almayan bir yenilik olarak erişimin engellenmesi kararında belirtilmesi gerekli hususlar uygulama birliğini sağlamak açısından 15. maddede düzenlenmiştir. Keza, Yönetmelikte "Erişimin engellenmesi usulü" başlıklı 16. madde, Kanun'un 8. maddesi 3. fıkrasına istinaden oluşturulmuştur. Yönetmelik, Kanun'da yer alan hakim, mahkeme veya Cumhuriyet savcısı tarafından verilen erişimin engellenmesi kararının birer örneğinin, gereği yapılmak üzere TİB'na gönderilmesine ilişkin düzenlemeye açıklık getirmiş ve kararların, doğrudan erişim sağlayıcılara gönderilemeyeceğini belirtmiştir. Kararlar TİB'na gönderilecek ve buradan kararlara ilişkin bilgiler gereği derhal yapılmak üzere elektronik ortamda erişim sağlayıcılara bildirilecektir.

16. maddenin devamında erişimin engellenmesine ilişkin prosedürler detaylı olarak açıklanmıştır. Buna göre, TİB bilgi ihbar merkezine kişiler veya kurumlarca yapılan ihbarların, teknik ve hukuki incelemeye alınacağı, söz konusu içerikte bu suçlardan birisinin olduğu konusunda yeterli şüphe sebebinin tespit edilmesi durumunda ihbarlara ilişkin işlem yapılacağı; aksi takdirde işleme alınmayacağı belirtilmiştir.

Devamında ise, erişimin engellenmesi kararlarına ilişkin bilgilerin, TİB'nca ilgili erişim sağlayıcılara elektronik ortamda bildirileceği ve kararların gereği erişim sağlayıcılar tarafından derhal ve en geç kararın bildirilmesinden itibaren 24 saat

içinde yerine getirileceği düzenlenmiştir. Ayrıca, erişimi engellenen yayınların, TİB tarafından hazırlanan ve mevcut sayfa yerine kararı veren merciin adı ile karar tarih ve sayısını belirten uyarı sayfasına yönlendirileceği belirtilmiştir.

Keza, erişim sağlayıcılara, TİB ile aralarındaki bağlantıdan aktarılacak erişimin engellenmesi kararlarını, kendi sistemlerinde derhal uygulayabilecek donanım ve yazılımı kurma ve gerekli düzenlemeleri yapma zorunluluğu getirmiştir. Ayrıca, erişim engellemesi kararına konu olan suçun olduğu konusunda yeterli şüphe sebebinin tespiti sürecinde, erişim engellenmeden önceki yayının durumunun elektronik ortamda TİB’nce arşivleneceği düzenlenmiştir.

Yönetmelikte 17. maddede düzenlenen “Erişimin engellenmesinin hükümsüz kalması” ve 18. maddede düzenlenen “Erişimin engellenmesinin kaldırılması”na ilişkin metinler de büyük oranda Kanun’da yer aldıkları şekliyle Yönetmeliğe aktarılmışlardır. İdari ve cezai yaptırımları düzenleyen 19. madde ise, idari tedbir ve koruma tedbiri olarak verilen erişimin engellenmesi kararlarını 24 saat içerisinde yerine getirmeyen erişim ve yer sağlayıcılara duruma göre faaliyet belgesi iptali, para veya hapis cezası gibi muhtelif cezalar öngörmektedir. 20. maddede ise, verilecek idari para cezalarına ilişkin kanun yoluna başvurulabileceği hatırlatılmıştır.

Yönetmeliğin 21. maddesi, Yasa’nın 10. maddesinde düzenlenen TİB’nin çalışma grupları oluşturabilmesine imkan tanıyan düzenlemeyi aynen almıştır. Yönetmelik, ek olarak çalışma kurullarının, Başkan’ın görevlendireceği personelin başkanlığında çalışmalarını yürüteceğini, çalışma usul ve esaslarının TİB’nce belirleneceğini ve her türlü giderlerinin TK tarafından karşılanacağını öngörmüştür. Keza, TİB’na Yönetmelikle verilen görevlerini yerine getirirken danışman kullanma, hizmet satın alma, tanıtma, kiralama gibi faaliyetlerde bulunabilme yetkisi de verilmiştir.

Yönetmeliğin “İşbirliği ve koordinasyon çalışmaları” başlıklı 22. maddesiyle, TİB’na bilişim ve İnternet alanındaki gelişmeleri izlemek amacıyla, uluslararası kurum ve kuruluşlarla işbirliği ve ortak çalışmalar yapma görevi verilmiştir. TİB’nin bu görevi yerine getirirken Türkiye’de ve yurt dışında yaptığı giderleri TK karşılayacaktır.

22. maddenin devamında TİB'na, katalog suçlarının işlenmesini konu alan her türlü temsili görüntü, yazı veya sesleri içeren ürünlerin tanıtımı, ülkeye sokulması, bulundurulması, kiraya verilmesi veya satışının önlenmesini temin etmek için yetkili ve görevli kolluk kuvvetleri ile soruşturma mercilerine, teknik imkanları dahilinde gereken her türlü yardımda bulunma veya koordinasyonu sağlama görevi vermiştir. Bu çerçevede TİB, söz konusu kurumlardan gelen talepleri inceler, değerlendirir ve katalog suçlarının önlenmesi için gerekli tedbirlerin alınmasını sağlayabilir.

22. maddenin son bölümünde Kanun'un 10. maddesinde düzenlenen İnternet Kurulu ile TİB'nın işbirliği ve koordinasyonu açıklanmıştır. Bu kapsamda TİB, Kurulca izleme, filtreleme ve engelleme yapılacak içeriğe sahip yayınların tespiti ve benzeri konularda yapılacak öneriler ile ilgili lazım olan her türlü tedbir veya kararları alacaktır. Düzenlemeye göre, TİB'na verilen görevlerin yerine getirilmesi amacıyla, Başkan veya görevlendireceği daire başkanı ile ilgili daire başkanları İnternet Kurulu toplantılarına katılacaktır. Keza Kurula, TİB'nın görevlerine ilişkin hususlarda Başkanlıktan görüş alınması zorunluluğu getirilmiştir.

3.3.1.3.4 Elektronik Haberleşme Sektörüne İlişkin Yetkilendirme Yönetmeliği

5809 sayılı Elektronik Haberleşme Kanunu'na dayalı olarak çıkartılan 28.05.2009 tarihli "Elektronik Haberleşme Sektörüne İlişkin Yetkilendirme Yönetmeliği", İnternet sektöründeki işletmecilerle ilgili bazı yeni düzenlemeler getirmiştir. Yönetmeliğin 19. maddesine göre mevcut veya yeni işletmeciler, elektronik haberleşme sistemleri üzerinden milli güvenlikle, 5397 sayılı Kanun, 5651 sayılı Kanun ve ilgili diğer kanunlarda getirilen düzenlemelerle ilgili taleplerin karşılanmasına yönelik teknik altyapıyı, elektronik haberleşme sistemini kurmak ve güncellemekle yükümlü tutulmuştur. Bu hususun temini için işletmecilerin yapacakları tüm harcamaları kendilerine ait olacak hizmetlerin usul, esas ve standartları BTK'unca belirlenecektir.

Yönetmeliğe göre aynı şekilde, işletmeciler, bahsi geçen düzenlemelerle ilgili olarak, tüm harcamaları kendilerine ait olmak üzere; ilgili mevzuat gereği verilmesi gereken

bilgi, belge ve veriyi BTK tarafından belirlenecek usul, esas ve standartlarda eksiksiz ve zamanında kanunen yetkili mercie teslim etmekle yükümlüdür. Keza, aynı mevzuat çerçevesinde her türlü sistemin işletilmesi bakımından, altyapı kullanımının sağlanması ile söz konusu sistemlerin çalışır vaziyette tutulması için gerekli donanım, yazılım, bakım, onarım, teknik destek gibi gerekli tedbirleri almakla ve bunları etkileyen donanım, yazılım, altyapı ve şebekeye ilişkin değişiklikleri BTK onayını alarak yapmakla yükümlüdürler.

Böylece, İnternet sektörü de dahil olmak üzere elektronik haberleşme sektöründe faaliyet gösteren tüm işletmelerin denetim ve kontrolü için geniş bir çerçeve çizilmiş ve kapsamlı bir düzenleme yapılmıştır.

3.3.1.3.5 Elektronik Haberleşme Sektöründe Tüketici Hakları Yönetmeliği

5809 sayılı Elektronik Haberleşme Kanunu’na istinaden çıkarılan 28.07.2010 tarihli “Elektronik Haberleşme Sektöründe Tüketici Hakları Yönetmeliği” İnternetin güvenli kullanımıyla ilgili yeni bir düzenleme getirmiştir. Buna göre, Yönetmeliğin “İnternetin güvenli kullanımı” başlığını taşıyan 10. maddesinde işletmecilerin, İnternetin güvenli kullanımına ilişkin olarak tüketicileri bilgilendirmekle, TİB tarafından belirlenen yasadışı ve zararlı içeriklere karşı tüketicilerin korunmasına yönelik altyapı seviyesindeki hizmetleri ek ücret olmaksızın seçenekli olarak sunmakla yükümlü oldukları düzenlenmiştir. Ayrıca, bu hususun uygulamasına ilişkin usul ve esasların BTK tarafından belirleneceği belirtilmiştir.

Bu düzenlemenin Türkiye’deki İnternet içerik düzenlemeleri açısından önemli bir adım olduğu söylenebilir. Böylece, konunun tüketici talepleri boyutuyla ilk defa bu önemde ele alındığı ve mevzuata yansıtıldığı görülmektedir. Bu adımla, kullanıcı açısından mecburi “tek bir İnternet” değil, tercihe dayalı seçenekli “birden çok İnternet”in önü açılmıştır. Zira, düzenleme, tercihlerine göre kullanıcılara farklı kullanıcı profili seçebilmelerine imkan sağlayan “Güvenli İnternet” uygulamasının hukuki dayanağını oluşturmuştur.

3.3.1.3.6 Bilgi Teknolojileri ve İletişim Kurumu Teşkilat Yönetmeliği

08.06.2011 tarihli “BTK Teşkilat Yönetmeliği”nin “Telekomünikasyon İletişim Başkanlığı” başlığını taşıyan 18. maddesi; TİB’nin, 5651 sayılı Kanun kapsamında katalog suçları oluşturan içeriğe sahip faaliyet ve yayınları önlemeye yönelik çalışmalar yapmak, İnternet ortamında yapılan yayınların içeriklerini izleyerek 5651 sayılı Kanun kapsamına giren suçların işlendiğinin tespiti halinde, bu yayınlara erişimin engellenmesine yönelik olarak Kanunda öngörülen gerekli tedbirleri almakla görevli olduğunu belirtmektedir. Böylece bu Yönetmelik, ilgili mevzuata göre TİB’nin Türkiye’deki İnternet içerik düzenlemesine ilişkin en önemli yetkili, sorumlu ve görevli kamu kurumu olduğunu açık bir şekilde tekrar vurgulamıştır.

3.3.2 İnternet İçerik Düzenlemesi İle İlgili Kurumlar

Türkiye’de genel olarak İnternet, özel olarak ise İnternet içeriğinin düzenlenmesi ile doğrudan veya dolaylı ilgili kurumların başlıcaları Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, BTK, TİB, İnternet Geliştirme Kurulu, Çocuk ve Aile Profil Kriterleri Çalışma Kurulu, Çocukları Muzır Neşriyattan Koruma Kurulu, Sinema Genel Müdürlüğü Değerlendirme ve Sınıflandırma Kurulu, RTÜK, Bilgi Toplumu Dairesi Başkanlığı ve Aile ve Toplum Hizmetleri Genel Müdürlüğü’dür.

3.3.2.1 Ulaştırma, Denizcilik ve Haberleşme Bakanlığı

Türkiye’de İnternette sorumlu Bakanlık olan Ulaştırma Bakanlığı’nın 1987 tarihli ve 3348 sayılı Yasa ile oluşturulan teşkilat yapısı ve ismi, 1.11.2011 tarihli ve 655 Karar sayılı "Ulaştırma, Denizcilik ve Haberleşme Bakanlığı (UDHB) Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname" ile önemli bir değişikliğe uğramıştır. Düzenleme, Bakanlığın “haberleşme” boyutlu olarak İnterneti ilgilendiren görevlerine 2. maddede yer verirken, 13. madde bu görevleri detaylandırarak teşkilat içindeki muhatabın Haberleşme Genel Müdürlüğü olduğunu belirlemiştir. Kararname ayrıca, İnternetin düzenlenmesine ilişkin kurumsal bir yapı olarak 29. madde ile sürekli ve geçici kurullarla ilgili düzenleme kapsamında İnternet Geliştirme Kurulu’nun ihdasını öngörmüştür.

Diğer yandan, Elektronik Haberleşme Kanunu İnterneti ilgilendiren bir takım düzenlemeler getirmiş ve bunlarla Bakanlığı ilişkilendirerek Bakanlığa İnternetle ilgili birçok görev ve yetki vermiştir. Bu bağlamda dikkat çeken düzenlemelerden birisi İnternet alan adlarının tahsis ve yönetimine ilişkindir. Kanun'un 35. maddesi İnternet alan adlarının tahsisini yapacak kurum veya kuruluşun tespiti ile alan adı yönetimine ilişkin usul ve esasların Ulaştırma Bakanlığı tarafından belirleneceğini hükme bağlamıştır. Böylece konu ile ilgili görev ve yetki Bakanlığa verilmiştir.

Bakanlığa yakın dönemde İnternetle ilgili ulusal siber güvenliğin sağlanmasına ilişkin çeşitli görevler de tevdi edilmiştir. Bakanlar Kurulunca alınan 2012/3842 sayılı "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar" ile siber güvenlikle ilgili alınacak önlemleri belirlemek, hazırlanan plan, program, rapor, usul, esas ve standartları onaylamak ve bunların uygulanmasını ve koordinasyonunu sağlamak amacıyla UDHB'nın başkanlığında "Siber Güvenlik Kurulu" kurulmuştur.¹¹² Karar ile Bakanlığa konuyla ilgili bir takım kritik görevler verilmiş ve verilen bu görevleri BTK ve diğer kamu kurum ve kuruluşları aracılığıyla yerine getirebileceği hüküm altına alınmıştır.

Böylece, giderek daha büyük bir tehlike haline gelen ve bu zamana kadar her devlet dairesinin net bir strateji ve koordinasyon olmaksızın kendince bir şeyler yapmaya çalıştığı siber tehditlere karşı, bu karar çerçevesinde ilk kez, devletin tüm kurum ve kuruluşları bir koordinasyon içinde hareket edecek hale getirilmeye başlanmıştır.

Fakat bu defa da Bakanlar Kurulu Kararı'nın 5. madde 4. fıkrasında yer alan "Bakanlık, kamu düzeninin korunması açısından zorunlu hallerde, ilgili makamlar ve Siber Güvenlik Kurulunca yapılacak talep çerçevesinde, ulusal siber güvenlikle ilgili tedbirleri alır" ibaresinin son derece ucu açık olduğu, Bakanlık inisiyatifiyle bunun site kapatmalara veya siber müdahalelere zemin hazırlayabileceği belirtilmektedir.

¹¹² Karar da 4. maddeye göre Kurul'a Dışişler Bakanlığı, İçişleri Bakanlığı, Milli Savunma Bakanlığı, Kamu Düzeni ve Güvenliği Müsteşarlığı, MİT Müsteşarlığı, Genelkurmay Başkanlığı Muhabere Elektronik ve Bilgi Sistemleri Başkanlığı, BTK, TUBİTAK, Mali Suçları Araştırma Kurulu, TİB ve UDHB tarafından belirlenecek diğer bakanlık ve kamu kurumlarının katılımı öngörülmüştür.

Sonuçta etkili bir “siber güvenlik politikası” ile “sansür uygulamalarını” birbirinden ayıran oldukça ince bir çizginin olduğu hatırlatılmaktadır (Aru, 2012).

Görüldüğü gibi Bakanlık hukuki açıdan ve kurumsal yapısı itibariyle bilgi-iletişim alanlarında hem politika belirleme, kural koyma, düzenleme ve denetleme, hem de ana hizmet birimlerinin proje ve faaliyetlerini yerine getirme bakımından önemli ve kapsamlı görev ve yetkilere sahiptir. Bakanlık ile ilişkili bağımsız üst kurul olarak oluşturulan BTK, Bakanlığın doğrudan İnternete yönelik görevlerinin önemli bir kısmını üstlenmiştir.

3.3.2.2 Bilgi Teknolojileri ve İletişim Kurumu

4502 sayılı Kanun’la kurulmuş bulunan TK, 5809 sayılı Elektronik Haberleşme Kanunu ile yeni bir düzenlemeye tabi tutulmuş ve adı “Bilgi Teknolojileri ve İletişim Kurumu” (BTK) olarak değiştirilmiştir. BTK’nın Türkiye’de İnternet özelinde en yetkili kurum olduğu söylenebilir. Nitekim, Elektronik Haberleşme Kanunu BTK’ya İnternetle ilgili birçok görev ve yetkiler vermiştir.

Kanun’da, elektronik haberleşme hizmetlerinin yetkilendirilmesi konusunda özellikle “yetkilendirme usulü” başlığı altında 9. maddenin 9. ve 11. fıkralarıyla BTK’ya verilen yetkiler oldukça dikkat çekicidir. Düzenlemeye göre 9. fıkra BTK’nın kullanım hakkı¹¹³ verilmesi taleplerini, milli güvenlik, kamu düzeni, kamu sağlığı ve benzeri kamu yararı gerekleri, tahsis edilmesi gereken kaynakların yetersizliği ve ihale aşamasında belirlenen yeterlik şartlarının sağlanmaması sebepleriyle reddedebilmesine imkan tanırken; 11. fıkrası Kurum’a kamu güvenliği, kamu sağlığı ve benzeri kamu yararı gereklerinden kaynaklanan sebeplerin tespiti halinde, şirketlerin elektronik haberleşme alanında faaliyete geçmelerini veya elektronik haberleşme sağlamalarını gerektiğinde Bakanlığın görüşünü de alarak engelleyebilme yetkisi vermektedir. Bu düzenlemelerle ve özellikle 11. fıkraya dayanarak, elektronik haberleşmenin ve İnternet erişiminin engellenmesinin veya

¹¹³ Kanun’a göre “kullanım hakkı”, “Frekans, numara, uydu pozisyonu gibi kıt kaynakların kullanılması için verilen hakkı” ifade etmektedir.

kesintiye uğratılmasının kamu düzeni, kamu güvenliği, milli güvenlik, kamu sağlığı, kamu yararı gibi gerekçelerle mümkün hale getirildiği görülmektedir.

Kanun, işletmecilerin hak ve yükümlülüklerini düzenlediği 12. maddesinde BTK'nın işletmecilere sektörün ihtiyaçları, uluslararası düzenlemeler, teknolojiye meydana gelen gelişmeleri gözeterek bir takım hususlarda mevzuat doğrultusunda yükümlülükler getirebileceğinden bahsetmektedir. Buna göre, “Kişisel veri ve gizliliğin korunması” ile “tüketicinin korunması” hususları, BTK'nın bu kapsamda yükümlülükler kaynaklık teşkil edebileceği konular arasındadır.

Nitekim, Kanun'daki bu hükme dayanarak, “Elektronik Haberleşme Sektöründe Tüketici Hakları Yönetmeliği”yle İnternetin güvenli kullanımıyla ilgili yeni bir düzenlemeye gidilmiştir. Buna göre, işletmecilere, İnternetin güvenli kullanımına ilişkin olarak tüketicileri bilgilendirme, TİB tarafından belirlenen yasadışı ve zararlı içeriklere karşı tüketicilerin korunmasına yönelik altyapı seviyesindeki hizmetleri ek ücret olmaksızın seçenekli olarak sunma yükümlülüğü getirilmiştir.

Kanun'un 12. maddesi ise işletmecilere, elektronik haberleşme sistemleri üzerinden milli güvenlikle ve 5397 ile 5651 sayılı kanunlar ve ilgili diğer kanunlarda getirilen düzenlemelerle ilgili taleplerin karşılanmasına yönelik teknik alt yapıyı, BTK tarafından belirlenecek süre içerisinde ve tüm harcamaları kendilerine ait olmak üzere kurmakla yükümlü kılmıştır. Nitekim, “Elektronik Haberleşme Sektörüne İlişkin Yetkilendirme Yönetmeliği” bu hükme dayanarak konuya ilişkin biraz daha geniş düzenleme yapmıştır.

Elektronik Haberleşme Kanunu'yla Ulaştırma Bakanlığı'na verilen ve daha sonra BTK'ya görev ve yetki olarak tevdi edilen İnternetle ilgili düzenlemelerden birisi de İnternet alan adlarının tahsisi ve yönetimi konusudur. Başlangıçta Türkiye'de alan adı yönetimi, 1991 yılından itibaren Türkiye'yi ilk defa İnternete bağlayan ODTÜ bünyesinde devam etmekteydi. 1991-1998 yılları arasında ODTÜ Bilgi İşlem Dairesi Başkanlığınca yerine getirilen bu görev 1998 yılından itibaren yine üniversite bünyesindeki “Nic.tr” isimli kuruluşa devredilmiştir (Nic.tr, 2012).

Bakanlık görev ve yetki kendisine geçtikten sonra 3.3.2009 tarihli kararıyla "İnternet Alan Adları" tahsisine ilişkin iş ve işlemlerin yürütülmesi hususunda BTK'yı yetkilendirmiştir. Bu şekilde ODTÜ'den alınarak BTK'ya verilen alan adları yönetimi hukuki bir çerçeveye de kavuşmuştur. BTK bu alandaki düzenleyici ve denetleyici görevi üstlenmiş ve ".tr" uzantılı İnternet alan adlarına ilişkin danışma görevini İnternet Alan Adları Ulusal Koordinasyon Kurulu (tr.UKK)'na devretmiştir. Bu çerçevede yapılan çalışmalar sonucunda, konuyla ilgili tarafların katkılarının da değerlendirildiği etkileşimli bir sürecin sonunda hazırlanan "İnternet Alan Adları Yönetmeliği" 7.11.2010 tarihinde yayınlanarak yürürlüğe girmiştir (Dal, 2010: 491).

BTK bu Yönetmeliğin 14. maddesinin 1. fıkrasının (a) bendine göre, ".tr" Ağ Bilgi Sistemi'ni (TRABİS)¹¹⁴ kurmak ve işletmek veya belirlediği usul ve esaslar çerçevesinde üçüncü bir tarafça kurulması ve işletilmesini sağlamakla görevlidir. Bu çerçevede TRABİS kurulum çalışmaları devam etmektedir (TRABİS, 2013).

Yakın zamanda BTK ile anılan konulardan birisi de "siber güvenlik"tir. Giderek daha büyük bir tehdit haline gelen siber saldırılara karşı ulusal ölçekte karşı koyma ve gerekli tedbirleri alma maksadıyla yürütülen çalışmalarda odakta yer alan kurum BTK olmaktadır. BTK tarafından siber güvenliğin sağlanmasına yönelik olarak son yıllarda yürütülmekte olan çalışmalar, Elektronik Haberleşme Kanunu ile kendisine verilen yetkilere dayanmakta ve BTK'nın Türkiye'yi temsilen üyesi bulunduğu ITU'nun çalışmalarına paralellik göstermektedir (BTK, 2013b).

Bu çerçevede BTK, önce TÜBİTAK ile "Ulusal Siber Güvenlik Tatbikatı-2011"¹¹⁵ ve daha sonra elektronik haberleşme sektöründe faaliyet gösteren 12 işletmecinin katılımı ile "Siber Kalkan Tatbikatı-2012" organizasyonlarını gerçekleştirmiştir (BTK, 2012a).

¹¹⁴ Yönetmelik TRABİS'i, ".tr" uzantılı İnternet alan adı sisteminin ve buna ait merkezi veritabanının işletilmesine, rehberin oluşturulmasına, güncellenmesine ve rehberlik hizmetinin sunulmasına ve alan adı başvuru işlemlerinin gerçek zamanlı olarak yapılmasına imkan veren, tüm bu faaliyetlerin güvenli ve iş sürekliliğini sağlayacak şekilde gerçekleştirildiği sistem" olarak tanımlanmaktadır.

¹¹⁵ Tatbikat, finans, bilgi teknolojileri ve iletişim, eğitim, savunma, sağlık sektörlerinin; adli birimlerin, kolluk kuvvetlerinin ve çeşitli bakanlıkların ilgili birimlerinin temsilcilerinden oluşan 41 kamu kurumu ve özel sektör kuruluşunun ve STK'larının katılımıyla gerçekleştirilmiştir (BTK, 2011).

Siber Güvenlik Kurulu'nun kurulması, başkanlığının UDHB'na verilmesi ve Bakanlığın siber güvenlikle ilgili görevlerini BTK ve diğer kamu kurum ve kuruluşları aracılığı ile yerine getirmesine karar verilmesinden sonra BTK'nın ulusal siber güvenliğin sağlanmasıyla ilgili çalışmalarının artarak süreceği öngörülebilir. Nitekim, UDHB'nın koordinasyonunda BTK ve TÜBİTAK'ın birlikte yürüttüğü ve siber saldırılara karşı hazırlıklı olunmasını amaçlayan "Ulusal Siber Güvenlik Tatbikatı-2013", 61 kamu ve özel sektör kuruluşu ile STK'larının katılımıyla 24 Aralık 2012 - 11 Ocak 2013 tarihleri arasında gerçekleştirilmiştir (BTK, 2013c).

Bu süreçte Siber Güvenlik Kurulu, Siber Güvenlik Strateji Belgesi ile Eylem Planı'nı onaylamış ve bu belgeye istinaden Ulusal Siber Olaylara Müdahale Merkezi (USOM)'nin kurulmasına karar verilmiştir (Sabah, 10.01.2013). Hazırlıkları tamamlanan USOM, BTK bünyesindeki TİB'nda faaliyete başlamıştır.

Elektronik Haberleşme sektörünü düzenlemek ve denetlemekle görevli ve yetkili olan BTK'nın görev alanlarını kısaca; yetkilendirme, denetleme, uzlaştırma, tüketici haklarını koruma, sektörde rekabeti sağlama, bilgi teknolojileri, teknik düzenlemeler, spektrum yönetimi ve denetimi olarak ifade edebiliriz (BTK, 2013d).

BTK, Bilgi Teknolojileri ve İletişim Kurulu ile Başkanlık teşkilatından oluşmaktadır. Kurul, Kurum'un karar organıdır ve biri başkan 7 üyeden oluşmaktadır. Başkan ve Kurul üyeleri Bakanlar Kurulu tarafından 5 yıllık süre için atanmaktadır. Kurul üyelerinin ikisi telekomünikasyon sektörünü temsilen işletmecilerin göstereceği adaylar arasından, birisi de tüketicileri temsilen atanmaktadır. Başkan ve diğer üç üye ise kamudan gelmektedir. Kurul Başkanı Kurum'un en üst idari amiridir ve Kurum'un yönetim ve temsil yetkisine sahiptir. Kurum'un hizmet birimleri; hukuk müşavirliği, daire başkanlıkları ve müdürlükler şeklinde teşkilatlanan ana hizmet, danışma ve yardımcı hizmet birimleriyle bölge müdürlükleri şeklinde teşkilatlanan taşra teşkilatı birimlerinden oluşmaktadır (BTK, 2013e).

BTK, içerik düzenlenmesine yönelik temel yetkilerini 5651 sayılı Kanun vesilesiyle bünyesinde bulundurduğu TİB'na verilen yetki ve sorumluluklardan almaktadır.

3.3.2.3 Telekomünikasyon İletişim Başkanlığı

Haberleşme hürriyeti açısından istisnaları düzenleyen 2559, 2803 ve 2937 sayılı Kanunlarda değişiklik yapan TİB'nin kuruluşuna ilişkin 5397 sayılı “Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun” 23.07.2005 tarihinde Resmi Gazete’de yayınlanmıştır. 2559 sayılı Polis Vazife ve Salahiyet Kanunu’nun ek 7. maddesi, 2803 sayılı Jandarma Teşkilat, Görev ve Yetkileri Kanunu’nun ek 5. maddesi ve 2937 sayılı Devlet İstihbarat Hizmetleri ve MİT Kanunu’nun 6. maddesinde değişiklikler yapan sözkonusu Kanun, yeni kurulacak olan TİB’na önemli görev ve sorumluluklar yüklemiştir.

5397 sayılı Kanun, ilgili Kanunların Polis, Jandarma ve MİT’ına, 5271 sayılı Ceza Muhakemesi Kanunu hükümleri çerçevesinde yetki verdiği iletişimin tespiti, dinlenebilmesi, sinyal bilgilerinin değerlendirilebilmesi ve kayda alınabilmesine ilişkin faaliyetlerine yeni bir düzenleme getirmiştir. Buna göre, bahsi geçen telekomünikasyon yoluyla yapılan iletişimin adli, istihbari ve önleyici amaçlı olarak denetlenmesi işlemlerinin tek merkezden ve TİB’nca yürütülmesini öngörmüştür. Bu amaçla kurulan TİB, eski adıyla TK yeni adıyla BTK bünyesinde faaliyet gösterecek ve Kurum başkanına doğrudan bağlı olacaktır.

Kanun’un 1. maddesine göre, bu maddede belirlenen usul ve esaslara aykırı dinlemeler hukuken geçerli sayılmayacak ve bu şekilde dinleme yapanlar hakkında 5237 sayılı TCK hükümlerine göre işlem yapılacaktır. Düzenlemeye göre, TİB’nda bir başkan ile daire başkanlıklarının yanı sıra MİT, EGM ve Jandarma Genel Komutanlığı’nın ilgili birimlerinden birer temsilci bulunacaktır. TİB Başkanı, Kurul üyelerinin sahip olduğu özlük haklarına sahip olacak ve TK Başkanı’nın teklifi üzerine Başbakan tarafından atanacaktır. Nitekim, 11.08.2005 tarihinde Cumhuriyet Savcısı Fethi ŞİMŞEK, TİB Başkanı olarak bu göreve atanmıştır (TİB, 2013).

5397 sayılı Kanun’dan sonra Başkanlığın “Kuruluş, Görev ve Yetkileri Hakkında Yönetmelik” 10.11.2005 tarihinde yayınlanmıştır. Kuruluş ve altyapı çalışmalarını tamamlayan TİB, 23.7.2006 tarihinde fiilen faaliyete başlamıştır (TİB, 2013). 5651

sayılı Kanunla TİB'ına, İnternet ortamı ve bu ortamda işlenen bazı suçlarla mücadeleyle ilişkin görevler verilmiştir. Bu doğrultuda anılan görevleri yerine getirmek üzere İnternet Daire Başkanlığı ihdas edilmiştir. 5651 sayılı Kanuna ilişkin görevler ile İnternet Daire Başkanlığı'nın Başkanlık teşkilatındaki yerini düzenleyen Yönetmelik ise, 07.08.2009 tarihinde yayımlanarak yürürlüğe girmiştir.

23.11.2007 tarihinde TİB İnternet Bilgi İhbar Merkezi faaliyete geçmiş ve ihbar almaya başlamıştır. 30.11.2007 tarihinde "İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik" in yürürlüğe girmesiyle, TİB tarafından İnternet sitelerine erişimin engellenmesine ilişkin kararların uygulanmasına başlanmıştır. Keza, TİB'in hazırladığı bilinçlendirme siteleri "www.guvenliweb.org.tr" 23.3.2008 tarihinde, "www.guvenlicocuk.org.tr" 23.2.2010 tarihinde yayına başlamıştır (TİB, 2013).

Diğer yandan, Anayasa Mahkemesi'nin 29.01.2009 tarihli Kararı ile, 5397 sayılı Kanun'da yer alan Telekomünikasyon İletişim Başkanı'nın, TK Başkanı'nın teklifi üzerine Başbakan tarafından atanmasına ilişkin düzenleme iptal edilmiştir.

TİB'nda "Teknik İşletme Daire Başkanlığı" ve "Bilgi Sistemleri Daire Başkanlığı" kurulmasına ilişkin Yönetmelik 09.09.2011 tarihinde yayımlanarak yürürlüğe girmiştir. Böylece, TİB bünyesinde İdari, Hukuk ve İnternet Dairesi'nden sonra Teknik İşletme ve Bilgi Sistemleri Daire Başkanlıkları da teşekkül ettirilmiştir.

Son dönemde TİB'na siber güvenlikle ilgili görevler de verilmiştir. Siber Güvenlik Strateji Belgesi ile Eylem Planı belgesinde yer alan Ulusal Siber Olaylara Müdahale Merkezi (USOM)'ni kurma görevi 2013 yılı Şubat ayında TİB'na tevdi edilmiştir. USOM, 2013 yılı Mayıs'ında TİB bünyesinde faaliyete başlamıştır (Vidinli, 2013).

USOM, siber ortamdaki tehditlerin hızla belirlenmesi, önlemlerin geliştirilmesi ve paylaşılmasını sağlayan, kurum ve kuruluşların siber olaylara müdahale yeteneği kazanması için çalışan, ülkeyi etkileyebilecek tehditlere karşı 7/24 müdahaleyi öngören, sektörel ve kurumsal "Siber Olaylara Müdahale Ekipleri" (SOME) oluşturan, SOME'lere ve ilgili olduğu sektöre özel bilgilendirme ve bilinçlendirme

faaliyetleri yürüten bir merkez olarak kurulmuştur. Bu kapsamda, ilgili uluslararası kuruluşlar, İnternet aktörleri, SOME'ler, araştırma merkezleri, özel sektör kuruluşları ile kolluk ve adli merciler ile işbirliğini öngörmektedir (Vidinli, 2013).

3.3.2.4 İnternet Geliştirme Kurulu

5651 sayılı Kanun öncesinde İnternet Kurulu, 17.04.1987 tarihli ve 3348 sayılı “Ulaştırma Bakanlığının Teşkilat ve Görevleri Hakkında Kanun”un Ek 1. maddesine dayanılarak Ulaştırma Bakanlığı bünyesinde danışma kurulu niteliğinde oluşturulan bir kurumdur. Kurulun amacı, İnternet hizmet ve uygulamalarının kısa, orta ve uzun vadeli hedeflerini belirlemek, bu hedeflere yönelik ulusal stratejik kararların alınması ve uygulanması gibi hususlarda Ulaştırma Bakanlığına tavsiyelerde bulunmak ve konu ile ilgili birimler arasında koordinasyon sağlamaktır (Günaydın, 2010: 43).

5651 sayılı Yasa'nın yeni bir İnternet Kurulu oluşturması üzerine mevcut kurul sona ermiştir. Yasa, yeni Kurulun Adalet ve İçişleri Bakanlığı, çocuk, kadın ve aileden sorumlu Devlet Bakanlığı ile BTK ve ihtiyaç duyulan diğer bakanlık, kamu kurum ve kuruluşları ile İSS'leri ve ilgili STK arasından seçilecek bir temsilcinin katılımıyla oluşturulmasını öngörmüştür. TİB'na, Kurul ile gerekli işbirliği ve koordinasyonu sağlama; Kurulca izleme, filtreleme ve engelleme yapılacak içeriği haiz yayınların tespiti ve benzeri konularda yapılacak önerilerle ilgili gerekli her türlü tedbir veya kararları alma görevi vermiştir. Düzenlemenin son cümlesi ile Kurul'a içeriklerle ilgili tedbirler kapsamındaki kurumsal işbirliği mekanizmaları içerisinde çok önemli ve ayrıcalıklı bir işlev yüklendiği anlaşılmaktadır (Altınay, 2011: 75-76).

Bilahere, 2011 tarihli 655 Sayılı KHK'nin 29. maddesiyle İnternet Kurulunun adı “İnternet Geliştirme Kurulu” olarak değiştirilirken, Kurul'un; Bakanlığa, görev alanına giren konularla ilgili olarak çalışmalarda bulunmak, araştırma, inceleme ve değerlendirme yapmak üzere bakanlık, kurum ve kuruluş, STK temsilcileri ve konuyla ilgili uzmanların katılımıyla, sürekli faaliyette olması hükme bağlanmıştır.

Aynı düzenleme, Kurul'un görevlerini şöyle belirlemiştir: a) İnternet ortamının ekonomik, ticari ve sosyal hayat ile bilim, eğitim ve kültür alanında etkin, yaygın,

kolay erişilebilir olarak kullanımını teşvik edecek politika ve strateji önerileri hazırlamak, b) Türk Kültürü, Türk Tarihi ve Türk Dünyasıyla ilgili bilgilerin İnternet ortamında daha fazla yer alması ve bunların tanıtılması hususunda çalışmalar yapmak, yaptırmak ve öneriler hazırlamak, c) İnternet ortamının güvenli, serbest, özgür ve faydalı kullanımı ile katma değer üretmesine yönelik öneriler hazırlamak, ç) Bakan tarafından verilen benzeri görevleri yapmak. Kurul, Başkan da dahil 4 STK temsilcisi, BTK Başkanı, Haberleşme Genel Müdürü ve 1 akademisyen olmak üzere 7 üyeden oluşmaktadır (İnternet Geliştirme Kurulu, 2013).

3.3.2.5 Çocuk ve Aile Profil Kriterleri Çalışma Kurulu

Elektronik Haberleşme Kanun’una istinaden çıkartılan 28.07.2010 tarihli “Elektronik Haberleşme Sektöründe Tüketici Hakları Yönetmeliği” İnternetin güvenli kullanımıyla ilgili yeni bir düzenleme getirmiştir. Yönetmeliğin 10. maddesiyle, işletmecilerin İnternetin güvenli kullanımına ilişkin olarak tüketicileri bilgilendirmekle, TİB tarafından belirlenen yasadışı ve zararlı içeriklere karşı tüketicilerin korunmasına yönelik altyapı seviyesindeki hizmetleri ek ücret olmaksızın seçenekli olarak sunmakla yükümlü oldukları düzenlenmiş ve bu hususun uygulamasına ilişkin usul ve esasların BTK tarafından belirlenebileceği belirtilmiştir.

Bu çerçevede BTK, 24.08.2011 tarihli ve 2011/DK-14/461 Nolu Kurul Kararı ile “Güvenli İnternet Hizmetine İlişkin Usul ve Esaslar”ı belirlemiştir. Buna göre işletmecilere, “Güvenli İnternet Hizmeti”ni talep eden abonelere “çocuk” ve “aile” olmak üzere iki farklı profil imkanını ücretsiz olarak sunma zorunluluğu getirilmiştir. 10. madde, “Çocuk ve Aile Profil Kriterleri Çalışma Kurulu’nun yapısı ve görevleri” başlığı altında; Çocuk ve Aile Profil listelerinin oluşturulmasına ilişkin kriterlerin, Çocuk ve Aile Profil Kriterleri Çalışma Kurulu tarafından tespit edileceğini belirtmiş ve ihdas edilen Kurul’un yapısını ve görevlerini düzenlemiştir (BTK, 2011b).

Buna göre, Çocuk ve Aile Profil Kriterleri Çalışma Kurulu, BTK koordinasyonunda 11 üyeden oluşmaktadır. Kurul’da, biri başkan olmak üzere BTK’dan 3, Aile ve Sosyal Politikalar Bakanlığında 2, İnternet Kurulu’nun sivil toplum temsilcisi

üyelerinden 2, Türkiye Dijital Oyun Federasyonu'ndan 1 ve psikoloji, pedagoji, sosyoloji, hukuk gibi ilişkili alanlarda uzmanlığı olan kişiler arasından BTK tarafından seçilen 3 üye bulunmaktadır. Kurul'un, tespit ettiği ilkeler çerçevesinde, Çocuk ve Aile Profil listeleri TİB tarafından belirlenmektedir. 11. madde, Kurul'a ayrıca, BTK'nın müracaatı ile kullanıcılar ve İnternet site sahiplerinin yapmış olduğu başvuru ve itirazların değerlendirilmesi görevi de vermiştir (BTK, 2011b).

Oluşturulan bu Kurul, seçenekli ve talebe bağlı olarak verilen Güvenli İnternet Hizmetinin temelini oluşturan çocuk ve aile profillerinin kriterlerini belirlemesi açısından büyük önem arz etmektedir. Bir tür İnternet içeriklerini sınıflandırmaya yarar ölçütleri belirleme işlevi de gören bu Kurul'da, İnternetin tarafı olan tüm kesimlere söz hakkı tanınması amacıyla, konunun bağımsız uzmanları ile STK temsilcilerine de yer verilmesi oldukça önemlidir. Bu yaklaşım, son dönemde revaçta olan regülasyon çalışmalarının yönetim ilkesine göre "birlikte düzenleme" anlayışıyla yapılmasına yönelik beklentilere uygun düşmektedir. Aksi takdirde, Güvenli İnternet Hizmeti kapsamındaki profillerin içeriğinin (alan adı listelerinin) hangi kriterlere göre, kim tarafından oluşturulacağı hususlarında daha büyük tartışmaların yaşanması kaçınılmaz olacaktır.

3.3.2.6 Küçükleri Muzır Neşriyattan Koruma Kurulu

18 yaşından küçük çocukların zararlı içerikten korunmasına ilişkin olarak 5237 sayılı TCK'nın 226. maddesinde yer alan düzenleme dışında 1927 tarihli 1117 sayılı Küçükleri Muzır Neşriyattan Koruma Kanunu'nda da hükümler bulunmaktadır. Atatürk döneminde çıkartılan 1117 sayılı Kanun, muzır olarak adlandırdığı zararlı içeriğin belirlenmesi konusunda Küçükleri Muzır Neşriyattan Koruma Kurulu'nu ihdas etmiştir. MEB bünyesinde oluşturulan Kurul'un asli işi 1 aylık veya daha uzun süreli aralıklarla yapılan yayınları incelemektir. Kanun'da daha sonra 1986 tarihli 3266 sayılı Kanun'la yapılan değişikliklerle Kurul Başbakanlığa bağlanmıştır.

Bu değişiklikle Kurul, kendisine verilen görevlerin yanında, TCK'nun 426, 427 ve 428. maddelerinde belirtilen suçlara ilişkin olarak yargı organlarına resmi bilirkişilik

yapmakla da görevlendirilmiş ve zararlı yayınların tespiti konusunda, re'sen inceleme yapabileceği gibi, resmi makamlar ile gayeleri içinde çocuk ve gençlerin korunmasına yer veren derneklerin, kadın ve basın dernek ve kuruluşlarının başvurularını da inceleyerek karara bağlama görevi tevdi edilmiştir.

Kanun'un 4. maddesine göre, Kurul'un sakıncalı gördüğü içeriğin yayınlanabilmesi veya gösterilebilmesi için herkesin kolayca görüp okuyabileceği şekil ve büyüklükte "küçüklere zararlıdır" ibaresinin ilgili içeriğin üzerine basılması zorunludur. Benzer şekilde, bu tür içerik ancak 18 yaşından büyüklere, içi görülmeyen zarf veya poşet içinde, üzerinde "küçüklere zararlıdır" etiketiyle satılabilir. Kanun, 5237 sayılı Kanun'un 226. maddesinde düzenlendiği gibi "fikri, içtimai ve bedii kıymeti haiz olan" eserleri kapsam dışı kabul etmiştir.

Kanun'a göre, Kurul; Başbakanlığın en az onbeş yıl kamu hizmeti yapmış kişiler arasından, Adalet Bakanlığı'nın hakim ve savcılar arasından, İçişleri Bakanlığının üst kademe yöneticileri arasından, Sağlık Bakanlığının tıp dalından, Kültür ve Turizm Bakanlığının güzel sanatlar dalında ün yapmış kişilerden, YÖK'nun sosyal bilimler dalında en az doktor unvanını almış üniversite öğretim elemanlarından, DİB'nin Din İşleri Yüksek Kurulu üyelerinden, Ankara, İstanbul ve İzmir Gazeteciler Cemiyetlerinden seçeceği birer üye ile MEB Talim ve Terbiye Kurulu üyelerinden seçilecek iki üye olmak üzere 10 üyeden oluşmaktadır.

Kanun'a göre Kurul Başkanı, bu üyeler arasından Başbakanlıkça seçilir. Üyelerin görev süresi 3 yıldır. Süresi dolanlar yeniden seçilebilirler. Kurul, üye sayısının salt çoğunluğu ile toplanır ve toplantıya katılanların salt çoğunluğu ile karar verir. Kurul tarafından gerekli görülen hallerde sürekli veya geçici olarak görev yapmak üzere özel ihtisas komisyonları kurulabilir. Kurul'un, bu komisyonlarda görev yapmasını uygun göreceği kamu personeli Başbakanlıkça görevlendirilir.

Kurul, gelişen ve çeşitlenen iletişim teknolojileri nedeniyle "muzır" yayınlardaki kontrolsüz artıştan ve İnternet teknolojisi karşısında, gençleri ve çocukları "muzır neşriyattan koruma" kabiliyetlerinin azaldığından; az sayıda personelle her yıl yüz

binlerce materyali inceleyerek, görevlerini yerine getirmeye çalıştıklarından şikayet etmektedir. Keza, Kurul'un bir yılda incelediği "muzır" içerikli CD sayısının 243 bini bulduğu belirtilmektedir. Örneğin, 2011 yılında yargı organlarından 43.650 adet compact disk, 20 adet hard disk, 499 adet videokaset incelenmek üzere gönderilmiştir (Milliyet, 08.04.2012). Bu tablo Kurul'un hem kapsamı, hem sayısı, hem kriterleri, hem de iş yüküyle ilgili daha fonksiyonel çalışması için yeni bir yapılanmaya ihtiyaç olduğunu ortaya koymaktadır.

3.3.2.7 Sinema Genel Müdürlüğü Değerlendirme ve Sınıflandırma Kurulu

Kültür ve Turizm Bakanlığı Sinema Genel Müdürlüğü bünyesinde sinema filmleri için Değerlendirme ve Sınıflandırma Kurulu ve Alt Kurulları bulunmaktadır. 2004 tarihli 5224 sayılı "Sinema Filmlerinin Değerlendirilmesi Ve Sınıflandırılması İle Desteklenmesi Hakkında Kanun"a göre oluşturulan Kurullar, 18.2.2005 tarihinde yayınlanan "Sinema Filmlerinin Değerlendirilmesi Ve Sınıflandırılmasına İlişkin Usul Ve Esaslar Hakkında Yönetmelik" çerçevesinde faaliyet göstermektedir.

İlgili mevzuat, ülke içinde üretilen veya ithal edilen her türlü sinema filminin, ticari dolaşıma ve gösterime sunulmadan önce kayıt ve tescile de esas olacak şekilde değerlendirilmesi ve sınıflandırılmasını düzenlemektedir. Buna göre, düzenleme, Bakanlık bünyesinde oluşturulan Kurullarca sinema filmlerinin gösterim ve iletim biçimlerini de dikkate almak suretiyle kamu düzeni, genel ahlak, küçüklerin ve gençlerin ruh ve beden sağlığının korunması, insan onuruna uygunluk ve Anayasa'da öngörülen diğer ilkeler doğrultusunda denetlenmesi, değerlendirilmesi ve sınıflandırılmasını ele almaktadır.

Yönetmeliğe göre, Kurullar, bu ilkeler doğrultusunda yaptıkları değerlendirmeye bağlı olarak; cinsellik, korku veya şiddet unsurlarının ağırlıklı olup olmadığı gibi hususları da dikkate alarak, genel izleyici kitlesi tarafından izlenebilirlik ve yaş bakımından sinema filmlerini sınıflandırır. Keza cinsellik, korku veya şiddet unsurlarının ağırlığını dikkate alarak bazı filmlerin aile eşliğinde izlenmesinin uygun olacağına karar verebilirler. Aynı şekilde, yaş bakımından sınıflandırılan sinema

filmlerinin, radyo-televizyon gibi araçlarla veya dijital iletim de dahil olmak üzere işaret, ses, ve/veya görüntü nakline yarayan araçlarla yayın ve/veya iletiminin günün hangi saatlerinde yapılamayacağı Kurullar tarafından karara bağlanır.

Yönetmeliğe göre, yapılan değerlendirme ve sınıflandırma sonucunda kullanılması zorunlu tutulabilecek işaret ve ibareler belirlenebilir. Buna göre, ticari dolaşıma veya gösterime uygun bulunan ancak içerikleri nedeniyle seyircinin bilgilendirilmesi veya izleyici kitlesi için yaş sınırı uygulanması gereken filmlerde içerik gösteren; “Genel İzleyici Kitlesi”, “7 yaş ve üzeri izleyici kitlesi içindir”, “7 yaş altı izleyici kitlesi aile eşliğinde izleyebilir”, “13 yaş ve üzeri izleyici kitlesi içindir”, “13 yaş altı izleyici kitlesi aile eşliğinde izleyebilir”, “15 yaş ve üzeri izleyici kitlesi içindir”, “15 yaş altı izleyici kitlesi aile eşliğinde izleyebilir”, “18 yaş ve üzeri izleyici kitlesi içindir”, “Şiddet ve korku unsurları içerir”, “Cinsellik Unsurları içerir”, “Olumsuz örnek oluşturabilecek davranışlar içerir” ibarelerinin yer aldığı işaretlerin kullanılmasına karar verilebilir. Ya da, ticari dolaşıma veya gösterime uygun bulunmayan filmlerde “Ticari dolaşıma veya gösterime sunulması uygun bulunmamıştır” uyarıcı ibare ve işaretinin bulunması istenebilir. Genel izleyici kitlesi tarafından izlenebilecek filmler için herhangi bir işaret ve ibare kullanılmaz, ayrıca, eğitim amaçlı olduğu belirlenen filmlerde yalnızca "eğitim amaçlıdır" ibaresi kullanılır.

5224 sayılı Kanun’a göre, Değerlendirme ve Sınıflandırma Kurulu, Bakanlık ile İçişleri ve MEB’ndan birer üye, ilgili alan meslek birliklerince önerilen uzman kişiler arasından Bakanlıkça seçilecek üç üye ile Bakanlık tarafından belirlenecek, alanında doktora derecesi bulunan bir sosyolog, bir psikolog ve bir çocuk gelişim uzmanı olmak üzere toplam dokuz üyeden oluşmaktadır. Kurul’a Bakanlık temsilcisi başkanlık eder, en az altı üyenin katılımıyla toplanır ve en az beş üyenin aynı yöndeki oyuyla karar alır. Değerlendirilmesi ve sınıflandırılması yapılan filmin yapımcısı istediği takdirde Kurul’a gözlemci olarak katılabilir.

Kanun, Kurul’a, ön değerlendirme ve sınıflandırma yapılması amacıyla alt kurullar oluşturma yetkisi vermiştir. Alt kurul, Bakanlık temsilcisi, meslek birliklerince önerilenler arasından Bakanlıkça seçilecek sektörden bir temsilci ile bir psikolog

olmak üzere üç kişiden oluşacaktır. Yönetmelik ise, Bakanlık temsilcisinin alt kurulun başkanı olmasını, Alt kurulun İstanbul'da ve üye tam sayısı ile toplanmasını, 2/3 çoğunlukla karar almasını ve Alt kurulların toplantılarına üyeler dışında kimsenin katılamamasını düzenlemiştir. Keza, Bakanlık, gerekli hallerde birden fazla alt kurul oluşturabileceği gibi, alt kurulların diğer illerde toplanmasına da karar verebilecektir.

Kanuna göre, yapılan ön değerlendirme ve sınıflandırma sonucunda, gerekli görülen hallerde veya filme ilişkin öngörülen kısıtlayıcı tedbire yapımcının muvafakat etmemesi halinde, Alt kurul, filmi bir kez daha değerlendirilmek ve karara bağlanmak üzere Değerlendirme ve Sınıflandırma Kurulu'na gönderir. Kanun ayrıca, Bakanlığa; insan onurunun, kamu düzeninin, genel ahlakın, çocukların ve gençlerin ruh sağlığının korunması amacıyla; şiddet, pornografi ve insan onuruyla bağdaşmayan görüntü ve etkiler içeren filmleri yeniden değerlendirilmek üzere Değerlendirme ve Sınıflandırma Kurulu'na sevk edebilme yetkisi de vermiştir.

Kanun'a göre, değerlendirme ve sınıflandırma sonucunda uygun bulunmayan filmler, ticari dolaşıma ve gösterime sunulamaz. Değerlendirme ve sınıflandırma sonrası uygun bulunan veya istenilen gerekli düzeltmeleri yapılan filmler kayıt ve tescil edilir ve bu filmleri içeren taşıyıcı materyaller bandrollenir. Keza, filmlerin, değerlendirme ve sınıflandırma sonucunu gösterir işaret veya ibareleri taşıması zorunlu tutulduğu takdirde, bu işaret veya ibarelerin her türlü tanıtım ve gösterim alanında ve taşıyıcı materyal üzerinde kullanılması zorunludur. İlgili Yönetmelik, uygun görülen ibare ve işaretlerin üzerinde taşınmamasına, bunlara göre satış, dağıtım ve gösterim yapılmamasına ilişkin denetim ve müeyyideler öngörmüştür.

Bahsi geçen değerlendirme ve sınıflandırma kurulları, İnternet içeriğinin ve her nevi yayın içeriğinin sınıflandırılması ve kategorize edilmesi konusunda birikimlerinden faydalanılabilecek bir uygulama olarak dikkate değerdir.

3.3.2.8 Radyo ve Televizyon Üst Kurulu

Dünya genelinde 1980 sonrası yaşanan süreçte, kamu yayıncılığının yerini özel radyo ve televizyon yayıncılığının almasıyla birlikte, düzenleyici kurullar ön plana çıkmaya

başlamış ve bu yönde yasal değişikliklere gidilmiştir. Biraz geçte olsa, Türkiye’de bu sürecin içerisinde yer alarak özel radyo ve televizyon yayınlarını düzenleyen Radyo ve Televizyonların Kuruluş ve Yayınları Hakkında Kanun’un 1994 yılında yürürlüğe girmesiyle, RTÜK kurulmuştur. Kanun’a göre RTÜK, radyo ve televizyon hizmetlerini düzenlemek ve denetlemekle görevli, Anayasa’nın 133. Maddesine göre üyeleri TBMM Genel Kurulu’nca seçilen, özerk ve tarafsız bir kamu tüzel kişiliğidir.

Söz konusu Kanun’un yasalaşma sürecinde, İnternet içeriğine müdahaleye imkan tanıyacağı iddiasıyla ciddi eleştirilere muhatap olduğuna; fakat, Kanunu’nun 1. maddesi gereği RTÜK’ün yetkisini radyo ve televizyon yayınlarının denetlenmesi ve düzenlenmesi ile sınırlı tuttuğuna, İnternetle sadece bu yolla yapılan radyo ve televizyon yayınları kapsamında ilgilendiğine daha önce değinmiştik.¹¹⁶

Bilahere 03.03.2011 tarihinde yayınlanan 6112 sayılı “Radyo Ve Televizyonların Kuruluş Ve Yayın Hizmetleri Hakkında Kanun”da yapılan bir düzenleme ile İnternet üzerinden yapılan radyo ve televizyon yayınlarına ilişkin müdahale de 5651 sayılı Yasa kapsamına alınarak sorumluluk BTK’na ve TİB’e havale edilmiştir.

6112 sayılı Kanun, yayın teknolojisindeki gelişmeler ve hızlı değişim, mevcut düzenlemelerin sayısal yayıncılığa uygun olmaması, sektörün ve toplumun beklentileri göz önünde bulundurularak, AB müktesebatına uyum çerçevesinde, AB Görsel-İşitsel Medya Hizmetleri Yönergesi hükümleri esas alınarak düzenlenmiştir.

Yayıncılık hizmetlerinin tüm dünyada olduğu gibi ülkemizde de “analog”dan hızla “sayısal(dijital)”e evrildiği görülmektedir. Bu süreçte, TV kanal sayısı ile izleme oranları artarken, sayısallaşma ile birlikte yayın kalitesi de artmakta; yüksek çözünürlüklü (HD) ve üç boyutlu yayın (3D) gibi yeni teknolojiler hızla pazardaki yerlerini almaktadır. Buna paralel olarak günümüz tüketicisinin İnternet, telefon ve televizyon gibi elektronik haberleşme hizmetlerine tek bir bağlantı üzerinden erişme isteği ile IPTV, Mobil TV ve Web TV gibi yayıncılıkta genişbant erişim teknolojileri kullanan uygulamalar da hızla yaygınlaşmaktadır (Paçacı vd., 2011: 10-11).

¹¹⁶ “Yasal Düzenlemeler” maddesine bkz.

Sayısal yayıncılığa uygun üretilmiş yeni TV cihazları ise karasal sayısal yayınları herhangi bir ara cihaza gerek duymadan doğrudan alabilmektedir. Bu nedenle, başta Avrupa olmak üzere gelişmiş pek çok ülkede sayısal yayınlara başlanmış ve hatta önemli kısmında analog TV yayınlarına son verilmiştir. Keza, ITU tarafından Ekim 2006'da gerçekleştirilen Bölgesel Radyo Konferansı'nda (RRC-06) imzalanan anlaşmaya göre, Türkiye'nin de içinde bulunduğu Avrupa bölgesinde en geç 2015 yılına kadar tamamen sayısal yayıncılığa geçilecektir (Paçacı vd., 2011: 16-17).

Nitekim, Türkiye bugün için 1,5 milyar TL'yi bulan büyüklüğü ile sayısal TV yayıncılığı için ciddi bir potansiyele sahiptir. Ülkemizde karasal, sayısal, uydu, kablo ve İnternet ortamından IPTV yayını yapacak kuruluşlara lisans ve yayın izni RTÜK tarafından verilmektedir. Buna göre günümüzde Türkiye'de uydu platformu (Digitürk, D-Smart), kablo platformu (Türksat-Teledünya) ve IP platformu (TTNET Tivibu) olmak üzere değişik platformlardan sayısal yayıncılık yapılmaktadır. Ayrıca çeşitli mobil TV uygulamaları da yayındadır (Paçacı vd., 2011: 32).

Dolayısıyla, tüm dünyada ve ülkemizde bilgi ve iletişim teknolojilerinin gelişmesi ile haberleşme ve yayıncılığın sayısal yayıncılığa yakınsaması süreci yaşanmaktadır. bu süreçte özellikle, mobil telefon ve İnternet hizmetleri için alternatif iletim ortamı tesisi ile genişbant uygulamalar ve diğer elektronik haberleşme hizmetlerinin sayısal yayıncılığa yakınsaması söz konusudur.

Sayısal yayıncılığın ülkemizde de giderek yaygınlaşması ve yakınsama teknolojilerinin kullanımı, bu alanla ilgili denetim ve düzenleme görevi yürüten iki kurum olan RTÜK ve BTK arasında bazı sorunların ortaya çıkması potansiyeli taşımaktadır. Elektronik Haberleşme Kanunu ile 6112 sayılı RTÜK Yasası beraber incelendiğinde, iki kurum arasında iç içe girmiş olan yetki ve görevler konusunda bugün için önemli bir sorun gözükmemektedir (Paçacı vd., 2011:49).

6112 sayılı Kanun'a göre, yayın hizmetlerinin iletimine ilişkin her iki Kurumu da ilgilendiren teknik ve idari konularda RTÜK ve BTK işbirliği yapacaktır. BTK, tarafından elektronik haberleşme hizmetlerini sunmak için yetkilendirilen

iřletmeciler, söz konusu hizmetlere ilişkin hususlarda BTK düzenlemelerine tabidirler. Fakat, yayın hizmetlerinin iletimi için faaliyette bulunmak isteyenler, 6112 sayılı Kanun’a göre RTÜK’ten gerekli yayın iletim yetkisini almak ve RTÜK düzenlemelerine uymak zorundadırlar (Paçacı vd., 2011: 34-49).

Diğer yandan, 6112 sayılı Yasa RTÜK’e sayısal yayını yürürlüğe koyabilmesi ve düzenlemeler yapabilmesi için gerekli yetki ve sorumluluğu vermiştir. Bu konuda Elektronik Haberleşme Yasası ile BTK’ya sadece milli frekans planı çerçevesinde RTÜK’e frekans tahsisi yapma görevi verilmiştir. RTÜK, tahsis edilen frekans bantlarında sayısal yayıncılık için frekans planlamalarını yapacak ve uygulayacaktır.

Buna karşılık, zaman içinde asıl sorunun içerik düzenlemesi konusunda yaşanacağı beklenebilir. Her ne kadar RTÜK, İnternet üzerinden yapılan yayınların denetimini 5651 sayılı Yasanın yetkisine ve dolayısıyla TİB’na bıraksa da, süreç içerisinde yayıncılığın büyük bir kısmının IP tabanlı hale gelmesiyle içerik denetimi konusunda bazı karışıklıkların, yetki ve görev alanı tartışmalarının yaşanacağı muhtemeldir. Bu nedenle, yayıncılık alanını düzenleme ve denetleme görevini birlikte yapan ve sayısal yayıncılığın ve yakınsama teknolojilerinin daha da yaygınlaşması nedeniyle görev alanları iyice birbirine girecek bu iki kurumun, tek bir çatı altında birleştirilerek, tek bir kurum ile yola devam edilmesi daha doğru olacaktır. Bu bütünleşme güçbirliğini tesis ederek yayıncılık alanının ihtiyaçlarına daha iyi cevap verebilecektir.

RTÜK’ün İnternet içerik düzenlemeyle ilgi diğer bir uygulaması ise, yayınların olumsuz etkileri konusunda çocukların ve gençlerin bilgilendirilmelerine yönelik olarak hayata geçirilen “koruyucu sembol sistemi”dir. 6112 sayılı Kanun, medya hizmet sağlayıcılarına, bu sistemi kullanarak, izleyicileri program hizmetlerinin içeriği hakkında sesli veya yazılı olarak bilgilendirme zorunluluğu getirmiştir.

Daha sonra 02.11.2011 tarihli “Yayın Hizmeti Usul Ve Esasları Hakkında Yönetmelik”le koruyucu sembol sistemine ilişkin usul ve esaslar Üst Kurulca belirlenmiştir. Buna göre, sembol sınıflandırmasının, yaş ve içerik gruplarını belirten sembollerin birlikte kullanılması suretiyle yapılacağı; bu çerçevede, bir programın

şiddet ve korku, cinsellik ve olumsuz örnek oluşturabilecek; ayrımcılık, alkol ve sigaranın aşırı kullanımı, madde kullanımı, yasa dışı davranışlar ile kaba ve küfürlü konuşmalar içermesi durumunda, o programın olası zararlı içerikte olabileceğine ilişkin “Şiddet/Korku”, “Cinsellik”, “Olumsuz Örnek Oluşturabilecek Davranışlar” sembollerinin kullanılacağı belirtilmiştir.

Keza, Yönetmeliğe göre, bir programın hangi yaş grubuna uygun olduğu ise; programdan etkilenme düzeyleri göz önüne alınarak oluşturulan “Genel İzleyici”, “7 Yaş”, “13 Yaş” ve “18 Yaş” sembolleriyle belirtilir. “13 Yaş” ve “18 Yaş” sembolleri programın yayını süresince ekranın bir köşesinde sabit ve sürekli olarak yayınlanacaktır. 7+ bir programın günün her saatinde yayınlanabileceği, 13+ bir programın 21.30’dan sonra yayınlanabileceği, 18+ bir programın 24:00-05:00 aralığı dışında yayınlanamayacağı anlamına gelmektedir.

Yönetmeliğe göre, bir programın hangi türde zararlı içerik taşıdığı ve hangi yaş grubuna uygun olduğu, medya hizmet sağlayıcıların görevlendirdiği ve sistem hakkında önceden eğitilmiş sertifika sahibi kodlayıcıların Üst Kurulun resmi İnternet sitesinde yer alan Örnek Kodlama Formunun elektronik ortamda doldurulması sonucunda verilen cevaplara göre sistem tarafından otomatik olarak saptanacaktır.

RTÜK’ün hazırladığı bu sistem, Avrupa ülkelerinde görsel-işitsel medya türlerinin değerlendirilmesinde kullanılan ve işlerliği sınanmış olan Hollanda’daki NICAM’ın geliştirdiği sınıflandırma sistemidir. Bu sistem yasaklayıcı ya da denetleyici değil; esas olarak yayıncı kuruluşların çocuklar ve gençleri televizyonun olası zararlı etkilerinden koruma sorumluluğuna işlerlik kazandıran bir öz-denetim mekanizmasıdır (Öktem, Ferhunde vd., 2006: 34).

Diğer yandan, RTÜK ile Kültür ve Turizm Bakanlığı televizyon programları için hazırlanan sembollerin sinema filmlerinde de kullanılması konusunda işbirliğine gitmiştir. Hazırlanan semboller, 2005 tarihli “Sinema Filmlerinin Değerlendirilmesi ve Sınıflandırılmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik” kapsamında Kültür ve Turizm Bakanlığı tarafından da kullanılmaktadır. Böylece, sinema ve

televizyonlarda kullanılan sembollerin aynı olması görsel-işitsel eserlerin sınıflandırılmasında bir bütünlük oluşturmuştur (Öktem, Ferhunde vd., 2006: 7).

Buraya kadar gözden geçirilen kurumlardan özellikle derecelendirme ve sınıflandırma benzeri işler yapan Çocuk ve Aile Profil Kriterleri Çalışma Kurulu, Küçükleri Muzır Neşriyattan Koruma Kurulu, Sinema Genel Müdürlüğü Değerlendirme ve Sınıflandırma Kurulu ile RTÜK'ün çalışmalarındaki ortak paydanın “yayın içeriklerini değerlendirme ve sınıflandırma” olduğu görülmektedir. Dolayısıyla, farklı yöntemler kullansalar ve konuya farklı açılardan yaklaşıyor olsalar da, çalışma alanları büyük ölçüde örtüşen dört farklı kamu kurumunun varlığı söz konusudur. Yayın içeriklerini değerlendirme ve sınıflandırma amacına yönelik olarak faaliyet gösteren bu kadar farklı kurum yerine; tüm bu kurumların mevcut görevlerini yerine getirdiği gibi, diğer bu konularla ilgili talep ve ihtiyaçlara cevap verecek şekilde her tür yayın içeriğini değerlendirip sınıflandırmasını yapacak ihtisaslaşmış bir “Sınıflandırma Kurumu”nun daha faydalı olacağı düşünülebilir.

Bu bağlamda, kamu görevlileri yanında tüm yayıncılık mecralarının meslek ve tüketici temsilcilerinin, STK'ların, konularında uzman kişilerin ve ilgili akademisyenlerin de yer alacağı söz konusu Kurul'un diğer basın yayın ürünleri yanında İnternet içeriğinin sınıflandırmasında ve katalog suçlarının değerlendirilmesinde yetkili bir kurum haline getirilmesi düşünülebilir.

3.3.2.9 Bilgi Toplumu Dairesi Başkanlığı

Türkiye’de “bilgi toplumu” çalışmaları çerçevesinde 2003 yılından bu yana e-Dönüşüm Türkiye Projesi’nin koordinasyonu Bilgi Toplumu Dairesi tarafından yapılmaktadır. Keza, bilgi toplumuna dönüşüm kapsamında; 2003-2004 Yılları Kısa Dönem Eylem Planı, 2005 Yılı Eylem Planı, 2006-2010 Yılları Bilgi Toplumu Stratejisi ve Eylem Planı hazırlanmış ve uygulanmıştır. Ayrıca, 2004 yılında Bilgi Toplumu Dönüşüm Politikası Belgesi yayınlanmıştır.

Bu belgelerin ve bundan sonra yapılacak plan ve strateji belgelerinin Türkiye’deki İnternet politikalarına yön veren ve verecek temel metinler olması nedeniyle dikkatle

ele alınması ve Bilgi Toplumu Dairesi Başkanlığı'nın bu çerçevede yapmış olduğu çalışmalar önem arz etmektedir. 08.06.2011 tarihinde yayınlanan 641 Karar sayılı "Kalkınma Bakanlığının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname" ile DPT'nin Kalkınma Bakanlığı olarak yeniden örgütlenmesi sonrası da ülkemizin bilgi toplumuna dönüşüm hedefi çerçevesindeki politika, hedef ve stratejilerin belirlenmesi görevi Bilgi Toplumu Dairesi tarafından üstlenilmiştir.

Fakat, 2006-2010 Yılları Bilgi Toplumu Stratejisi ve Eylem Planı'nın uygulama dönemi tamamlandıktan sonra bugüne kadar yeni bir strateji veya eylem planı hazırlanmamış olması büyük bir eksikliktir. Halihazırda Türkiye'nin 2013-2020 döneminde uygulanması öngörülen bilgi toplumu stratejisinin oluşturulma çalışmaları BTD tarafından yürütülmektedir (Bilgitoplumstratejisi, 2013). Türkiye'nin İnternet içerik düzenlemeleri için de temel referans metni olacak bu yeni strateji belgesinde konunun nasıl ele alınacağı ve nasıl bir yol haritası çıkarılacağı dikkatle takip edilmesi ve önemle üzerinde durulması gereken bir konudur.

3.3.2.10 Aile ve Toplum Hizmetleri Genel Müdürlüğü

İnternetle ilgili kurumlardan birisi de Aile ve Toplum Hizmetleri Genel Müdürlüğü (ATHGM)'dür. Sosyal problemlerin tespiti ve çözüm yollarının araştırılması ile ailenin korunması, güçlendirilmesi ve sosyal huzurunun arttırılmasına yönelik çeşitli çalışmalar yapmak amacıyla 1989 yılında Aile Araştırma Kurumu olarak faaliyete başlayan ATHGM, 13.11.2004 tarihli 5256 sayılı Teşkilat Kanunu ile Aile ve Sosyal Araştırmalar Genel Müdürlüğü (ASAGEM) olarak revize edilmiştir. ATHGM mevcut halini ise 08.06.2011 tarihli 633 Karar sayılı Kanun Hükmünde Kararname ile almıştır. Söz konusu düzenleme ile yeni kurulan Aile ve Sosyal Politikalar Bakanlığı'na bağlı bir ana hizmet birimi olarak yapılandırılmıştır.

Bu düzenleme ile ATHGM'ne, aile yapısının ve değerlerinin, aileyi oluşturan bireylerin korunması ve güçlendirilmesine ilişkin olarak; aile yapısını ve değerlerini, huzur ve mutluluğunu tehdit eden kötü alışkanlık ve bağımlılık, aile içi şiddet ve istismar, intihar ve benzeri sorunları ve bu sorunlara yol açan faktörleri tespit etmek,

nedenleri ve sonuçları bakımından incelemek, araştırmak, bunların önlenmesine ve sorunların çözümüne yönelik, aileyi destekleyici ve eğitici programlar hazırlamak ve uygulamak benzeri birçok görevler verilmiştir.

Bu çerçevede ATHGM, ASAGEM olduğu dönemden beri aile bireyleri için yaptığı çalışmalar arasına aileyi ve çocukları İnternet'in olası zararlarından korumayı da almıştır. Buna göre, Genel Müdürlük bir takım yayınlar, araştırmalar ve konferanslar yapmış, konu ile ilgili organizasyonlara iştirak etmiştir. Bu bağlamda, 20-22 Eylül 2006 tarihlerinde, INSAFE tarafından Selanik'te düzenlenen "İnternet'te Daha Güvenli Çocuklar İstiyoruz" konulu uluslararası konferansa katılım sağlamıştır (ATHGM, 2006). Keza, 20-21 Haziran 2007 tarihinde Lüksemburg'da düzenlenen Safer Internet Forum 2007 toplantısına iştirak etmiştir (ATHGM, 2007).

ATHGM bunun yanında, 2007 yılında "İnternet Kullanımı ve Aile Araştırması" yapmış ve 2008'de bunu kitap olarak yayınlamıştır. Bu araştırmada; aile bireylerinin İnternet'i kullanma alışkanlıkları, kullanım sıklıkları, kullandıkları yerler ve süreler, İnternet'in olumlu etkileri, özellikle çocuklar ve gençler üzerindeki olumsuz etkileri, İnternet'in güvenlik-etik boyutu irdelenmiş ve elde edilen bulgular ışığında sonuçlar değerlendirilerek yapılması gerekenler hakkında öneriler geliştirilmiştir (ATHGM, 2008). Yine, 2008'de "Dijital Oyunlar ve Çocuklar Üzerine Etkileri Raporu" yayınlanmıştır (ATHGM, 2008a). ATHGM'nin yakın gelecekte İnternetin çocuk ve aile üzerindeki etkileri ve ortaya çıkan sosyal problemler konusunda daha aktif bir politika izlemesi beklenmektedir.

İnternetle ilgili örgütsel yapıların ortaya konulduğu yukardaki bilgilerden, Türkiye'de genel olarak İnternetin düzenlenmesiyle ilgili doğrudan veya dolaylı sorumluluk ve görev üstlenen kamu kurumlarının dağınık ve çok parçalı bir yapıya sahip oldukları görülmektedir. Halbuki, Dünya'da bu konuyla ilgili gelişen yeni trend söz konusu kurumların birleşmesi ve bütünleşmesi yönündedir.

Öncelikle, ülkemizde ilgili mevzuata göre, İnternetin de içinde yer aldığı bilgi ve iletişim teknolojileri, elektronik haberleşme ve yayıncılık alanlarına ilişkin görev ve

sorumluluklar üç bakanlık arasında paylaştırılmıştır. UDH Bakanlığı bilgi ve iletişim teknolojileri ve elektronik haberleşme alanlarıyla ilgili sorumluluğu üstlenirken, yayıncılıkla ilgili olarak RTÜK’e yetki verilmiş ve bu kurumun hükümet ile olan ilişkilerini Başbakan veya görevlendireceği bir bakan aracılığıyla yürütmesi öngörülmüştür. Bilgi toplumuna ilişkin politika, hedef ve stratejileri hazırlamak, bu alanda kamu kurum ve kuruluşları, STK’ları ve özel sektör arasındaki koordinasyonu sağlamak ve uygulamayı etkin bir biçimde yönlendirmek gibi görevler ise, Kalkınma Bakanlığı bünyesindeki Bilgi Toplumu Dairesi Başkanlığına verilmiştir. Bunların dışında, Bilim Sanayi ve Teknoloji Bakanlığına verilmiş bir takım görevler yanında Aile ve Sosyal Politikalar Bakanlığı’na bağlı bir ana hizmet birimi olan ATHGM’nün de İnternetle ilgili sorumlulukları vardır.

Ülkemizdeki bu dağınık ve parçalı yapıya karşın dünyadaki uygulamalar yakınsama teknolojilerinin gelişmesi ve yaygınlaşmasından dolayı giderek bütünleşik hale gelmektedir. Bu kapsamda, öncelikle haberleşme ve yayıncılık ile bilgi ve iletişim teknolojilerini düzenleyen ve denetleyen bağımsız üst kurullar birleştirilirken, bu alanların tümünün aynı bakanlık bünyesinde toplanmasına ilişkin örnekler giderek artmaktadır. İngiltere’de Kültür, Medya ve Spor Bakanlığı, Almanya’da Ekonomi ve Teknoloji Bakanlığı, Avustralya’da Genişband, Haberleşme ve Dijital Ekonomi Bakanlığı, ABD’de Ticaret Bakanlığı bu örneklerden bazılarıdır.

Bu hizmetleri, kimi ülkelerin, hizmetlerin meydana getirdiği kültürel değerleri dikkate alarak İngiltere’de olduğu gibi “kültür” başlığını da dahil ederek, Almanya gibi kimi ülkelerin ise, hizmetlerin oluşturduğu ekonomik yararı dikkate alarak “ekonomi” ve “teknoloji” başlığını da içerecek şekilde düzenlediği görülmektedir (TBMM, 2012: 281-290).

Diğer yandan, ülkelerin giderek bilişim ve bilgi teknolojileriyle ilgili alanlara daha fazla önem vermekte olduğu ve bunun bir göstergesi olarak bu alanlarla ilgili müstakil bakanlıklar teşekkül ettirmekte oldukları görülmektedir. Nitekim, aralarında Çin, Hindistan, Bangladeş, İsveç, İsviçre, Pakistan, İran gibi ülkelerinde bulunduğu

43 ülke bilgi teknolojileri alanında bakanlık düzeyinde örgütlenmiştir. Yani, her dört ülkeden birisi bu yolu tercih etmiştir (CIA, 2012).

Sonuç olarak, Dünya'daki genel yaklaşımın, yakınsama teknolojilerinin gelişmesiyle uyumlu olarak, ülkelerin elektronik haberleşme, yayıncılık ve bilgi teknolojileri hizmetlerini aynı çatı altında toplayarak bu hizmetler için izlenecek politikaları, başta tüketicinin korunması ve rekabete dayalı dijital ekonominin güçlendirilmesi açısından ortak unsurlar üzerine bina ettiği görülmektedir. Bu yaklaşım aynı zamanda bütüncül bir bilgi toplumu ve İnternet politikası oluşturmaya imkan sağlamakta, söz konusu alanlara ilişkin hizmetlerde izlenecek politikaları tek bir elden düzenleme ve yönetmeyi mümkün kılmaktadır (TBMM, 2012: 290-291). Bu nedenlerle, ülkemizde de benzer bir yaklaşımla bu alanlara ait hizmetlerin tek bir bakanlık çatısı altında toplanmasının daha faydalı olacağı değerlendirilmektedir.

3.3.3 5651 Sayılı Kanun'un ve TİB'in Uygulamaları

5651 sayılı Kanun yürürlüğe girmesi ve TİB tarafından uygulanmaya başlamasıyla İnternet içerik düzenlemesine ilişkin Türkiye'de yeni bir dönem başlamıştır. Böylece, Türkiye'de İnternet içeriğinde yer alan tehlike ve risklere karşı içeriğin izlenmesi ve engellenmesini de kapsayan bir takım önlemlerin geliştirildiği ve mücadelede aktif rol alındığı yeni bir sürece girilmiştir.

Bu yeni dönem, 5651 sayılı Kanun'da İnternet içerik düzenlemesine yönelik olarak TİB'na tevdi edilen temel görevler ve bu görevlere ilişkin olarak TİB'nın süreç içerisinde yapmış olduğu uygulamalar bakımından İnternet Bilgi İhbar Merkezi, erişim engellemesi, içeriğin yayından çıkarılması, Güvenli İnternet Hizmeti, içerik filtreleme, yetkilendirme, İnternetin güvenli kullanımı ve koordinasyon çalışmaları başlıkları altında ele alınabilir.

3.3.3.1 İnternet Bilgi İhbar Merkezi

TİB Bilgi İhbar Merkezi, 5651 sayılı Yasa gereği kurulmuş ve 23.11.2007 tarihinden bu yana katalog suçlarıyla ilgili ihbar almaktadır. Merkez, "www.ihbarweb.org.tr"

web ve “ihbar@ihbarweb.org.tr” e-posta adresi yanında “166” telefon hattı ile “1199” kısa mesaj servislerinden kullanıcılarına ücretsiz olarak ihbarda bulunma imkanı sunmaktadır (İhbarweb, 2013). Ayrıca, “www.bim.org.tr” adresinden de kurumlardan gelen ihbarları kabul etmektedir. Bilgi İhbar Merkezi’nin web sitesi Türkçe ve İngilizce dillerinde yayın yapmaktadır (Şen, 2008: 26).

Merkez, 18.05.2011 tarihinde 40. üye olarak INHOPE’a kabul edilmiştir. Üyelik ile uluslararası işbirliği ve bu yapı üzerinden çabuk ve etkili bilgi paylaşımı sağlanması, Yasa’da belirtilen suçlarla mücadelede alınacak tedbirlerin daha hızlı ve etkin hale gelmesi beklenmektedir (BTK, 2013: 90). Nitekim Merkez, 2011 yılı Temmuz ayından bu yana INHOPE üyesi ihbar merkezlerine çocukların cinsel istismarı içerikleri ile ilgili 500’ü aşkın ihbar iletmiştir. Bunların 254’ü ABD’ye, 176’sı Hollanda’ya gönderilmiştir. Yine, INHOPE üyesi ihbar merkezlerinden çocukların cinsel istismarı içerikleri ile ilgili 20 ihbar alınmış ve 18’inde belirtilen içerikler çıkarılmıştır. Bir tanesinin ise savcılık soruşturması devam etmektedir (TİB, 2012).

Merkez vasıtasıyla TİB’na intikal eden ihbarlar, 5651 sayılı Kanun’un uygulama usul ve esaslarını belirleyen düzenlemeler çerçevesinde ön inceleme, teknik inceleme ve hukuki değerlendirme işlemleri ile Türkiye’den ulaşım yoğunluğu ve özellikle çocukların doğrudan ulaşabilmesi gibi kriterlerde dikkate alınarak değerlendirilmekte ve sonuçlandırılmaktadır (İhbarweb, 2013a; Bozkurt, 2012:124-129).

Merkez, şeffaflık adına yapmış olduğu iş ve işlemlere, bağlı bulunduğu mevzuata ve uygulamalarına ilişkin bilgileri kısa ve öz bir şekilde web sitesinde yayınlamaktadır (İhbarweb, 2013a). Bu kapsamda, 5651 sayılı Yasa ve yönetmelikler, Yasa’nın çıkış amacı, hangi tür yayınların engelleneceği, bu kararları kimlerin verebileceği, engelli sitelerin ne yapabileceği, engelleme yöntemleri, ihbarların nasıl yapılabileceği ve nasıl değerlendirildiği gibi konularda bilgi verilmektedir. Ayrıca, kişisel hakları ihlal edilen veya dolandırılan kişiler için kısa yönlendirmeler de bulunmaktadır.

Merkez, geri dönüş isteniyor ise ihbarı yapandan e-mail adresi istemekte ve ilgiliye bilgi vermektedir. Bunun dışında kişisel bilgi talep edilmemektedir. Merkez’in web

sitesinde “Gizlilik Bildirimi” yayınlanmakta; ziyaretçilerin ve ihbar yapanların her türlü bilgilerinin kurumsal koruma altında bulunduğu ve başkalarıyla paylaşılmaksızın saklanacağı belirtilmektedir (İhbarweb, 2013b).

İhbar Merkezi faaliyete başladıktan sonra bilinirliği giderek artmış ve bunun sonucu olarak aldığı ihbar sayısında düzenli artış olmuştur. Keza, dünyadaki diğer ihbar merkezleri arasında en fazla ihbar alan birkaç merkezden birisi durumuna gelmiştir (Bozkurt, 2012:131). Nitekim, Merkezin faaliyete başladığı günden 31.12.2012 tarihine kadar yapılan ihbarların toplam sayısı 558.099’a ulaşmıştır. Merkez, 2008 yılında 2.864 ihbar alırken bu rakam 2009’da 112.253’e, 2011’de 177.387’ye çıkmıştır. 2012 yılında ise 156.399 ihbar alınmıştır (BTK, 2013: 110). Almanya’da FSM İhbar Merkezi’nin 2000-2009 yılları arasında 10.000 civarında ihbar aldığı (FSM, 2010), Fransa’da Point de Contact İhbar Merkezi’nin 2010 yılında 8.196 ihbar aldığı (AFA, 2011), Kanada’da Cybertip İhbar Merkezi’nin, 2002-2012 yılları arasında toplamda 50 bin civarında ihbar almış bulunduğu (CYBERTIP, 2013) ve Avustralya’da ACMA İhbar Merkezi’nin, 2011 yılındaki ihbar sayısının 6.043 olduğu (ACMA, 2012g) hatırlanırsa, TİB Bilgi ve İhbar Merkezi’nin kısa zamanda ulaştığı bu nokta daha iyi anlaşılacaktır.

Merkeze yapılan ihbarlardan katalog dışı içeriklere ait olanların fazlalığı dikkat çekicidir. Nitekim, Merkez’e 2012 Haziran ayına kadar gelen ihbarların %25’i katalog dışıdır (TİB, 2012). Katalog dışı olarak alınan şikayetlerin ayrıca analiz edilip değerlendirilmesinde ve faydalanılacak bir hale getirilmesinde yarar vardır.

TİB Bilgi İhbar Merkezi Türkiye’de birçok kamu ve STK’u ile işbirliği içinde çalışmaktadır. Çocukların korunması ve güvenli İnternet bilincinin artırılması konusunda MEB, İnternet Geliştirme Kurulu ve Aile ve Sosyal Politikalar Bakanlığı, Mutlu Çocuklar Derneği ve Yeşilay ile, sağlığa zararlı maddelerin temini konusunda Sağlık Bakanlığı ve Tarım ve Gıda Bakanlığı ile, bahis ve şans oyunları konularında Milli Piyango İdaresi ile işbirliği yapmaktadır. Soruşturma gereken durumlarda kolluk ve adli birimlerle sıkı bir işbirliği yürütülmektedir. Özellikle Türkiye’de

barındırılan çocuk pornografisi içerikleri ile ilgili olarak EGM ile yakın bir çalışma ve işbirliği sürdürülmektedir (Bozkurt, 2012:123).

Ayrıca, 2011 yılı içinde bir STK, TİB İnternet Daire Başkanlığı'nın önderliği, tavsiyeleri ve tecrübe paylaşımı desteği ile Türkiye'de ilk kez bir İnternet yardım hattı kurulmasına teşebbüs etmiştir. Bu yardım hattı merkezinde İnternette olumsuz etkilenen bireylerin, özellikle de çocukların ve gençlerin, konusunda uzman personelden eğitim ve psikolojik destek almaları hedeflenmiştir. Yaklaşık 6 ay süren bu girişim finansal sıkıntılar yüzünden devam edememiştir (Bozkurt, 2012: 131).

Merkezin daha fonksiyoner olabilmesi için bir takım öneriler dile getirilmektedir. Bunların ilki, Merkez'in tanınırlığının artırılması için logosu ve web bağlantısının İnternet ortamındaki diğer web sitelerinde yaygın bir şekilde paylaşılmasını sağlamakla ilgilidir. Bu kapsamda, Türkiye'deki en çok ziyaret edilen 1000 sitenin ana sayfasına mümkün olduğunca logo ve web bağlantısı eklenmeye çalışılması önerilmektedir. Benzer şekilde, logo ve web bağlantısının e-devlet kapısına ve kamu kurumlarının web sitelerinin ana sayfalarına konulabileceği, MEB'nin ücretsiz olarak dağıttığı kitapların arka kapak sayfalarına İhbarweb, Güvenliweb, Güvenliçocuk ve Güvenli İnternet Hizmeti ile ilgili tanıtıcı ve kısa bilgilendirici bölümlerin konulabileceği hatırlatılmaktadır (Bozkurt, 2012:133).

İkincisi ise, ihbarların artırılmasına yöneliktir. Buna göre, web sayfasındaki ihbar formunun mobil cihazların küçük ekranlarına sığacak şekilde sade ve kısa mobil sürümü bulunmalıdır. Ayrıca Android, Blackberry, Windows Phone gibi platformlar için ihbar uygulamaları tasarlanarak hizmete sunulmalıdır (Bozkurt, 2012:132).

Son öneri ise, ihbarların etkinliğini artırmayı esas almaktadır. Buna göre, ihbar formunun en başında içeriğin barındırıldığı ülkenin bilinip bilinmediğinin sorulması; eğer içeriğin nerede barındırıldığı biliniyor ve ilgili ülkede INHOPE üyesi ihbar merkezi bulunuyor ise ihbarı yapan kişiden o ülkedeki ihbar merkezine de ihbarda bulunmasının istenilmesi ve ilgili bağlantıların sunulması önerilmektedir. Keza, İhbarweb'de ihbar merkezinin işleyişi ile ilgili şikayetlerin alındığı bir

mekanizmanın bulunması ve bunun ilan edilmesi teklif edilmektedir (Bozkurt, 2012:135-136).

3.3.3.2 Erişim Engelleme Uygulamaları

Daha önce de belirtildiği gibi, 5651 sayılı Kanun'a göre Cumhuriyet savcılıkları, ceza mahkemeleri ve TİB belirtilen katalog suçlar kapsamında erişimin engellenmesi kararı verebilmektedir. Fakat, TİB'nin bu kararı verilebilmesi için İnternet sitesinin içerik veya yer sağlayıcısının yurt dışında bulunması gerekmektedir. TİB, Yurt içi yayınlarda sadece çocukların cinsel istismarı ve müstehcenlik suçunda hakim onayına sunmak şartıyla erişimin engellenmesi kararı alabilmektedir. Ama, her halukarda erişim engellemesinin uygulaması TİB üzerinden gerçekleştirilmektedir. Adli makamlarca verilen erişim engelleme kararları da gereği yapılmak üzere TİB'na gönderilmekte ve kararlar TİB tarafından yerine getirilmektedir.

İnternet ortamındaki yasadışı ve zararlı içerikle mücadelenin bir parçası olarak 5651 sayılı Yasa uyarınca uygulanan erişim engellemeleri, sansüre dönüştüğü/dönüşeceği noktasında yoğun eleştiri ve tartışmalara neden olmaktadır. Bu kapsamda, müstehcenlik kavramının belirsiz olmasından, sakıncalı içerik yanında sitenin tamamına erişimin engellenmesi nedeniyle suç ve cezada orantısızlık bulunduğu, TİB'nca re'sen engellenen sitelerle ilgili yetki tartışmalarına, yasaklar konusunda ihtisas mahkemelerinin bulunmamasından, kapatılan sitelere ilişkin bilgi verilmemesi ve savunma hakkı tanınmamasına kadar birçok eleştiri dile getirilmektedir (Bulut, 2009: 163-185; Akdeniz ve Altıparmak, 2008: 50-75; Köse ve Özen, 2010: 121-122).

Bu eleştirilere karşılık TİB, yaptığı uygulamalara ilişkin bilgileri değişik mecralarda kamuoyu ile paylaşmaktadır. Buna göre sürecin başlangıcında adli mercilerden gelen talepler ile İhbar Merkezine ulaşan ihbarlar veya TİB'in idari tedbir gereği re'sen şüpheli gördüğü içerikler, 5651 sayılı Yasa'da yer alan usul ve esaslara göre ön inceleme, teknik inceleme ve hukuki değerlendirme işlemlerinden geçirilmektedir. Bu süreçte, Türkiye'den erişim yoğunluğu ve özellikle çocukların doğrudan ulaşabilmesi gibi kriterler de dikkate alınmaktadır. Tüm bu değerlendirmeler

sonucunda içerikle ilgili katalog suçlarının kapsamı içinde olduğuna dair yeterli şüphe oluşursa erişim engellemesi kararı uygulanmaktadır (TİB, 2013a).

TİB, bu süreçte verilen kararlarda Anayasa’da geçen, temel hak ve özgürlüklerin kısıtlanmasının sınırı olarak ortaya konulan “ölçülülük ilkesi”ne uygunluğun gözetildiğini ve bu bağlamda, öncelikle erişimin engellenmesi tedbirlerinin uygulanması öncesi ve sonrasındaki süreçlerde “uyar-kaldır” mekanizmasını işletmeye çalışıldığını belirtmektedir. Keza Başkanlık, resen erişimin engellenmesi kararlarının, tamamıyla yasal olmayan içerik barındıran sitelere (örneğin, çocuk pornografisi içerikleri) ya da suç unsuru içerikleri çıkarmamakta direnen İnternet sitelerine yönelik olarak uygulandığını ifade etmektedir (Güvenliweb, 2013).

Sonraki süreçte, engelleme tedbirlerinin etkinliğinin gözetildiği ve bu kapsamda etkinlik analizinin yapılarak tedbirlerin tedricen uygulandığı belirtilmektedir. Buna göre, İnternette halihazırda her an ulaşılabilir aktif milyonlarca suç içeriğinin var olduğu ve bunların uluslararası hukuk düzenlemeleri yönüyle farklılık arz ettiği gerçeği çerçevesinde, engelleme önceliği olarak Türkiye’den ulaşım yoğunluğu önemli bir kriter olarak dikkate alınmaktadır (Bozkurt, 2012:105).

TİB, engellenme tedbirinin uygulanabilmesi için gerekli olan yeterli şüphenin tespitinde yargı içtihatlarını esas aldığını, bu çerçevede; müstehcenlik ve çocukların cinsel istismarı suçlarında kazara, tesadüfen rastgelinen ve özellikle çocuklar için ciddi riskler bulunan içeriklerle mücadelenin öncelenmekte ve önemsenmekte olduğunu, çocuklar için sakıncalı olabilecek içeriğe doğrudan ulaşmalarının engellenmesine yönelik tedbirler alındığını belirtmektedir (Bozkurt, 2012:105).

TİB, erişim engelleme yöntemi olarak alan adı veya IP adresinden engelleme yöntemlerini kullanmaktadır. TİB, IP’den engelleme yapıldığında, o IP adresinde yer sağılanan bütün alan adlarına birden engelleme yapıldığının farkında olarak, çocukların cinsel istismarı içerikleriyle ilgili hususlar dışında IP’den engelleme yöntemini çok sıkı şartlar altında, sınırlı olarak tercih edildiğini belirtmektedir (TİB, 2013a; Bozkurt, 2012:119).

Fakat, TİB'nin daha çok tercih ettiğini duyurduğu alan adından erişim engelleme yönteminde de, IP engellemeye göre daha sınırlı olsa da, benzer bir sakınca vardır. Zira, bazen engellenen alan adı içerisinde tek bir sayfada bulunan yasadışı içerik nedeniyle alan adındaki tüm içerik engellemeye uğrayabilmektedir. Nitekim, Türkiye'nin erişim engellenme uygulamalarında en çok eleştirilen konulardan birisi de, sitedeki sakıncalı bulunan sayfaları engellemek yerine bütün bir web sitesi için erişim yasağı getirilmesidir. Mahkemeler ve TİB'in, ilgili sayfayı URL'si üzerinden engellemek yerine sunucu IP'sinden veya alan adından engellemesinin, büyük bir kütüphanede bulunan binlerce kitaptan bir tanesinde sakıncalı bir içerik var diye tüm kütüphanenin kapatılmasından farklı bir şey olmadığı; dolayısıyla bunun hukuki açıdan orantısız bir tedbir olduğu dile getirilmektedir (Akgül, 2010: 285-300).¹¹⁷

Nitekim, Boz'da tamamında yasadışı içerik bulunan sitelerin engellenmesinde sıkıntı yaşanmadığını; ama, örneğin bir blog sitesinin bir kısmında yasadışı içerik bulunması ve ilgili içerik sağlayıcının uyarılmasına rağmen bunu yayından çıkarmaması durumunda sorunla karşılaşıldığını dile getirmektedir. Bu durumda blogun tümüne erişim engellemek zorunda kalınmaktadır (Ömer Boz ile kişisel iletişim, 30.07.2013).

Ancak, URL tabanlı filtreleme yapacak sistem için ilave yatırım gerektiği ve bunun ekonomik maliyetinin yüksek olması yanında, İnternette bir takım teknik sorunlara sebep olduğu ve yavaşlattığı gibi nedenlerle İSS'ların direnciyle karşılaştığı; oysa web sitelerinin tamamen kapatılmasının çok daha kolay ve masrafsız olduğu vurgulanmaktadır. Bu yüzden, ülkemizde erişimi engelleme konusunda zor, masraflı ancak yararlı olan yöntemi kullanmak yerine kolay, ucuz, ancak bilgiye erişimi engelleme potansiyeli bulunan yöntemin tercih edildiği savunulmaktadır. Bu çerçevede, TİB'nca 2008 yılı Haziran'ında URL tabanlı erişim engelleme konusunda İSS'lar ile çalışmalara devam edildiği yönünde bir açıklama yapıldığı, fakat sonrasında herhangi bir somut gelişme olmadığı hatırlatılmaktadır (TİB, 2008a).

¹¹⁷ Keza, bu uygulamanın Youtube örneğinde olduğu gibi, böylesine zengin bir bilgi kaynağından ülkemizin yararlanmasını istemeyen bir güç tarafından rahatlıkla sistemi sabote ederek bilgi kaynaklarının dünyada sadece Türkler'e kapalı olmasını sağlayabileceği; yani sistemin işleyişinin bu haliyle provokasyon ve sabotajlara açık olduğu ifade edilmektedir (Bulut, 2009: 163-185)

Konu hakkında Boz, URL tabanlı engellenmenin zor, zahmetli, maliyeti yüksek fakat bütün bunlara rağmen çok kolay aşılabilen etkisiz bir yöntem olduğunu; 2008 de konuyla ilgili TİB’nda bir çalışma yapılarak rapor hazırlandığını fakat içaçıcı bir sonuca ulaşamadığını belirtmektedir (Ömer Boz ile kişisel iletişim, 30.07.2013).

TİB, resmi web sitesinde şeffaflık adına erişim engellemelerle ilgili mevzuat, yapılan işlemler, kararı kimlerin vereceği, engellenen sitenin yeniden açılmasının nasıl mümkün olacağı, erişim engelleme yöntemleri gibi konularda kullanıcılara ve ilgililere kısa bilgiler sunmaktadır (TİB, 2013a). Bunun yanında, yine web sitesinde idari tedbir olarak uygulamakta olduğu engelleme kararlarına karşı itirazda bulunulabileceğini hatırlatarak, bunun için önce “eekg.tib.gov.tr” adresinden ilgili siteye erişimin olup olmadığının sorgulanmasını talep etmektedir. Sitede ayrıca, web siteleriyle ilgili bilgilerin sorgulandığı, özet ve hızlı bilgi elde edilebilmesini sağlayan ayrı bir “Site Bilgileri Sorgu Sayfası” oluşturulmuştur (TİB, 2013b).

TİB, Hukuk mahkemelerince erişimi engellenmiş İnternet site yetkililerinin, engelleme nedenini ve ne yapmaları gerektiğini nasıl öğrenebilecekleri konusunda yönlendirici bilgi de vermektedir. Nitekim, bu tür erişimi engelleme işlemlerinin başta Türk Telekom A.Ş. olmak üzere “http://www.tib.gov.tr” adresinde yer alan erişim sağlayıcılar vasıtasıyla yerine getirilmekte olduğunu hatırlatarak, söz konusu erişim sağlayıcılardan bilgi alınabileceğini belirtmektedir (TİB, 2013a).

Diğer yandan TİB’nın açıkça, erişim engellemesi uygulanan sitelere buna rağmen erişimin mümkün olabileceğini belirtmesi dikkat çekicidir. TİB, İnternetin dağıtık ve düzenlenemeyen yapısı nedeniyle kesin bir engellenmenin söz konusu olamayacağı, bunun ancak içeriğin yayından çıkarılmasıyla mümkün hale gelebileceği; bunun dışında yapılan her türlü işlemin, erişimi zorlaştıracı tedbirlerden ibaret kalacağını dile getirmektedir. Asıl olanın eğitim, bilgilendirme ve bilinçlendirme olduğu; maksada bu şekilde daha rahat ulaşılabilceği vurgulanmaktadır (TİB, 2013a).

Nitekim, her ne kadar 5651 Sayılı Yasa katalog suçlar kapsamındaki içerikleri engellemeyi amaçlasa da bu pratikte çoğu zaman mümkün olmamaktadır. Erişim

engellemeleri, ülkemizde en büyük erişim sağlayıcı olarak Türk Telekom ve diğer firmalar üzerinden, alan adı ve IP adreslerinin bloke edilmesiyle yapılmaktadır. Fakat, engellemeyi aşma yöntemlerinde görüldüğü gibi, engellenen sitelere kullanıcılar, vekil sunucular, tünel siteler veya yurt dışından VPN (Sanal özel ağ) bağlantısı sağlanması gibi farklı yöntemler kullanarak rahatlıkla ulaşabilmektedir. Bu açıdan İnternet sitelerine erişimin engellenmesinin teknik olarak çok mümkün olmadığı ve erişim engelinin kaldırılması için teknik olarak çok bilgili olunması gerekmediği açıktır. Nitekim, Türkiye’de yasaklı olmalarına rağmen bir çok sitesinin ciddi görüntülenme rakamlarına ulaştıklarına tanık olunduğu gibi, ktunnel.com, vtunnel.com ve tunnel.com gibi engellemeyi aşmaya yönelik yöntemler sunan tünel web sitelerinin ülkemizde oldukça rağbet gördükleri de bilinmektedir.¹¹⁸

Diğer yandan, Türkiye’de yargı kararı veya idari tedbir olarak erişimi engellenen site sayısı hakkında güncel resmi istatistiki veri yoktur. TİB, re’sen erişimi engellenen veya adli mercilerce engelleme kararı alınan sitelerin sayısı hakkında bilgi vermemekte, bunun yerine katalog suç türlerini esas alan oransal istatistikler yayınlamaktadır. Buna mukabil, bazı İnternet siteleri gayri resmi bir takım istatistikler yayınlamaktadır. Bunlardan birisi olan “Engelliweb.com”, tespit ettiği kadarıyla engellenmiş siteleri listelemekte ve istatistiklerini yayınlamaktadır. Buna göre, Türkiye’de 12.05.2013 tarihine kadar toplam 30.240 site engellenmiştir. Bunun içinde, TİB’nca re’sen engellenen site sayısının 26.207 olduğu iddia edilmektedir (Engelliweb, 2013, 2013a).

TİB, 2009 yılı Mayıs ayından bu yana erişim engelleme sayılarını açıklamamaktadır. Son açıkladığı verilere göre, 11.05.2009 tarihine kadar 5651 Sayılı Yasaya göre erişimi engellenen site sayısı 2.601’dir. Bu web sitelerinden 475’i (%18) mahkeme

¹¹⁸ Nitekim, yasaklama kararı yürürlükte iken 2008 yılı Haziran ayında YouTube Türkiye’den en çok girilen 5. web sitesi olmuştur. Bir başka kaynağa göre, erişim yasağına rağmen YouTube Türkiye’den hergün 1,5 milyon ziyaretçi almıştır. Keza, Alexa.com’un “en çok ziyaret edilen 50 web sitesi” listesi içinde Türkiye’den düzenli olarak erişilen engelli siteler de vardı. Örneğin, 18.8.2008 tarihinde engelli olan “youporn.com”a erişim 48., “dailymotion.com”a erişim 55. sırada yer almıştır. Keza, “Ktunnel.com” ve “Vtunnel.com” gibi kimlik gizleyen sunucuların İnternet siteleri de “ilk 50” arasına yerleşirken, DNS temelli engellemelerde kullanılan “OpenDNS” 54. sıraya yükselmiştir (Zaman, 2008; CNNTURK, 2008)

kararıyla, 2.126'sı (%82) TİB tarafından re'sen erişme kapatılmıştır (TİB, 2009a). Başkanlık, engelleme sayılarına ait bilgileri kamuoyu tarafından "negatif veya yanlış yorumlanacak" düşüncesiyle açıklamamaktadır (TİB, 2013a). Bu uygulama açıklık ve şeffaflık ilkesine aykırı hareket edildiği gerekçesiyle eleştirilere neden olmaktadır. Hatta, Başkanlığa karşı 4982 Sayılı Bilgi Edinme Hakkı Kanunu kapsamında idari dava açılmıştır (Akdeniz, 2010). Fakat, bu davadan uygulama aleyhine bir sonuç çıkmamıştır (Ömer Boz ile kişisel iletişim, 30.07.2013).¹¹⁹

Benzer eleştiriler TİB'nin engellediği sitelerin listesini yayınlamadığı konusunda ve erişim engelleme sayfasında çıkan uyarı yazısında kapatılan sitenin isminin yer almamasıyla ilgili olarak da yapılmaktadır. TİB, bu verileri yayınlamama nedeni olarak; Boz'un da belirttiği gibi, yasadışı içerikle mücadeleye ilişkin yöntemin ve bu sitelerin isimlerinin deşifresine yol açabilme ihtimalini ve İnternetin doğası gereği söz konusu sitelerin erişim engellemesinin tamamen sağlanamayacağı için adlarının yayınlanmasının adeta suç işlenmesini teşvik etmek anlamına geleceği gerekçelerini dile getirmektedir (Ömer Boz ile kişisel iletişim, 30.07.2013; TİB, 2013a).

Dünyadaki uygulamalar incelendiğinde, hem engelli sitelerin sayısal verilerinin yayınlanmasında, hem de isim listelerinin açıklanmasında ilgili kurumların ve devletlerin genellikle ketum davrandıkları, bu tür bilgileri kamuoyu ile paylaşmadıkları görülmektedir. Engelli sitelerin sayılarının yayınlanması konusunda az da olsa bazı ülkelerin şeffaf davrandığına rastgelinse de, istisna birkaç uygulama dışında, özellikle yasaklı siteler ve filtrelemeye konu kara listeler tüm dünyada genel bir politika olarak gizli tutulmaktadır. Erişim engelini aşmanın birçok yolunun bulunması, yasadışı olanın yaygınlaşmaması, suç işlemeye imkan ve teşvik oluşturulmaması yanında, ulusal ve uluslararası kamuoyundan gelen sansür karşıtı eleştirilere daha fazla malzeme vermemek gibi sebepler tüm ülkeleri bu noktada ortak bir anlayış ve uygulama birliğine yönlendirmiş gözükmektedir.

¹¹⁹ Boz, söz konusu davada, davacı tarafın erişim engellemelerine ilişkin sayısal istatistik yayınlayan örnek bir ülke uygulaması gösteremediğini, delil olarak sunulan rakamların ise ihbar sayılarını gösterdiğini ifade etmektedir (Ömer Boz ile kişisel iletişim, 30.07.2013)

Nitekim, Boz, engellenen site isimlerinin ve sayılarının suça teşvik olmaması ve aleyhte kullanılmaması için hiçbir ülkede yayınlanmadığını, engelli sayfalarla ilgili olarak bile genellikle herhangi bir ikaz veya bilgilendirme ibaresinin yer almadığını, bir çoğunda İngiltere’de olduğu gibi, hata sayfasıyla karşılaşıldığını belirtmektedir. Hatta, bu konuda TİB kadar açık ve şeffaf davranan; engellemeyi yapan kurumu, kararı veren mahkemeyi, kararın tarih ve sayısını engelleme sayfasında yayınlayan başka bir ülke bulunmamaktadır (Ömer Boz ile kişisel iletişim, 30.07.2013).

Keza, Berber ve Kaya, şeffaflığa aykırı olarak, AB devletlerinin ağ hatası tekniğini sıklıkla uyguladığını ve kullanıcıların, teknik bir sorundan dolayı siteye erişimin sağlanamadığı yanılgısına düşürüldüğüne dikkat çekmekte ve söz konusu bilgilerin engelleme mesajında yer almasının işletilmesi gereken itiraz mekanizmalarını belirlemeye yardımcı olduğu için yerinde bir uygulama olduğuna ve hak arama hürriyetine hizmet ettiğine değinmektedir (Berber ve Kaya, 01.12.2010).

Bu bağlamda, TİB’nin, erişimi engellenen sitelerin isimlerini yayınlama konusundaki endişe ve kaygılarını makul ve mantıklı görmekle birlikte, tüm ileri sürülen gerekçelere rağmen, engelli sitelerin sayısal verilerinin yayınlanmasının açıklık politikası ve şeffaf yönetim ilkesi açısından daha doğru bir tercih olacağı açıktır. Nitekim, gayri resmi olarak erişimi engellenen sitelerin listelerini ve sayılarını yayınlayan “Engelliweb.com” adlı web sitesi hakkında TİB’nin herhangi bir idari veya hukuki girişimde bulunmaması, Başkanlığın bu konuda toleranslı olduğunun bir kanıtı sayılabilir. Aynı şekilde, resmi web sitesinde “eekg.tib.gov.tr” adresinden erişimi engellenen sitelerin sorgulanmasına imkan sağlaması da bu konudaki esnek yaklaşımın bir tezahürü olarak görülebilir.

Diğer taraftan, 5651 sayılı Kanun’da yer alan katalog suçları kapsamında, TİB’nca re’sen erişimi engellenen sitelerin suç türlerine göre oransal dağılımı TİB’nin bilinçlendirme sitesi olan “www.guvenliweb.org.tr”de yayınlanmaktadır. Buna göre, başlangıcından 21.3.2013 tarihine kadar re’sen erişimi engellenen sitelerin dağılımı şöyledir: Müstehcenlik %74,82, çocukların cinsel istismarı %18,88, fuhuş %4,66, kumar %1,31, intihara yönlendirme %0,14, Atatürk aleyhine işlenen suçlar %0,09,

sağlık için tehlikeli madde %0,08, uyuşturucu ve uyarıcı madde %0,02 (Güvenliweb, 2013). Görüldüğü gibi, müstehcenlik, çocukların cinsel istismarı ve fuhuş suçları tüm engelleme tedbirlerinin %98,36 gibi büyük bir çoğunluğunu oluşturmaktadır.

5651 sayılı Kanun yürürlüğe girdikten sonra, ilk engelleme kararı Atatürk aleyhine işlenen suçlar kapsamında Ankara 11. Sulh Ceza Mahkemesi tarafından verilmiştir. Akabinde birçok mahkemeden Atatürk aleyhine işlenen suçlar ve TCK'nın 301. maddesinde yer alan Türklüğü, Cumhuriyeti, Devlet kurumlarını ve organlarını aşağılama suçundan dolayı erişim engelleme kararları gelmiştir(Türk İnternet, 2008).

Katalog suçlarına ilişkin en yoğun tartışma Atatürk'e hakaret sebebiyle Youtube'un engellenmesi nedeniyle ortaya çıkmıştır. 5651 sayılı Kanun yürürlüğe girmeden önce de mahkeme kararı ile aynı nedenle erişimi engellenen Youtube, bu Kanun'dan sonra da mahkeme kararları gereği TİB'nca erişime kapatılmıştır. Youtube'un kapatılması Türkiye'de ve Dünya'da büyük yankı uyandırmıştır. Nitekim bu durum AB 2008 Türkiye İlerleme Raporu'nda ifade hürriyeti önündeki engellerden birisi olarak metne girmiştir (Eur-lex, 2008a). Bu süreçte TİB, Youtube yetkilileriyle farklı zamanlarda yaptığı birçok görüşmeden sonuç alamamış, Youtube her seferinde TİB ile işbirliği yapmayı reddetmiştir (TK, 2008). İlerleyen süreçte, kısmi bir uzlaşuya varılmış ve her bir erişim engellemesinden sonra Youtube'un söz konusu içerikleri kaldırmasıyla erişim tekrar sağlanmıştır.¹²⁰ Diğer yandan, Türkiye Youtube web

¹²⁰ Atatürk'e hakaretle ilgili engellemelerin oluşturduğu sorunlar sebebiyle bu suç türünün Yasa'dan çıkartılması için teklifler de yapılmıştır. Örneğin Av. Atamer'in değerlendirmesi şöyledir: "Mustafa Kemal Atatürk'ün Türkiye'nin kurucusu, tarihsel atası ve manevi önderi olarak saygıdeğer kişiliğine yönelik hakaret suçunun İnternet siteleri vasıtasıyla işlenmesi her ne kadar rahatsız edici olsa da, Atatürk'ün manevi şahsiyetine hakaret suçu bir erişim engelleme nedeni olmamalıdır. Şöyle ki, her şeyden önce Atatürk'ün manevi şahsiyeti zaten 5816 sayılı kanunla koruma altına alınmış olup söz konusu suçu işleyenler için 1 yıldan 3 yıla kadar hapis cezası öngörülmüştür. Dolayısıyla bir web sitesi vasıtasıyla Atatürk'e hakaret eden bir kişi için soruşturma makamları gerekli soruşturmayı yaparak faili tespit ederek cezalandırılmasını sağlayabilmektedir. Buna ek olarak erişim engelleme tedbirinin uygulanması fiilen imkansız, orantısız ve gereksiz bir tedbirdir. Kaldı ki Atatürk'e hakaret suçunun erişim engelleme gerekçesi olduğunu bilen kişiler özellikle bu suçu işleyerek 5651 sayılı yasayı bir nevi kötüye kullanmaktadır. Bu sayede devlet 5651 sayılı yasayı uygulayıp Atatürk'e hakaret içeren her siteyi (başta Youtube olmak üzere) erişime kapatmak ile Atatürk'e hakaret içeren sitelere göz yummak, bir başka deyişle kanunu uygulamamak arasında bir tercih yapmaya zorlanmaktadır. Bu itibarla Atatürk'e hakaret bir erişim engelleme sebebi olmamalı ancak Atatürk'e internet siteleri ile hakaret eden kişilerin işlediği suçlar ilgili kanun çerçevesinde soruşturulmalı ve kovuşturulmalıdır."(Atamer, 2012).

sitesini engelleyen tek ülke değildir. İran, BAE, Fas, Tayland, Irak, Brezilya, Avustralya (okullarda), Çin ve Hindistan gibi devletler farklı nedenlerden ötürü Youtube'a erişimi engellemişlerdir (Mashable (2007)).

Youtube'un engellenmesi dışında, dünyaca ünlü e-ticaret platformu alibaba.com'un, evrimci biyolog Richard Dawkins sitesinin, Google'nin blogger.com ve blogspot.com servislerinin, Geocities'in, Wordpress'in myspace.com'un ve dailymotion.com'un engellenmesi gibi uygulamalar Türkiye'de ve dünyada çeşitli tartışmalara ve sansür eleştirilerine neden olmuştur. Açık İnternet Girişimi (OpenNet, 13.11.2012), Freedom House (Freedom House, 2011), Dünya Sınır Tanımayan Gazeteciler Örgütü (RSF, 2012), AGİT (Akdeniz, 2010a) gibi uluslararası örgütler yanında ülke içinde akademisyenler, hukukçular ve STK'lar¹²¹ bu engellemelerden dolayı ifade ve bilgi edinme hakkına müdahale edildiği gerekçesiyle TİB'na karşı eleştiriler yöneltmişlerdir.

Halbuki, tarafsız olarak incelendiğinde, söz konusu erişim engellemelerinin tamamının mahkeme kararı ile gerçekleştirilmiş olduğu ve Geocities sitesinin engellenmesi dışında diğer engellemeler ile TİB'nın hiçbir ilgisinin olmadığı görülmektedir. Dolayısıyla bahsi geçen erişim engellemelerine ilişkin eleştirilerde TİB'ni muhatap almak yerine, eleştirileri ilgili mevzuata, mahkeme kararlarına ve uygulanma yöntemlerine yöneltmek daha hakkaniyetli olacaktır.

Zira, bu süreçte dile getirilen eleştirilerde bilerek veya bilmeden yapılan bir hataya dikkat çekmek gerekmektedir. O da, 5651 sayılı Kanun'un yürürlüğe girmesinden sonra Türkiye'de meydana gelen erişim engellemesi uygulamalarının tamamının bu Kanun kapsamında ve TİB'na gerçekleştiğine ilişkin yanlış bilgidir. Hukukçular arasında 5651 sayılı Kanun'dan sonra katalog suçları dışında herhangi bir konuya

¹²¹ Örneğin, TBD, INETD, TİD, LKD, TİEV ve TUBİDER'in İnternet yasaklarının Türkiye'ye zarar verdiğini bildiren açıklaması için bkz. **"İnternet Yasakları Türkiye'ye Zarar Veriyor"**, 24.3.2008, <http://www.tiev.org.tr/modules.php?name=News&file=article&sid=1546>; Sektördeki 30 STK'nın ortak başka bir deklarasyonu için bkz. **"Sansüre karşı ortak deklarasyon"**, 23.06.2010, <http://www.ntvmsnbc.com/id/25108644/>; Tüm bunların yanında "http://bt-stk.org.tr", "http://kampanya.org.tr" ve "http://yasakli.org.tr" gibi web sayfalarında pek çok kampanya başlatılmış ve yasaklar yayınlanan bildirilerle protesto edilmiştir.

ilişkin engelleme kararının alınamayacağına dair görüşler bulunsa, uygulamada telif ve kişilik hakları ihlalleri ile özel yaşamın gizliliği ile ilgili nedenlerden dolayı mahkemelerin erişim engellemesi kararları vererek doğrudan ilgili erişim sağlayıcılar aracılığıyla bu kararları uygulattıkları görülmektedir da (Akdeniz ve Altıparmak, 2008: 42-49, 54-55).

Nitekim, iç ve dış kamuoyunda ses getiren söz konusu erişim engellemesi uygulamalarının çoğu bu kapsamdadır. Bunlardan alibaba.com, myspace.com ve dailymotion.com siteleri ile blogger.com ve blogspot.com servislerinin telif hakkı ihlalleri nedeniyle,¹²² Richard Dawkins'in sitesi ile Wordpress'in, hakaret ve kişilik hakları ihlalleri gerekçesiyle engellemeye tabi tutulduğu görülmektedir.¹²³

Ayrıca, 5651 sayılı Kanun kapsamı dışında burada bahsedilen konulardan başka nedenlerle mahkemelerce verilen erişim engellemesi kararları da bulunmaktadır. Buna göre, TCK'nın 301. maddesinde yer alan "Türklüğe hakaret"ten ve terör ve PKK lehine propaganda yapmaktan dolayı 3713 sayılı TMK kapsamında engellenen web siteleri de bulunmaktadır.¹²⁴ Dolayısıyla, Türkiye'deki erişim engellemelerini "5651 sayılı Kanun kapsamındaki engellemeler" ve "5651 sayılı Kanun dışındaki mevzuata göre yapılan erişim engellemeleri" olarak ikiye ayırmaksızın, toptancı bir anlayışla hepsiyle ilgili olumsuzlukları ve eleştirileri 5651 sayılı Kanun'a ve TİB'na yöneltmek doğru olmayacak, ilgili Yasa'ya ve TİB'na haksızlık olacaktır (Türkiye Bilişim Vakfı, 2011:2-3).

Keza, kendileriyle görüştüğümüz TİB çalışanları bu konuda kendilerine haksızlık yapıldığını, özellikle Youtube'un kapatılması üzerinden hem ülke içinde, hem de ülke dışında TİB ve Türkiye ile ilgili bir "sansürcü" algısının oluşturulduğunu,

¹²² Bkz. Akdeniz ve Altıparmak, 2008: 42-49; Metin Yılmaz, "alibaba.com kapatmasının 5651 ya da TK ile ilişkisi yok", 6.3.2008, <http://turk.internet.com/haber/yazigoster.php3?yaziid=20398>; Çetin Kasırga, "BlogSpot ve Blogger Erişime, Telif Hakkı Nedeniyle Engellendi", 24.10.2008, <http://turk.internet.com/haber/yazigoster.php3?yaziid=22246>; Özgür Uçkan, "Myspace, Lastfm, sansür, kültür ve "bir avuç insan"...", 20.9.2009, <http://sansuresansur.blogspot.com/2009/09/myspace-lastfm-sansur-kultur-ve-bir.html>

¹²³ Bkz. Akdeniz ve Altıparmak, 2008: 44-47.

¹²⁴ Bkz. Akdeniz ve Altıparmak, 2008: 47-48.

kendilerinin de bu algının oluşumuna engel olamadıklarını belirtmektedirler (Osman N. Şen ile kişisel iletişim, 06.08.2013; Ömer Boz ile kişisel iletişim, 30.07.2013).

Diğer yandan, 5651 sayılı Yasa kapsamı dışında mahkeme kararı ile doğrudan İSS'lar tarafından gerçekleştirilen engellemelerde TİB'nin devre dışı kalması uyar-kaldır sürecinin işletilmesine engel olmaktadır. Hem, içerik düzenlemelerinin bu en çok kabul gören yönteminin uygulanmasına imkan vermemesi, hem de uygulama birliğini bozması nedeniyle 5651 sayılı Yasa dışındaki erişim engelleme karar ve uygulamaları eleştirilmektedir (Türkiye Bilişim Vakfı, 2011:2). Nitekim, erişim sağlayıcılar bu yöntem ile erişim engellemesi yapılmasına karşı çıkarak, uygulamada birlik sağlamak amacıyla TİB'nin engelleme kararlarında tek elden uygulama yapacak merkezi bir aracı kurum olarak yapılandırmanın daha doğru olacağını dile getirmektedir (Vodafone, 2012).

Erişim engellemelerine ilişkin önemli eleştirilerden birisi de, TİB'nin idari tedbir olarak re'sen uyguladığı engelleme kararlarına yöneliktir. Bu bağlamda, Anayasa'ya göre haberleşme özgürlüğü ve özel yaşamın gizliliğine müdahaleye ancak bir mahkeme tarafından karar verilebileceği; bu nedenle yapılan idari işleme ilişkin olarak idare mahkemelerine itiraz yolu açık dahi olsa, ortaya çıkan bu Anayasal eksikliğin giderilemeyeceği iddia edilmektedir (Akdeniz ve Altıparmak, 2008: 71). Bu görüşten hareketle, TİD ve TBD, Anayasa'da şikayet kurumu olarak öngörülmediklerinden Anayasa Mahkemesi'ne gidememişlerse de, TİB'na tanınan yetkilerin anayasaya aykırılığını ileri sürerek, 5651 Sayılı Kanun kapsamında çıkartılan yönetmeliklerin tümünün iptali için Danıştay'a dava açmıştır (Nebil, 2008b). Fakat henüz Danıştay'dan bu konuda herhangi bir iptal kararı çıkmamıştır.

Diğer yandan, yasadışı ve zararlı içeriklerle mücadele kapsamında, idari kurumların kararlarıyla doğrudan veya yönlendirmeleriyle dolaylı olarak “öz düzenleme” çerçevesinde “zorunlu gönüllük” şeklinde ya da sektördeki büyük şirketlerle özel anlaşmalar yapma yoluyla, erişim engelleme veya filtreleme yapılmasına ilişkin uygulamaların tüm dünyada yaygın olarak kullanıldığına ülke uygulamalarında sıkça rastgelinmişti. Nitekim, AB ülkelerinde; İngiltere'de çocuk pornografisi ve ırkçılıkla

mücadele etmek amacıyla IWF'nin oluşturduğu kara listelerin, ülkedeki tüm erişim sağlayıcılar tarafından “gönüllü” olarak kullanılmakta olduğuna, benzer şekilde Fransa, Finlandiya, Danimarka, İsveç ve Norveç'te İSS'ların, güvenlik birimlerinin sağlamış oldukları kara listelere erişimi engellemekte kullandıklarına, yine, Almanya'da Federal Hükümetin, varılan anlaşma gereği İSS'larına pornografi, şiddet ve neo-Nazi aktivitelerine yönelik yasadışı web sitelerini içeren kara liste sağlamakta olduğuna daha önce değinilmişti.

Nitekim, Söyler de bu konuya dikkat çekerek, birçok Avrupa ülkesinde bu türden idari kararlarla filtreleme ve erişim engelleme uygulamalarının gerçekleştirildiğini belirtmektedir. Özellikle terör konusunda, ulusal güvenlik gerekçesiyle idari mercilere İnternet içeriğini izleme ve müdahalede bulunmayla ilgili geniş bir hareket alanı verildiğini dile getirmektedir (Yasin Söyler ile kişisel iletişim, 01.08.2013).

Diğer yandan, Boz konuyla ilgili ilginç bir duruma dikkat çekmektedir. TİB'nin göreve başladığı günden bu yana re'sen engellemelerle ilgili olarak yapılan onbinlerce idari işleme rağmen, bu işlemlere karşı TİB aleyhine açılmış dava sayısı sadece beş ile sınırlıdır. Bunların 2'si kumar ve bahis, 3'ü müstehcenlikle ilgidir ve hepsinde mahkemeler işlemleri hukuka uygun bulmuştur. Keza, AİHM'nden de bugüne kadar konuyla ilgili olumsuz bir karar çıkmamıştır. Bu durum TİB'nin Yasa ile kendisine verilen re'sen engelleme yetkisini özenle ve hukuka uygun olarak kullandığına bir delil sayılabilir (Ömer Boz ile kişisel iletişim, 30.07.2013).

Bunun yanında, Türkiye AHİM'de, Atatürk'e hakaretle ilgili mahkemece verilen ve TİB'nin uyguladığı erişim engelleme kararından dolayı haksız bulunmuş ve mahkum olmuştur. Bu davada, Denizli 2. Sulh Ceza Mahkemesi'nin 23.6.2009 tarihli kararıyla Google Sites hizmetinin yasaklanmasıyla birlikte, akademik çalışmalarını yayınladığı kendi sitesine erişme hakkından yoksun bırakılan Ahmet Yıldırım'ın başvurusuyla Türkiye ifade özgürlüğünü ihlal etmekten mahkum edilmiştir (Aru, 2012a).

Mahkeme kararını, 5651 sayılı Yasanın 8. maddesinin AİHS'nde 10. maddede ifade özgürlüğünün sınırlarını belirleyen düzenlemenin “yasayla öngörülebilirlik” şartını

yerine getirmemekte olduğu, başvurucuya demokratik bir toplumda hukuk devletinin sağladığı korumayı sağlamadığı gerekçesiyle vermiştir. AİHM, sorunun Türkiye'deki mahkemelerin işleyişinde değil, 5651 sayılı Yasa'da olduğunu belirtmiş ve bu çerçevede söz konusu Yasa'nın ifade özgürlüğü açısından yeniden düzenlenmesi gerektiğini belirtmiştir (Aru, 2012a).

Bu karar hem Türkiye hem de dünyaki içerik düzenlemeleri açısından önemlidir. Çünkü, sadece Türkiye'de değil Avrupa'da da web 2.0 uygulamalarıyla ilgili olarak erişim engellemeleri konusunda ifade özgürlüğü kapsamında, AİHM'in aldığı ilk karardır ve örnek niteliğindedir. Karar, bundan sonra hem Türkiye hem de tüm Avrupa Konseyi ülkeleri için yol gösterici olacaktır. Keza, AİHM'de Türkiye aleyhine açılmış başka birçok dava bulunmaktadır (Aru, 2012a; Türk İnternet, 2012).

Nitekim, 5651 sayılı Yasa uygulamasının, AİHM içtihadında yer alan ve elverişlilik testi, zorunluluk testi ve orantılılık testi olmak üzere toplam üç aşamadan oluştuğu kabul edilen ölçülülük koşulunu taşımadığına ilişkin Türkiye'de de itirazların bulunduğu bilinmektedir (Akdeniz ve Altıparmak, 2008: 52-64; Koç, 2013).

Türkiye'deki erişim engellemelerinin hukuksal boyutu üzerindeki eleştirilerin bir kısmı da, mahkemelerin verdikleri kararlarda bilirkişi kullanmamaları ve ihtisas mahkemelerinin bulunmamasına ilişkindir. Ülkemizde bilişim hukuku alanında ihtisaslaşmış mahkemeler olmadığı için engelleme kararlarının herhangi bir hukuk mahkemesi tarafından alınabilmesi bu alanda yaşanan sorunların nedenlerinden birisi olarak görülmektedir. Türkiye'de bir iki büyük ilde, geniş bir bilirkişi desteğiyle kurulacak ihtisas mahkemelerinin verilen kapatma kararlarında daha seçici davranacağı ve kararların daha sağlıklı verilebileceği öngörülmektedir (Akgül, 2008).

3.3.3.3 İçeriğin Yayından Çıkarılması Uygulamaları

5651 sayılı Kanun'un 9. maddesi, İnternet ortamındaki yayın içeriği dolayısıyla hakları ihlal edilen kişilere, içerik sağlayıcısından veya buna ulaşamaz ise yer sağlayıcısından içeriğin yayından çıkarılmasını talep etme ve cevap hakkını düzenlenmiştir. Basın Kanunu'nun 14. maddesinde "Düzeltilme ve cevap" başlığı

altında yer alan benzer bir düzenlemeye göre oluşturulan mekanizma, hakkı ihlal edilen kişilere, bu ihlalleri giderebilme olanağı sağlamaktadır. Düzenleme, hakkı ihlal edilen kişilere, söz konusu ilk başvurusu neticesiz kalması halinde yargı yoluna başvurma imkanı sunmaktadır. Yasa, yargı kararını bu maddede belirtilen şartlara uygun olarak ve süresinde yerine getirmeyen sorumlu kişilere, altı aydan iki yıla kadar hapis cezası öngörmüştür.

TİB, hakları ihlal edilen kişilerin muhataplarını tespitte faydalı olabilecek bilgi kaynaklarına erişimleri konusunda yardımcı olmaktadır. İlk olarak, 5651 sayılı Yasa ve ikincil düzenlemeleri içerik, yer ve erişim sağlayıcılara iletişim bilgilerini İnternet ortamında herkesin göreceği bir şekilde yayınlama zorunluluğu getirerek sorumluların İnternetin anonimliğinden yararlanmasının önüne geçmeye çalışmakta ve bu yolla mağdurlara yardımcı olmaktadır.

İkinci olarak ise, Yasa ve ilgili düzenlemeler gereği TİB'e başvurarak faaliyet belgesi almış yer sağlayıcılar ile yetkilendirilmiş olan erişim sağlayıcıların listesini ve iletişim bilgilerini resmi İnternet adresinde yayınlanmaktadır. Böylece, tespit olunan ilgililerin erişim ve yer sağlayıcı olarak Başkanlık kayıtlarında yer alıp almadığını sorgulanmak ve kayıtlı olanların iletişim bilgilerine buradan ulaşılabilme mümkün olmaktadır (TİB, 2013c). TİB ayrıca, yine kendi İnternet sitesinde yer alan site bilgileri sorgu sayfasından talebe konu adreslerle ilgili olarak açık kaynak bilgi sorgusu yapılabilmesine imkan sağlamaktadır.

TİB, içeriğin yayından çıkarılmasına ilişkin düzenlemeyi aynı zamanda bir “uyar-kaldır” sistemi olarak kurgulayıp, uygulamaktadır. Buna göre, yayın içeriklerine yönelik tedbir işlemlerinde; bir İnternet sitesinin tüm içeriğine yönelik tedbirlere değil, yalnızca sorunlu içeriğin çıkartılmasına yönelik işlemlere ağırlık vermektedir. Bu kapsamda, herhangi bir erişimin engellenmesi kararı verilmeden önce suç unsuru bulunan kısmi içeriklerin yer aldığı İnternet siteleriyle, ulaşılabilir iletişim bilgileri üzerinden irtibata geçmekte ve “uyar-kaldır” yöntemi ile yalnızca suça konu içeriğin kaldırılmasını temin etmektedir (Güvenliweb, 2013).

Böylece, TİB'nca gerçekleştirilen uyar-kaldır işlemleri ile 2012 Haziran ayına kadar 108 bin içeriğin yayından çıkarılması sağlanmıştır. Bu işlemi yapılan içeriklerin 62 bini müstehcenlik, 21 bini Atatürk aleyhine işlenen suçlar, 6 bini intihara yönlendirme ve 5 bin beşyüzü yasa dışı bahisle ilgilidir (TİB, 2012). 2012 sonunda uyar-kaldır işlemi yapılan içeriklerin sayısı 130 bini geçmiştir (BTK, 2013: 111).

5651 sayılı Kanun'la düzenlenen “uyar-kaldır” mekanizması tüm dünyada kabul gören ve uygulaması yaygınlaştırılmaya çalışılan bir sistemdir. Bu nedenle, TİB'in Yasa'da yer alan bu imkanı kullanarak, yasadışı ve zararlı içerikle mücadelede erişim engellemeden ziyade bu sisteme öncelik vermesi yerinde bir tercih ve yaklaşımdır.

3.3.3.4 Güvenli İnternet Hizmeti Uygulaması

Erişim engellemelerine ilişkin eleştiriler TİB'nı, tüm kullanıcıları kapsayan zorunlu uygulamalardan ziyade kişisel tercihe dayalı seçenekli alternatif uygulamalara yöneltmiştir. Bu kapsamda; “seçmek özgürlüktür” sloganı ile Güvenli İnternet Hizmeti sunulmuş, böylece kısıtlama isteyen kullanıcılar için, diğer kullanıcıların özgürlüklerini etkilemeyecek alternatif bir hizmet ortaya konulmuştur.

Bu çerçevede, Elektronik Haberleşme Kanunu'na istinaden “Elektronik Haberleşme Sektöründe Tüketici Hakları Yönetmeliği” çıkartılmış ve Yönetmeliğin 10. maddesi uyarınca Bilgi Teknolojileri ve İletişim Kurulu'nun, “İnternetin Güvenli Kullanımı”na ilişkin 24.08.2011 tarihli ve 2011/DK-14/461 Nolu Kurul Kararıyla “Güvenli İnternet Hizmetine İlişkin Usul ve Esaslar” yayınlanmıştır (BTK, 2011b).

Buna göre, 4. madde “Güvenli İnternet Hizmeti”ni, “Abonelerin talebi üzerine, ücretsiz olarak sunulan çocuk ve aile profilinden oluşan hizmet” olarak tanımlamaktadır. Aynı maddeye göre “çocuk profili”, “Kurum tarafından işletmecilere gönderilen, çocuk profiline ilişkin listedeki alan adı, alt alan adı, IP adresi ve portlara abonenin erişiminin sağlandığı profil”; “aile profili” ise “Kurum tarafından işletmecilere gönderilen aile profiline ilişkin listedeki alan adı, alt alan adı, IP adresi ve portlara abonenin erişiminin sağlanmadığı profil”dir (BTK, 2011b).

5. maddede Güvenli İnternet Hizmetini talep etmeyen abonelerin mevcut İnternet erişim hizmetinin, herhangi bir değişiklik olmaksızın sunulmaya devam edeceği belirtilirken, 6. madde ile işletmecilere, bu Hizmeti talep eden abonelere çocuk ve aile olmak üzere iki farklı profil imkanı sunma zorunluluğu getirilmiştir. 7. madde, Güvenli İnternet Hizmeti profillerinin seçiminin ilk abonelikte, çağrı merkezi, bayi kanalı ya da İnternet sitesi aracılığıyla yapılmasına imkan sağlanmasını ve söz konusu hizmetin ücretsiz olmasını düzenlerken; aile profilinin seçilmesi halinde şu alt seçeneklerden birini veya birkaçını seçebilmelerine ya da herhangi bir alt seçim yapmamalarına olanak sağlanmasını öngörmektedir: a) oyun site ve uygulamalarına girmek istemiyorum, b) Sohbet site ve uygulamalarına girmek istemiyorum, c) Sosyal Medya site ve uygulamalarına girmek istemiyorum (BTK, 2011b).

10. madde, Çocuk ve Aile Profil listelerinin oluşturulmasına ilişkin kriterlerin, Çocuk ve Aile Profil Kriterleri Çalışma Kurulu tarafından tespit edileceğini belirterek, ihdas edilen Kurul'un yapısını ve görevlerini düzenlemektedir (BTK, 2011b).

11. madde, başvuru ve itirazların değerlendirilmesini düzenlemiştir. Buna göre, kullanıcılar ve İnternet site sahipleri, İnternet sitelerinin değerlendirilmesi için Kurumca hazırlanan İnternet sayfası üzerinden başvurabilirler ve itiraz edebilirler. Kullanıcılar, başvurularını “Profil Düzenleme İnternet Sayfası”nda bulunan bağlantı ile, itirazlarını ise “Uyarıcı ve Bilgilendirici İnternet Sayfası”nda bulunan bağlantı vasıtasıyla yaparlar. Söz konusu başvuru ve itirazlar işletmeciler tarafından BTK’na gönderilir. BTK, başvurular ve itirazların değerlendirilmesi için Çocuk ve Aile Profil Kriterleri Çalışma Kurulu'nun görüşüne başvurabilir (BTK, 2011b).

12. maddede işletmecilerin bu Hizmet’in sunulması için gerekli altyapıyı kuracakları ve işletecekleri, BTK’unca İşletmecilere sadece listelerin gönderileceği belirtilmiştir. İşletmecilerin, BTK’unca gönderilen listeler üzerinde değişiklik yapamayacakları fakat, Güvenli İnternet Hizmetine ek olarak değişik isimler altında farklı hizmetler sunabilecekleri ayrıca düzenlenmiştir. 14. madde ise, işletmecilere abonelerine bu Hizmet’in tanıtımı için içeriği BTK tarafından uygun görülen bilinçlendirme amaçlı bilgilendirici metinleri gönderme zorunluluğu getirmiştir (BTK, 2011b).

Nitekim, 22.11.2011 tarihinden itibaren BTK Güvenli İnternet Hizmetini İSS'ler vasıtasıyla başlatmıştır. Bu hizmette, Çocuk ve Aile Profil Kriterleri Çalışma Kurulu tarafından tespit edilen kriterlere göre¹²⁵ TİB'in hazırladığı beyaz, gri ve siyah listeler esas alınmıştır. Bu listeler referans alınarak İnternet kullanıcılarına çocuk ve aile profillerini seçme özgürlüğü getirilmiştir.

“Güvenli İnternet Hizmeti”ne verilen isim çerçevesinde, Şen ve Güvener'in dikkat çektiği, “İnternetin güvenli kullanımı” ve “güvenli İnternet” ile “İnternet güvenliği” terimleri arasında bazı anlam farklılıklarının bulunduğuna değinmek gerekmektedir. Literatürde genellikle “İnternet güvenliği”, “Internet security” veya “secure Internet” karşılığı olarak İnternet güvenliğinin teknik boyutu, yani teknik güvenlik anlamında kullanılmaktadır. Dolayısıyla, zombi bilgisayar, izinsiz erişim, veri güvenliği, virüsten korunma, siber saldırı önlemleri vs. bu kapsamda değerlendirilmektedir ve bu alan teknikçilerin alanıdır. “İnternetin güvenli kullanımı” veya kısaca “güvenli İnternet” ise, “safer use of Internet”, “safe Internet” veya “Internet safety” karşılığı olarak daha çok İnternet içerik güvenliği kapsamında İnternetteki yasadışı veya zararlı içeriğe erişimi önlemek anlamında kullanılmaktadır. Dolayısıyla, bilinçlendirmeyi de kapsayan bu alan, İnternetin sosyal boyutunu ve sosyal bilimcileri ilgilendirmektedir (Osman N. Şen ile kişisel iletişim, 06.08.2013; Lutfi Güvener ile kişisel iletişim, 24.07.2013).

Nitekim, BTK'da benzer bir yaklaşımla, 22.02.2011 tarihli ve 2011/DK-10/91 sayılı ilk Kurul kararında Güvenli İnternet Hizmetinin adını “İnternetin Güvenli

¹²⁵ Kurul'un belirlemiş olduğu kriterler şöyledir: “1- Güvenli İnternet Hizmeti kapsamında yer alan web siteleri için, web sitelerinin kriterlere uygunluğu hususunda site sahiplerinin beyanı esastır. 2- Güvenli İnternet Hizmeti'nde; eğitim, kültür, sanat, iş, ekonomi, bankacılık ve finans, kariyer, medya, alışveriş, İnternet hizmeti, sağlık, spor, müzik, oyun vb. konularda içerik barındıran web siteleri ile resmi kurum ve kuruluşlara ait web siteleri yer almalıdır. 3- Güvenli İnternet Hizmeti'nde; kumar, intihara yönlendirme, Atatürk'e hakaret, çocukların cinsel istismarı, uyuşturucu ve uyarıcı madde kullanımını kolaylaştırma, sağlık için tehlikeli madde temini, fuhuş, müstehcenlik, ırkçılık, ayrımcılık, nefret, terör, şiddet-vahşet görüntüleri, kan ve şiddet içeren dövüş sporları, hayvan dövüşleri, dolandırıcılık, zararlı yazılım vb. içerikleri barındıran web siteleri ile bu içeriklere erişilmesini sağlayan web siteleri ve uygulamaları yer almamalıdır. 4- Güvenli İnternet Hizmeti'nde 3. maddedeki unsurlarla ilgili, örtülü reklam, bilinçaltını etkileyen reklam ve güdüleme içeren hiçbir içeriğin bulunmadığı web sitelerine yer verilmelidir. 5- Telif hakları, sağlık için tehlikeli madde temini, dijital oyunların envanteri, tütün ve alkol satışı gibi konularda uzman kurum ve kuruluşların görüşlerinin tam olarak yansıtılabilmesi önem arz etmektedir.”(BTK, 2011c).

Kullanımı” olarak belirlemişti (BTK, 2011d). Fakat, daha sonra 24.08.2011 tarihli ve 2011/DK-14/461 sayılı Kararı ile bu ismin uzun olduğu düşüncesiyle söz konusu uygulamanın adı kısaltılarak “Güvenli İnternet Hizmeti” olarak değiştirilmiştir.

Şen ise, bu kavramların ülkemizde birbirine karıştırıldığını ve çoğu zaman da bilerek ya da bilmeyerek birbirinin yerine kullanıldığını belirtmektedir. Şen’e göre, İnternet bir araçtır ve nötr bir değer taşır; bu nedenle tek başına “güvenli” veya “güvensiz” olarak nitelendirilemez. Dolayısıyla, “Güvenli İnternet” kavramı da yanlıştır, doğru terim “İnternetin güvenli kullanımı”dır. Çünkü “İnternetin güvenli kullanımı” terimi, İnternetin bizzat kendisinden ziyade, kişinin tercih ve iradesini ön plana çıkartmakta ve kullanım güvenliğine odaklanmaktadır. Doğru olan yaklaşım budur ve AB’de terimi bu anlamıyla kullanmaktadır (Osman N. Şen ile kişisel iletişim, 06.08.2013; Lütfi Güvener ile kişisel iletişim, 24.07.2013).

Diğer yandan, Güvenli İnternet Hizmeti, hazırlık aşamasında ve uygulamaya geçildikten sonra bazı kesimlerce yoğun eleştirilere maruz kalmıştır. Bazı STK’lar ve uzmanlar söz konusu uygulamayı devlet eli ile merkezi filtre uygulaması ve yeni bir sansür girişimi olarak kabul ederek “İnternetime dokunma” kampanyaları düzenlemişlerdir. Bu kapsamda basın açıklamaları, toplantılar, yürüyüşler ve protestolar yapılmıştır.¹²⁶ Fakat, Güvenli İnternet Uygulaması başladığı tarihten itibaren ilgi ile karşılanmış ve 1. yılında 1,4 milyon abone ve yaklaşık 5 milyon kullanıcı sayısına ulaşmıştır (TİB, 2012b). 2012 yılında 15.’si düzenlenen Geleneksel Tüketici Ödülleri yarışmasında, BTK, Güvenli İnternet Hizmeti dolayısıyla “Hizmet Ödülü” dalında ödüle layık görülmüştür (BTK, 2012b).

¹²⁶ Bkz: Kerem Altıparmak ve Yaman Akdeniz, **İnternet Filtresi Zorunlu Değil Ama Zorunlu**, 06.08.2011, <http://www.bianet.org/biamag/ifade-ozgurlugu/131976-internet-filtresi-zorunlu-degil-ama-zorunlu>; Gökhan Ahi, **“İnternet Kurulu, Filtre ve STK Üçlüsü”**, 24.05.2011, <http://sosyalmedya.co/internet-kurulu-filtre-ve-stk-uclusu/>; **“Bir Yıldır İnternette ‘Güvendeyiz!’”**, 23.11.2012, <http://www.bianet.org/bianet/bilisim/142317-bir-yildir-internette-guvendeyiz>; **“İnternet Derneği’nden aile ve çocuk filtresine eleştiri”**, <http://www.bilisimhukuk.com/2011/11/internet-derneginden-aile-ve-cocuk-filtresine-elestiri/> (24.06.2012); **Neden İnternet’e merkezi filtre istemiyoruz?** http://www.alternatifbilisim.org/wiki/Neden_Filtre_%C4%B0stemiyoruz; **Sansüre Karşı Yürüyoruz**, http://www.alternatifbilisim.org/wiki/Sansure_Karsi_Yuruyoruz (24.06.2012).

Güvenli İnternet Hizmeti uygulaması içerik düzenlemeleri konusunda kullanıcı odaklı ve kullanıcıya farklı tercih ve seçeneklerde bulunmayı sağlama açısından dikkate değer bir uygulamadır. Nitekim, bizdeki Güvenli İnternet Hizmetinin daha ileri uygulamasının İngiltere’de başlatılacağı 2013 yılı Temmuz ayında İngiltere Başbakanı Cameron tarafından kamuoyuna duyurulmuştur. Söz konusu uygulama, bizdekinin aksine 2014 yılından itibaren abone olan herkesin zorunlu olarak filtreli kullanıma dahil edilmesini ve ancak başvuru durumunda filtreli kullanımdan çıkartılmasını öngörmektedir (Bianet, 22.07.2013).

Diğer yandan, Güvenli İnternet Hizmeti çerçevesinde, mevcut güvenli İnternet profillerinin yetersiz olduğu, var olan profiller haricinde “Üniversite Profili” veya “Kamu Profili” olarak yeni profillerin oluşturularak, profillerin çeşitlendirilmesinin gerektiğine ilişkin görüş ve çalışmalar da bulunmaktadır (Ardıç, 2012).

3.3.3.5 İçerik Filtreleme Uygulamaları

5651 sayılı Yasa’nın 7. maddesi, ticari amaçla olup olmadığına bakılmaksızın tüm İnternet toplu kullanım sağlayıcıların, konusu suç oluşturan içeriklere erişimi önleyici tedbirleri almakla yükümlü olduğunu düzenlemiştir. “İnternet Toplu Kullanım Sağlayıcıları Hakkında Yönetmelik”in 5. maddesi ise, İnternet kafelerin bu amaçla TİB’nce onaylanan filtreleme yazılımını kullanmalarını zorunlu kılmıştır.

Ayrıca, Yasa’nın 10. maddesi ile, TİB’na İnternet ortamında herkese açık çeşitli servislerde yapılacak filtreleme, perdeleme ve izleme esaslarına göre donanım üretilmesi veya yazılım yapılmasına ilişkin asgari kriterleri belirleme görevi verilmiştir. Keza, aynı madde, TİB’nın, bu maddeye istinaden kurulan İnternet Kurulu ile gerekli işbirliği ve koordinasyonu sağlayarak, Kurulca izleme, filtreleme ve engelleme yapılacak içeriğe sahip yayınların tespiti ve benzeri konulardaki önerilerle ilgili gerekli her türlü tedbir veya kararları almasını düzenlemiştir.

Dolayısıyla, ilgili mevzuat, İnternet kafelere TİB’nce onaylanan içerik filtreleme programlarından birisini kullanma mecburiyeti getirirken, Başkanlığa da bu programların asgari ölçütleri ve yöntemlerini belirleme görevi vermiştir. Nitekim

TİB, onaylama kriterlerini ile bu kriterlere ve teknik özelliklere uygun üretilen ve onayladığı filtre programlarını resmi web sitesinde yayınlamaktadır (TİB, 2013d).

Diğer yandan, konusu suç oluşturan içeriklerin ve suçun önlenmesi ile suçluların tespiti amacıyla İnternet kafelere, aynı yönetmeliğin 5. maddesine göre, İç IP Dağıtım Loglarını elektronik ortamda kendi sistemlerine kaydetmek ve TİB'nca 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 saklamak zorunluluğu getirilmiştir. Nitekim, TİB da hazırladığı IP Log İmzalayıcı programı web sitesinde yayımlanmaktadır(TİB,2013e).

3.3.3.6 Yetkilendirme Uygulamaları

5651 sayılı Kanun ve ilgili yönetmelikler, İnternetin önemli aktörlerini ilk kez tanımlanmış ve bu aktörlere ilişkin yükümlülükler ve müeyyidelere ayrıntılı olarak yer vermiştir. Bu kapsamda bu aktörlerin yetkilendirilmelerine ilişkin olarak TİB'na önemli görevler verilmiştir. Buna göre TİB, yer sağlayıcılara faaliyet belgesi verilmesi, bu belgelerin iptali, yer sağlayıcıların barındırdıkları alan adlarına ilişkin dosyaların kontrolü ve alan adlarının veri tabanına aktarılması, yer sağlayıcıların belgesiz faaliyet göstermelerinden ve yükümlülüklerini yerine getirmemelerinden dolayı İnternet erişiminin engellenmesi ve bu engellenmenin kaldırılması, içerik, yer ve erişim sağlayıcıların tanıtıcı bilgilerini kendi sitelerinde bulundurmalarının takibi ve bulundurmadıkları takdirde yaptırım uygulanması ve faaliyetini sonlandıran erişim sağlayıcıdan trafik bilgilerinin temini gibi işlemleri yürütmektedir(TİB, 2010).

Nitekim TİB faaliyet belgesi vermeye başladığı 17.12.2007'den 31.12.2012 tarihine kadar bu konuda 23.300 başvuru almış ve bunun 2.783'üne yer sağlayıcı faaliyet belgesi vermiştir (BTK, 2013:61). Başvurular incelendiğinde, sadece Türkiye'de mukim olan ve oldukça sınırlı sayıda kişi ve kurumun bu belgeyi aldığı ve almak için başvuruda bulunduğu görülmektedir. Konuyla ilgili caydırıcı bir ceza sistematığı bulunmadığından birçok yer sağlayıcı şirket kayıt olmama yolunu seçmektedir. Ayrıca kayıtlı olan yer sağlayıcılar da iletişim bilgileri değişikliklerini düzenli bir

şekilde bildirmediğlerinden acil bir içerik çıkarma durumunda çaresiz kalınmaktadır. Keza, kayıtlı yer sağlayıcıların zorunlu olmalarına rağmen barındırdıkları sitelerin trafik bilgilerini saklamadıkları da görülmektedir. Nitekim, bir araştırmada kayıtlı yer sağlayıcıların sadece %55'inin iletişim bilgilerini güncelledikleri, %47'sinin de trafik bilgilerini sakladıkları görülmüştür (Özbey, 2011: 125-125).

Bunun yanında, Türkiye'deki yer sağlayıcıların sunucularını özellikle barındırma maliyeti çok düşük olan ülkelerde barındırdıkları görülmektedir (Özbey, 2011: 130). Nitekim, yasa dışı içeriklerle mücadele ederken bu içeriklerin çoğunun yurtdışında barındırıldığı tespit edilmektedir. Örneğin, TİB'nca 2012 sonuna kadar re'sen erişimi engellenmiş web sitelerinin %70'e yakını ABD'de barındırılmaktadır (TİB, 2012).

Bu iki veri birlikte değerlendirildiğinde, yer sağlayıcıların kayıt altına alınarak yasadışı ve zararlı içerikle mücadeleyi öngören söz konusu düzenlemeye yeterince işlerlik kazandırılmadığı söylenebilir. Zira, yer sağlayıcıların kayıt dışı kalmaları yasadışı içerikler ile mücadeleyi zorlaştırmaktadır. Dolayısıyla, mücadelenin bu aşamada aksamalar görülmekte, yeni tedbirlere ihtiyaç duyulmaktadır.

Bu bağlamda, içeriklerin yurtdışında barındırılmasının ana sebebinin, Türkiye'de yer sağlayıcılık hizmetlerinin pahalı ve düşük hızda olması gösterilmektedir. Bu pahalılığın sebebi ise büyük oranda ağır vergi yükü ve enerji fiyatlarının yüksekliğidir. Bu nedenle, içeriklerin yurtiçine çekilmesini sağlamak için kayıtlı yer sağlayıcıların vergi yükünün azaltılması, altyapının geliştirilerek bağlantı hızının artırılması ve kayıtlı yer sağlayıcılara, özel bir tarife üzerinden elektrik enerjisi verilmesi gerekmektedir (Özbey, 2011: 42-49).

Bunun yanında, yer sağlayıcılık belgesi olmayan ve izinsiz bir şekilde bu hizmeti verenlerle ilgili caydırıcı yasal düzenlemeler yapılırken, kayıtlı içerik sağlayıcılar için iletişim bilgisi değişiklikleri bildirmemenin caydırıcı bir cezası da olmalıdır (Bozkurt, 2011:136). Keza, yer sağlayıcıların bu tip yükümlülükleri için mevcut mevzuatta yer alan yaptırımların da uygulanması gerekmektedir. TİB'nın bu güne kadar yer sağlayıcılara bu yönde bir yaptırımı olmamıştır (Özbey, 2011: 150).

Diğer yandan, yurt içinde barındırılan çocuk pornografisi içerikleri ile ilgili olarak; içerik çıkarılması için yer sağlayıcı ile iletişim kurmaya çalışıldığında yer sağlayıcı kayıtlı değil ve/veya iletişim bilgileri yanlış, ulaşılamıyor ise, sunucunun İnternet omurgasına bağlanmasını sağlayan İnternet aboneliği erişiminin abonelik iptali yolu ile kesilebilmesi önerilmektedir. Bu konuda yasal düzenlemelerde bir engel olmadığı hatırlatılarak, uygulamanın istisnai olarak çocukların cinsel istismarı içerikleri için başlatılabileceği dile getirilmektedir (Bozkurt, 2011: 136).

3.3.3.7 İnternetin Güvenli Kullanımı Uygulamaları

İlgili mevzuat, TİB’na önleyici tedbirler alma görevi kapsamında, İnternetin güvenli kullanılmasına yönelik olarak bilinçlendirme faaliyetleri konusunda birçok görev ve sorumluluklar yüklemiştir. Bunların başlıcaları şunlardır: İnternetin güvenli kullanılmasının sağlanması için bilişim şuurunu geliştirmeye yönelik eğitim ve tanıtım faaliyetlerinde bulunmak ve bu amaçla çalışma kurulları oluşturmak, ulusal ve uluslararası alanda yapılan bilinçlendirme amaçlı yayın, site, proje, kişi ve organizasyonların durumunu güncel olarak takip etmek ve paralel projeleri hayata geçirmek, bilinçlendirme amaçlı yayınları sağlamak, hazırlamak ve dağıtmak, bilinçlendirme filmleri ile çocuklara yönelik eğitici ve eğlendirici oyunlar hazırlamak ve sunmak, ulusal ya da uluslararası etkinliklere katılmak ve benzer etkinlikler düzenlemek, İnternetin güvenli kullanımına ilişkin anket ve araştırmalar yaparak projeler üretmek, kamu, özel veya sivil otoritelerce gerçekleştirilen proje ve çalışmalara destek vermek, yabancı kaynaklı raporları incelenmek ve düzenlenmek, İnternet istatistiklerini incelenmek ve yayınlanmak (TİB, 2013f).

Bu çerçevede TİB, toplumda bilişim şuurunun oluşturulması ve İnternetin güvenli, etkin ve bilinçli kullanımını sağlamak amacıyla hazırlanan, özellikle aileler, eğitimciler, çocuklar için zengin içeriklerle desteklenen, “Güvenliweb” adında bir bilinçlendirme sitesi ile hizmet vermektedir. 2008 Mayıs’ında yayına başlayan sitede, kullanıcıların bilinçlenmesine yardımcı olmak için ülkemizden ve yurtdışından derlenen e-kitap içerikleri, haberler, makaleler ve duyurular paylaşılmaktadır. İnternet kafe denetimlerinde yeknesaklığı ve verimliliği sağlamak amacıyla, mülki

idare amirliklerinin yararlanmasına dönük olarak geliştirilen e-öğrenme modülü de Güvenli Web üzerinden hizmet vermektedir. Güvenli Web portalı, Avrupa ülkeleri ile Amerika, Kanada ve Avustralya gibi gelişmiş ülkelerin Güvenli İnternet portalları arasında en çok ziyaret edilen 4. web portalı olmuştur (BTK, 2012: 75).

TİB, çocukların hem eğlenip hem de güvenli İnternet kullanımı konusunda eğitici bilgiler edinebilecekleri “Güvenliçocuk” adındaki web sitesini 2010 yılı Güvenli İnternet Gününde hizmete sunmuştur. Sitede, Güvenli Çocuk Kulübü, Oyun Parkı, Benim Sayfam, Neşeli Kutular, Neler Olmuş, Neler Olacak, Bilgi Dolabı, Eğlence Köprüsü ve Web Gözcüsü gibi bölümler bulunmaktadır (Güvenliçocuk, 2013).

TİB, toplumda bilişim şuuru geliştirmek ve güvenli İnternet kullanımı konusunda farkındalık oluşturmak amacıyla bir takım faaliyetler yapmaktadır. Bu çerçevede, MEB Talim Terbiye Kurulu tarafından onaylanan Çocuklar için “Güvenli İnternet Kullanımı İçin Tavsiyeler” adlı rehber kitapçık, Ulaştırma Bakanlığı’nın desteğiyle 12 milyon adet bastırılarak 2009-2010 eğitim-öğretim yılında tüm ilköğretim öğrencileri ile öğretmenlerine ücretsiz olarak ulaştırılmıştır. Kitapçığın 6, 7 ve 8. sınıflara yönelik baskıları Türkçe ve İngilizce olarak hazırlanmıştır. İngilizce baskılar yurtdışı etkinliklerinde tanıtım amaçlı olarak da kullanılmaktadır (TİB, 2013g).

Yine, ebeveynlere yönelik olarak “İnternetin Güvenli Kullanımı İçin Anne-Babalara Öneriler” adlı bir rehber kitapçık hazırlanmış ve ilk olarak 23 Şubat 2010’da düzenlenen “Güvenli İnternet Günü” etkinliklerinde katılımcılara dağıtılmıştır. Çocukların ve ebeveynlerin İnterneti güvenli kullanımı için tavsiyeler içeren rehber kitapçıklar, e-kitap formatında “Güvenli Web” üzerinden online olarak da yayınlanmaktadır. Ayrıca, rehber kitapçıklar broşür formatında da basılmış olup, ücretsiz olarak dağıtımı yapılmaktadır (TİB, 2013g).

TİB, güvenli İnternet kullanımı konusunda yurtiçi ve yurtdışı toplantılara katılmakta, kamu kurumları, STK’ları ve işletmeler ile işbirliği yaparak farkındalığın artırılması için faaliyetler yürütmektedir. Ayrıca, Türkiye’nin farklı illerinden gelen talepleri

değerlendirerek öğrencilere, eğitimcilere ve ebeveynlere yönelik "İnternetin Güvenli Kullanımı ve Güvenli İnternet Hizmeti" seminerleri vermektedir (TİB, 2013g).

Türkiye de TİB'nın yaptığı bilinçlendirme çalışmalarının önemli bir bölümü çocuklara, velilere ve eğitimcilere yönelik olarak gerçekleştirilirken, buna paralel olarak TİB, diğer ilgili kamu kurumları ve yetkililerine yönelik olarak da konunun öneminin anlaşılmasını sağlamak için farkındalık oluşturmaya çalışmaktadır (Lütfi Güvener ile kişisel iletişim, 24.07.2013).

Fakat, yürütülen bu faaliyetlere rağmen Türkiye'de, İnternetin bilinçli, güvenli ve etkin kullanımıyla ilgili genel kullanıcı düzeyinin yeterli olmaması çoğu vatandaşın bilişim teknolojilerinin verimlilik artışında sağladığı olumlu etkiden yeterince yararlanmasına engel olurken, İnternet kaynaklı risk ve tehditleri de artırmaktadır.

Bunun yanında, ülkemizde adeta bir dijital nesil kopukluğu yaşanmaktadır. Çocukların ve gençlerin İnternet kullanımı ve bilgi düzeyi olarak ebeveynlerine oranla seviyelerinin daha iyi olması yanında, her iki neslin İnternet ile ilişkisi birbirinden oldukça farklılık göstermekte, bu konuda birbirlerini anlamakta zorlanmaktadırlar (Çubukcu ve Bayzan, 2013:151). Bu durum zararlı içerikten korunmalarında ebeveynlerin aktif rol almasını engellemektedir. Dolayısıyla, ebeveynlerin ve eğitimcilerin İnternetin bilinçli, güvenli ve etkin kullanımıyla ilgili ve İnternet okuryazarlığı düzeylerinin düşük olmasından ötürü çocuklara ve gençlere etkili yönlendiricilik yapamamaktadır. Bu çerçevede, İnternetin güvenli kullanımı her düzeydeki kullanıcı açısından önemli olmakla birlikte, özellikle çocuklar ve gençler için öncelikli bir ihtiyaç olduğundan rehber konumunda bulunan eğitimciler ve ailelere yönelik bilinçlendirme ve eğitim faaliyetleri büyük önem taşımaktadır.

Bu kapsamda, var olan bilgiye medya ve İnternet aracılığıyla eleştirel bir bakış açısıyla sahip olma yaklaşımı ile eleştirel düşünme ve medyayı doğru kullanma becerilerinin arttırılması ve medya manipülasyonu karşısında onları daha bilinçli hale getirmeyi hedefleyen medya okur-yazarlığı eğitimi ön plana çıkmaktadır (RTÜK, 2013).

Ülkemizde ise, ilköğretim ve ortaöğretim okullarında 2012 yılına kadar gösterilen bilgisayar derslerinin bilinçli bilgisayar ve İnternet kullanımıyla ilgili olarak yetersiz kaldığı, 2006 yılında müfredatımıza seçmeli olarak giren medya okur-yazarlığı dersinin de mevcut içeriği ile yeterli olmadığı görülmüştür (TBMM, 2013: 536). Özellikle medya okur-yazarlığı dersiyle bilinçli İnternet kullanımıyla ilgili kısmi bir bilgi düzeyi oluşturulsa da, bu dersin hem seçmeli hem de daha çok medya araçlarının tanıtımı ve nasıl kullanılacağına anlatılması şeklinde ele alınması ve televizyon üzerinde yoğunlaşmış olması İnternetin bilinçli kullanılmasıyla ilgili beklentilerin karşılanmasının önünde engel oluşturmaktadır (MEB ve RTÜK, 2006).

Oysa günümüzde kullanımı hızla artan İnternete ilişkin olarak çocuklara ve gençlere bilinçli kullanma ve eleştirel düşünme yaklaşımının kazandırılması büyük öneme sahiptir. Bugün Avrupa’da ilköğretim düzeyinde İnternetin bilinçli kullanımıyla ilgili müfredatı olmayan tek Avrupa ülkesi Türkiye’dir (TBMM, 2013: 536). Ülkemizde de bilinçli İnternet kullanımıyla ilgili ders programları oluşturulup müfredata yerleştirilmelidir. Keza, okullar dışında da tüm kullanıcılara yönelik olarak bilişim/teknoloji/İnternet okur-yazarlığını geliştirecek çözümler üretilmelidir.

Bilinçlendirme konusuyla bağlantılı olarak İnternet okur-yazarlığıyla birlikte İnternet etisinin geliştirilmesi de ayrıca üzerinde durulması gereken bir konudur. Zira, gerçekleştirilen İnternetin güvenli kullanımı faaliyetleri, etik konusunu da işleyerek bu görevi yerine getirebilecek altyapı ve birikime sahip bir çalışma alanıdır (Arıkan, 2011:94). İnternet toplumunda kabul gören ya da kabul görmeyen davranışlar bulunduğu ve bu toplumun bir ferdi olarak insanların etik ilke ve prensipler dahilinde yaşaması gerektiği bütün insanlara benimsetilmelidir.

3.3.3.8 Koordinasyon Çalışmaları

TİB’na ilgili mevzuatla, bilişim ve İnternet alanındaki faaliyetler ile ilgili yurt içi ve yurt dışı gelişmeleri takip etmek, bu kapsamda ulusal ve uluslararası kurum ve kuruluşlarla işbirliği ve koordinasyonu sağlamak ve gelişmelerin Başkanlık hizmetlerine yansıtılması için önerilerde bulunmak görevleri verilmiştir.

Bu çerçevede, TİB, AB Güvenli İnternet Programını takip etmekte, programdaki hedeflere uygun çalışmalar yapmakta ve AB Komisyonu Bilgi Toplumu ve Medya Genel Müdürlüğüyle irtibatlı olarak çalışmalar hakkında bilgi alışverişinde bulunmaktadır. Bu kapsamda, içerik düzenlemeleri konusunda AB uygulamalarını incelemek ve bu konudaki Türkiye uygulamalarını anlatmak üzere Hollanda, İngiltere, Fransa ve İtalya'ya ziyaretler gerçekleştirilmiş; STK'ları ve ilgili kamu kurumları ile görüşmeler yapılmıştır. Keza, TİB, 23.02.2010 tarihinde İstanbul'da ITU ve AB INSAFE programı yetkililerinin de katıldığı “Güvenli İnternet Günü” etkinlikleri düzenlemiştir. Yapılan çalışmalar sonucunda Türkiye AB'nden “Safer Internet Programme”na katılım daveti almıştır. Program'a katılım süreci, Dışişleri Bakanlığı ve AB Bakanlığı ile koordineli olarak devam etmektedir (TİB, 2013h).

TİB'nin girişimleri sonucu, OECD ve Asya-Pasifik Ekonomik İşbirliği Örgütü (APEC)'nün düzenlemiş oldukları “Çocuklar İçin Güvenli İnternet Ortamı Teşvik İnisiyatifleri Konusunda APEC-OECD Sempozyumu”nun hazırlıkları çerçevesinde, Türkiye'deki içerik düzenlemeleri ve TİB'nin uygulamalarıyla ilgili bilgiler OECD'nin hazırlamış olduğu “Online Ortamda Çocukların Korunması” adlı raporda yer almıştır (TİB, 2013h).

Diğer yandan, 5651 sayılı Yasa yürürlüğe girdikten sonra Türkiye'de İnternet içerik düzenlemesiyle ilgili önemli adımlar atılırken, konuya ilişkin eksikliği en çok hissedilen hususlardan birisi yerli içeriğin yetersizliğidir. İçerik düzenlemelerinde filtreleme ve erişim engelleme gibi sevimsiz yöntemlere karşılık daha sempatik geldiği için giderek daha da önemli hale gelen pozitif içeriğin çoğaltılması kapsamında, ülkemizde yerli içeriğin artırılmasının gerektiği konusu sıkça dile getirilmektedir. Bu zorunluluk mülakata katılan tüm uzmanlarca da teyit edilmiştir.

Nitekim, Şen, dünyada olduğu gibi ülkemizde de İnternet içeriğinin düzenlenmesi konsepti içinde pozitif içeriğin artırılmasına yönelik çalışmaların gerekliliğine önemle vurgu yapmaktadır. Şen'e göre, kamu/özel sektör/sivil toplum kuruluşları ve kullanıcıların pozitif içerik oluşturmaları bir takım düzenlemelerle teşvik edilmelidir. Bu şekilde, web sitesi bulunan her bir kamu veya özel sektör kuruluşunun çocuk ile

başlayan bir alt alan adına sahip olması sağlanabilir. Örneğin, “www.cocuk.selcuk.edu.tr” gibi (Osman N. Şen ile kişisel iletişim, 06.08.2013).

Aydın’a göre de, Türkiye’deki kullanıcıya hitap eden Türkçe içeriğin artırılması ve zenginleştirilmesi, uygulamaların geliştirilmesi ve gerçekten vatandaşın işine yarayan, ihtiyacını gideren kamu hizmeti, eğlence, ticaret, bilgi alma gibi her alanda içeriğin üretilmesi gerekmektedir. Bu anlamda ilk iş olarak kamu kurumları ellerinde gizlilik derecesi olmayan yayınlayabileceği ne varsa içerik haline getirebilirler (Emin S. Aydın ile kişisel iletişim, 25.07.2013).

Bu konuya TBMM Bilişim Komisyonu Raporu’nda da değinilmiş ve İnternet kullanıcılarına, içerik sağlayıcılar tarafından kolay erişilebilen pozitif içerik sunulmasının gerektiğinden bahsedilerek ve bu kapsamda yerli yazılımlarla İnternetteki yerli ve Türkçe içeriğin nicelik ve niteliğinin artırılması için özendirici ve teşvik edici adımların atılması istenilmiştir. Keza, yerli içeriğin yaygınlaştırılması amacıyla, vergi indirimleri ve mali kolaylıklar önerilmiştir. Ayrıca, çocuk ve ergenler için özel eğitici, eğlendirici ve bilgilendirici pozitif içerik bulunan web sitelerinin yapımı, ansiklopedik bilgi içeren resmi bir İnternet sitesinin yayına başlaması teklif edilmiştir (TBMM, 2013: 740, 968).

Benzer şekilde, Onuncu Kalkınma Planı (2014-2018)’nda sayısal içeriğin gelişmesi ve ticarileşmesi için başta oyun olmak üzere mobil uygulama, yazılım ve hizmetlerin destekleneceği, İnternetteki Türkçe içeriğin nicelik ve nitelik açısından gelişmesi ve erişilebilir olmasının sağlanacağı kayıt altına alınmıştır (DPT, 2013c: 111). Yine aynı konu ile ilgili olarak 655 sayılı KHK ile İnternet Geliştirme Kurul’una “Türk Kültürü, Türk Tarihi ve Türk Dünyasıyla ilgili bilgilerin İnternet ortamında daha fazla yer alması ve bunların tanıtılması hususunda çalışmalar yapmak, yaptırmak ve öneriler hazırlamak” görevi verilmiştir.

Diğer yandan, Bilgi Toplumu Stratejisinin Yenilenmesi Projesi kapsamında hazırlanan “İhtiyaç Tespiti ve Öneriler Raporu”nda bu konunun gündeme getirilmiş olması gelecek açısından ümit vericidir. Nitekim, Rapor’da nitelikli dijital içerik

üretim alışkanlıklarının geliştirilerek içeriğin zenginleştirilmesi kapsamında öğrencilerin nitelikli dijital içerik üretimine teşviki, İnternette faydalı ve ihtiyaçları karşılayan hizmetlerin ve uygulamaların çeşitlendirilerek geliştirilmesi kapsamında e-devlet ve e-belediyecilik hizmetlerinin artırılması, sanal kütüphane ve müzelerin oluşturulması gibi tespit ve önerilere yer verilmiştir (Bilgitoplumustratejisi, 2013a).

Bu çerçevede gündeme getirilen diğer bir konu da, Türkiye’deki İnternetin Facebook, Google ve Hotmail gibi küresel batılı içerik platformlarının hakimiyetinde bulunması gerçeğidir.¹²⁷ Bu platformların sunduğu içeriklerin Türkiye’deki İnternet kullanıcıları arasındaki yaygın kullanımı bunu açıkça göstermektedir. Buradan hareketle Güvener, Türkiye’nin bu küresel platformlara mahkum olmaması için hızla yerli pozitif içerik üretmesi ve güçlü yerli içerik sağlayıcılara sahip olması gerektiğini belirtmektedir. Güvener, buna mukabil ülkemizde içerik sağlayıcıların sektör olarak dahi kabul edilmediğine dikkat çekmektedir (Lütfi Güvener ile kişisel iletişim, 24.07.2013).

Güvener’e göre, Google ve Facebook benzeri şirketlerin tekellerinin kırılması için yerel içerik sağlayıcıların geliştirilmesi gerekmektedir. Özellikle hemen para kazanamayacak sosyal içerikler ve arama motorlarıyla ilgili olarak devlet teşvik edici olmalıdır. Twitter piyasaya çıktıktan 5-6 yıl sonra, daha yeni geçen yıl kar etmeye başlamıştır. Güçlü bir teknik altyapı gerektiren bu gibi İnternet platformlarının oluşturulmasına devlet yardımcı olmalıdır. Nitekim, ABD zamanında “melek sermaye” diye, aynı dönem içerisinde kurulan yüzlerce benzer firma içerisinde Facebook’u ve Google’ı destekleyerek büyümüştür. Bu firmalara devlet politikası olarak ilk kartopu oluşturulması aşamasında önemli destek sağlanmış; özellikle konvansiyonel medya kanalları ile tanınmalarına, yaygınlaşmalarına ve küresel güç olmalarına destek olunmuştur (Lütfi Güvener ile kişisel iletişim, 24.07.2013).

Benzer şekilde, Sarı’da gelecekte ekonomik gelişimin İnternet ile şekilleneceğini belirterek, Türkiye’nin “pazar mı? üretici mi?” olacağı sorusuna cevabın İnternetin

¹²⁷ Bu şirketlerin birçok ülkeden güvenlik belgesi alması ve vergi kaydı yaptırmasına rağmen, Türkiye’de irtibat bürosu açmaması, ciddi miktarlarda reklam geliri elde etmesine karşılık hiçbir vergi ödememesi eleştiri konusu olmaktadır. Örneğin, Google’ın Türkiye’den yıllık 100-200 milyon TL’lik reklam geliri olduğu tahmin edilmektedir (Ayaydın, 2010; Haberturk, 24.06.2010)

lkemizdeki geliřimine gre belireceđine vurgu yapmaktadır. Sarı’ya gre, toplumun İnterneti kullanma yeteneđi ve İnternetin lkemizdeki geliřimi ve zellikle yerli ieriklerin ve bunları sunacak yerli İnternet platformlarının geliřtirilmesi hayati nem tařımaktadır. Bu yzden, bugn iin “araba motoru”nu deđil “arama motoru”nu kimin yapacađı, Facebook gibi ierik platformlarını kimin ortaya ıkartacađı konusu en kritik tartıřma mevzusu haline gelmiřtir. Biliřim sektrne ciddi yatırım yapılması gerekmektedir. Sadece eriřim sađlayıcıların deđil, ierik sađlayıcıların da teřvik edilmesi lazımdır. Biz kendi ierik sađlayıcılarımızı geliřtiremezsek vatandařlarımız kresel platformların dijital kleleri olmaya devam edeceklerdir (Mehmet Sarı ile kiřisel iletiřim, 24.07.2013).

Bayzan da bu tr byk İnternet platformlarının kresel gce dnřtkten sonra lkelerine sađladıkları ekonomik, sosyal ve kltrel katma deđere ve kendilerini byten devlet tarafından veri alma řekliyle ulusal gvenlik vb. konularda kullanıldıđına dikkat ekmektedir. Bu nedenle benzer yerli platformların geliřtirilmesi iin devletin zel sektrn oluřturduđu projelere destek olması gerektiđini dile getirmektedir (řahin Bayzan ile kiřisel iletiřim, 24.07.2013).

Keza, řen ve Gvener’e gre, İnternetin geleceđindeki en kritik konulardan birisi “arama motorları” olacaktır. Zira, İnterneti sınırsız bir zgrlk alanı gryoruz fakat gerekte sınırları var ve bu sınırları arama motorları belirliyor. Aslında sınırsız bir İnternete eriřmiyoruz; ierik sunanların, arama motorlarının tercihlerine gre oluřturulmuř İnternete ulařıyoruz. Her aradıđını bulursun diyoruz ama aslında her aradıđımızı deđil Google’nin bize sunduđunu buluyoruz. nk, arama motorları kendi ierisindeki algoritmasını dizayn ederken bunu, kendi tercihiine gre n plana gelmesini istediđi ieriklere gre oluřturabilir. Dolayısıyla en basit konulardan en kritik konulara kadar her hususta ve zellikle nemli krizlerde insanları farklı řekilde ynlendirilebilme imkanları bulunmaktadır. rneđin, “Ermeni meselesi”nde arama motoru sahibi firma kendi anlayıřına gre Ermeni tezlerini konuyla ilgili arama yapıldıđında ncelikle kullanıcının nne getirebilir. Bu tr sakıncalarına rađmen, alternatif oluřturulmadıđı srece mevcuda mahkum olmaya devam edilecektir. Gvener’e gre ilgin olan ise, devletlerin tercihlerine gre řekillendirilmiř İnternete

karşı çıkanların, küresel şirketlerin tercihlerine göre şekillendirdikleri İnternete karşı aynı dozda tepki vermemeleridir (Osman N. Şen ile kişisel iletişim, 06.08.2013; Lütfi Güvener ile kişisel iletişim, 24.07.2013).

Keza, Söyler de bu kapsamda, yaptığı çalışmalarda “İnternet üzerinden ulus inşası” olarak nitelenen ilginç bir olguyla karşılaştığını dile getirmektedir. Bu çerçevede Almanya’da yaşayan Kürtlere ait İnternet siteleri üzerine yapılmış birçok çalışmaya ve yayına rastladığını; bu yayınlarda, söz konusu sitelerde ortak bayrak, ortak söylem, ulusal kahramanlar, ortak kültür propagandası yapılarak ulusallaşma sürecine yaptıkları önemli katkılardan bahsedildiğini aktarmaktadır. Söyler, benzer şekilde İnternetin ülkelerdeki iktidarları belli ölçüde belirleyebilme gücü bakımından, Arap baharında yaşanan süreci ve son dönemde Mısır’da gerçekleştirilen askeri darbe öncesi yapılan gösterileri de hatırlatmaktadır (Yasin Söyler ile kişisel iletişim, 01.08.2013).

Görüldüğü gibi, İnternetin tüm bu boyutları ile ele alınarak oluşturulacak bütüncül bir İnternet politikası çerçevesinde içerik düzenlemesi konusunun değerlendirilerek konuyla ilgili yeni bir yol haritasının ortaya çıkartılması gerekmektedir.

3.3.3.9 İçerik Düzenlemesi Ölçütleri ve Türkiye Uygulaması

Türkiye’nin içerik düzenlemesi uygulamalarını, içerik düzenlemelerinin meşruiyetini normatif olarak değerlendirmede kullanılan Bambauer’in açıklık, şeffaflık, kısıtlılık ve sorumluluk olarak belirlediği ölçütler bağlamında değerlendirilmesi faydalı olacaktır. Böylece, Türkiye örneğine ilişkin analitik bir analiz yapılmış ve nesnel sonuçlara ulaşılmış olacaktır.

Bambauer’in ilk ölçütü olan “açıklık”, bir devletin İnternete kısıtlama uyguladığını kabul edip etmediğini ve bu engellemenin gerekçesini açıkça belirtip belirtmediğini incelemektedir. Bu açıdan bakıldığında Türkiye uygulamasının oldukça “açık” olduğu görülmektedir. Türkiye, İnternet içeriğine müdahalede bulunduğunu, uyar-kaldır sistemini uyguladığını, erişim engellemesi ve filtreleme yaptığını ve bu müdahalelerin ve engellemelerin gerekçelerini açıkça beyan etmektedir. Çünkü,

yürürlükte olan içerik düzenlemesine özgü 5651 sayılı Yasa, çocukların, gençlerin ve ailenin korunması için bu hususların hepsini detaylı olarak düzenlemiştir.

Nitekim, bu amaçla kurulan TİB İnternet Dairesi, Yasa’da öngörülen usul ve esaslara göre, Yasa koyucunun gerekçelerini de gözönünde bulundurarak, sadece bu yasadışı içerik türleri ile sınırlı kalmak üzere uyar-kaldır yöntemi ile veya fiilen erişim engellemesi uygulayarak içeriğe müdahalede bulunmaktadır. Değişik gerekçelerle, engellemelere ilişkin sayıları ve engellenen sitelerin listelerini yayınlamasa da TİB, bu durumu oransal istatistikler yayınlayarak, resmi İnternet sitesinde duyuru yaparak, faaliyet raporlarında veya basın toplantıları ile açıkça deklare etmektedir. Ayrıca, engellenmiş bir siteye erişmek isteyen kullanıcıların karşlarına, bu siteye erişimin engellendiğini bildiren bir “engellenmiş sayfa” uyarısı yayınlayarak da TİB, bu konudaki açık tavrını ortaya koymaktadır.

Yani, Türkiye, uyar-kaldır, İnternet filtreleme ve erişim engelleme karar ve uygulamalarının varlığını kabul etmekte ve bu kısıtlamalara ilişkin gerekçelerini açıklamakta ve savunmaktadır. Dolayısıyla, Bambauer’in meşruiyet analizinde gerekli gördüğü ilk ölçüt olan “açıklık” bakımından Türkiye geçer not alabilir.

Bambauer’in analizinde ikinci ölçüt olarak kullanılan “şeffaflık”, engelleme uygulayan devletin, hangi tür içeriklerin engellendiği konusunda yeterince açık olup olmadığını ve engellemeyi belirleyen kriterlerin ne kadar belirgin olduğunu test etmektedir. Keza, engellenen içeriklerin tipleri ve kategorileri ile engelleme kriterleri ne kadar şeffaf ise uygulamaların meşruluğu o kadar yüksek olacaktır.

Bu ölçüt açısından da Türkiye’nin genel olarak iyi durumda olduğu iddia edilebilir. Özellikle, engellenen içeriklerin tipleri ve kategorilerinin netliği ve şeffaflığı açısından önemli bir sorun gözükmemektedir. Çünkü, ülkemizde İnternet içeriğine müdahalenin dayanağını ve sınırlarını oluşturan 5651 sayılı Yasa, sadece belirli sayıdaki katalog suçlarına ait içerikleri yasadışı olarak kabul etmiş ve bunları sayma yöntemi ile belirlemiştir. Burada, 5651 sayılı Yasa dışında mahkeme kararları ile İSS’lara uygulatılan değişik suç türlerine ait erişim engellemeleri fotoğrafı biraz

flulaştırmaktadır. Fakat, bunlar da genellikle telif hakları ihlalleri, dolandırıcılık, hakaret, iftira vs. gibi özel hukuk alanı içerisine giren türden ve daha ziyade bilişim suçları kapsamında değerlendirilebilecek konuları içerdiği için doğrudan içerik düzenlemesi bağlamında ele alınamayacağından değerlendirmede ihmal edilebilirler. Bunun dışında, fotoğraf açık ve nettir; Türkiye’de sadece belirli tip ve kategorideki sayılı içeriklere ilişkin erişim engellemesi uygulanmaktadır.

“Şeffaflık” ölçütünün ikinci kısmını oluşturan “engelleme kriterlerinin şeffaflığı” konusunda ise, kısmi olarak bir sorunun varlığından bahsedilebilir. Çünkü, Türkiye’de erişim engelleme kararlarının yargı tarafından verilen kısmında bir sorun olmamakla birlikte, TİB’nin re’sen verdiği erişim engelleme kararlarında kullandığı kriterlerin tam olarak açıklanmadığı ve bilinmediğiyle ilgili bir eleştiri söz konusudur. Nitekim, son dönemde uygulamaya geçirilen “Güvenli İnternet Hizmeti” ile ilgili olarak en çok eleştirilen konulardan birisinin, çocuk ve aile profiline dahil edilen veya edilmeyen içeriklerin hangi kriterlere göre belirlendiğinin açık ve şeffaf olmadığı noktasında düğümlendiği görülmektedir.

Lakin, TİB’in re’sen verdiği erişimi engelleme kararlarında söz konusu içeriklerin katalog suçu kapsamında olup olmadığı konusunda hiçbir kriter gözetmediğini veya kendisini bağlayacak hiçbir açıklanmış kriterinin olmadığını iddia etmek de doğru olmayacaktır. Nitekim, daha önce bahsedildiği gibi TİB, erişim engellemesi uygulamasının nasıl yapıldığını anlattığı İnternet sitesinde; içeriklerin Başkanlık bünyesinde çalışan hukukçular tarafından değerlendirmeye tabi tutulduğunu ve Türkiye’den erişim yoğunluğu ve özellikle çocukların doğrudan ulaşp ulaşamaması gibi kriterler de gözönünde bulundurarak karar verildiğini açıklamaktadır.

Bu noktada ilginç olan bir husus da, TİB’in bu tavrının birçok demokratik Avrupa ülkesinin filtreleme uygulamalarından daha ilerde bir şeffaflık içerisinde olduğunun görülmesidir. Ülke uygulamalarında da görüldüğü gibi, AB ülkelerinden birçoğu filtrelemeye konu kara listelerini hangi kriterlere göre oluşturduklarını açıklamadıkları gibi, bu listeyi belirleyenlerin genellikle emniyet mensupları veya içerisinde hukukçu bulunmayan ihbar merkezi görevlileri olduğuna rastlanılmaktadır.

Örneğin, İngiltere’de, ülkenin ünlü ihbar merkezi IWF’nin bünyesinde hiçbir hukukçu bulunmamasına rağmen, çocuk pornografisi yanında ırkçılıkla ve extreme pornografik içerikle mücadele etmek amacıyla oluşturduğu kara listeler, İngiltere’deki tüm İSS’lere, mobil operatörlere, arama motorlarına gönderilmekte ve bunlar tarafından “zorunlu gönüllü” olarak kullanılmakta ve erişimleri engellenmektedir. Keza, İnternet kullanıcılarına, bloke edilen içeriğe ilişkin herhangi bir bilgilendirilmede bulunulmamakta, bloke edilen sayfada sistem, “sayfa bulunamadı” uyarısını vermektedir. Yine, Almanya’da Federal Kriminal Polis Ofisi ile İSS’lar arasında gönüllü olarak yapılan sözleşme ile, Polis Ofisi’nin pornografi, şiddet ve neo-Nazi içerikli İnternet sitelerinden oluşturduğu kara listeye erişim engellenmektedir. Ancak sistemin şeffaf olmaması ve listede yer alan sitelerin halka açıklanmaması eleştirilmiştir.

Diğer yandan, erişimlerine karar verilecek olan katalog suçlarına ait içerikleri tanımlamaya yarayacak kriterlerin açık ve belirli olması açısından, Türkiye uygulamasının avantajlı olduğunu hatırlatmak gerekmektedir. Çalışmamızdaki katalog suçlarının temelini oluşturan suç türlerinin incelendiği kısma bakılacak olursa, gerek TCK’dan alınan gerekse Atatürk aleyhine işlenen suç türlerinin eskiye dayandığı ve zengin bir uygulama arka planına sahip oldukları görülmektedir. Yani, bu suç türleri tanımlanma, yorumlanma ve yerleşik içtihatlar oluşturma bakımından önemli bir birikime sahiptirler. Dolayısıyla, gerek adli makamlar, gerekse TİB’nda içerik değerlendirmesi yapan hukukçular bakımından, söz konusu suç türleri ile ilgili kriterler büyük oranda belirli ve şeffaftır. Bu noktada uygulayıcılar açısından belki de yapılması gereken, ürkmeden ve çekinmeden bu kriterleri açıklamak ve bu kriterlerle kendilerini bağladıklarını deklare etmektir.

Konuyla ilgili dikkat çekilmesi gereken diğer bir konu ise, bu suç türlerinin İnternet ortamında işlenip işlenmediğinin tespitinde, İnternetin kendine özgü yapısı ve teknik özellikleri nedeniyle mevcut kriterlerin yetersiz kalabilmesidir. Bu durumda bazı yeni kriterlerin oluşturulması veya eskilerin revize edilmesi gerekebilmektedir. Türkiye’de bu kapsamda bir sorunun yaşandığı veya yaşanabileceği öngörülebilir.

Görüldüğü gibi Türkiye, İnternet filtreleme ve erişim engellemeye konu suç tipi ve kategorilerinin şeffaflığı açısından sorunsuz gözükmeyle birlikte, engellenen içeriği tanımlamak için kullanılan kriterlerin şeffaflığı açısından, özellikle TİB'nin re'sen verdiği kararlar bakımından, kısmen eleştirilebilir uygulamalara sahiptir. Dolayısıyla, Bambauer'in meşruiyet analizinde gerekli gördüğü ikinci ölçüt olan “şeffaflık” açısından Türkiye'nin “sorumlu geçtiği” söylenebilir. Bu iki ölçütü birleştirerek bir analiz yaparsak, Türkiye çocukların, gençlerin ve ailenin korunması için sınırlı sayıda ve belirli türdeki içerikleri “açıkça” ve “şeffaf” bir şekilde yasadışı olarak kabul etmekte ve bu tür içeriğin engellenmesi için mücadele verdiğini beyan etmektedir; keza, beyan ettiği engelleme gerekçeleriyle kabul ettiği suç türleri arasında büyük oranda bir uyum gözükmektedir, fakat engellenen içerikleri tanımlamak için kullandığı kriterleri tam olarak açıklamamaktadır.

Bambauer'in analizinde üçüncü ölçüt olarak kullanılan “kısıtlılık” ile test edilen husus, devletlerin engellemeye ilişkin iddiaları ile yaptıkları arasındaki uyum ve uygunluktur. Yani, “kısıtlılık” ölçütünde, engelleme uygulamalarının engellemeye ilişkin beyanlarda belirtilen sınırlar içerisinde yapılıp yapılmadığı, uygulamaların dar veya geniş kapsamlı olup olmadığı incelenmektedir.

Bu ölçüt bakımından incelendiğinde Türkiye uygulaması değişken sonuçlar vermektedir. Ülkemizde, erişim engellemesi uygulamalarının bir kısmının “kısıtlılık” ölçütünden başarıyla geçebileceği görülmektedir. Lakin, bazen engellemelerin teknik sınırlılıklar nedeniyle kastın ötesinde ve aşırı sayılabilecek şekilde gerçekleştiğine tanık olunabildiği gibi, bazen de uygulamaların engelleme iddiasındaki içerik türlerini yeterince engellemediğine ve dolayısıyla dar kapsamlı kaldığına da rastlanılmaktadır. Bu nedenle, ilk izlenim; her iki yönlü sapmalar nedeniyle Türkiye'nin bu kriter açısından durumunun pek iyi gözükmediği yönündedir.

Fakat, konunun biraz detayına girildiğinde bu ilk izlenimin yanıltıcı olduğu görülmektedir. Birincisi, Türkiye yasadışı içeriğin engellenmesinde genel prensip olarak önceliği “uyar-kaldır” mekanizmasının işletilmesine vermiş gözükmektedir. Buradan bir sonuç alamaz ise, engelleme yoluna gitmektedir. İkincisi, engelleme

yöntemi olarak IP veya alan adı üzerinden engelleme yapılması, tüm diğer ülkelerde olduğu gibi Türkiye’de de kastın üzerinde ve aşırı engellemeye neden olmaktadır. Engellenen IP veya alan adı üzerindeki bir veya birkaç yasadışı içerik yüzünden diğer yasal içeriklerin de engellenmesi bu haksız durumu ortaya çıkarmaktadır. Bu durum TİB’nın da açıkladığı gibi, Başkanlığın da rahatsız olduğu ve istemediği bir sonuçtur. Lakin, mevcut teknik altyapı ancak bu yöntemlerin uygulanmasına imkan vermektedir ve bu sakıncanın giderilmesi için önerilen URL’den engelleme yöntemi dünyada da çok yaygın kullanım alanı bulabilmiş değildir. Çünkü, bu yöntemin hatırı sayılır ekonomik maliyeti ve teknik olarak bir takım handikapları bulunmaktadır.

Üçüncü konu ise, Türkiye’nin yasadışı içerik ile mücadelede yetersiz kaldığına, engelleme iddiasındaki içerik türlerini yeterince engellemediğine ve dolayısıyla engellemelerin dar kapsamlı kaldığına ilişkin detaylardır. Bu iddia bir bakıma doğru gözükmektedir. Örneğin, Türkiye’nin yasadışı olarak belirlediği pornografik içeriğe ülkeden halen kolaylıkla erişim sağlanabilmektedir. Nitekim, Türkiye’deki İnternet kullanıcıları Google üzerinden basit bir arama yaparak rahatlıkla bu tür içeriklere ulaşabilmektedir. Dolayısıyla, Türkiye’nin İnternet ortamındaki pornografik içerikle mücadelesinin yetersiz olduğu iddia edilebilir.

Fakat, bir süredir kullanıma sunulan “Güvenli İnternet Hizmeti” bu konuya bir çözüm bulmuş gibidir. İsteğe bağlı olarak aile veya çocuk profilini tercih edenler, pornografik içerik de dahil olmak üzere diğer yasadışı içeriklerden de arındırılmış bir İnternet hizmetini ücretsiz olarak alabilmektedir. Ancak, bu hizmetten faydalanabilmek için önce konudan haberdar olmaları, sonra ise ilave bir çaba ile hizmet aldıkları işletmecilere başvuruda bulunmaları gerekmektedir. Yani, bu duruma göre “ana veya temel hizmet”, içerisinde katalog suçlarına ait içeriklerinde bulunduğu serbest profil, “tercihli veya isteğe bağlı hizmet”, içerisinden yasadışı içeriklerin ayıklandığı aile ve çocuk profilleri olmaktadır.

Bambauer’in “kısıtlılık” ölçütüne göre, bu durum meşruiyet açısından sorunludur. Çünkü, Türkiye, çocukların, gençlerin ve ailenin korunması gerekçesiyle katalog suçlarına ait içeriklerin yasadışı olduğunu ve bunlara engelleme uygulayacağını

beyan etti ise; uygulamada bunun gereğini yerine getirmelidir ki iddialarının geçerliliği ve dolayısıyla uygulamalarının meşruiyeti olsun. Keza, meşruiyetin sağlanması için uygulamaların ne dar ne de geniş kapsamlı olmaması, beyan ve iddialarla uyumlu olması gerekmektedir. Aksi halde, bu durum Türkiye'nin erişimi kısıtlama için geliştirdiği ve beyan ettiği gerekçelendirmeye temelden zarar verecek; engelleme karar ve çabalarının doğruluğu, inanırlılığı ve ciddiyeti konusunda şüpheler uyandıracak ve engelleme sistemi üzerinde güvensizlik oluşturacaktır.

Dolayısıyla, Türkiye'nin bu durum ile karşılaşmaması için “Güvenli İnternet Hizmeti”ni sunarken, erişim engellemeye ilişkin beyan ve iddialarının gereği olarak, içerisinden yasadışı içeriklerin ayıklandığı bir profili (bu aile veya yeni oluşturulacak bir profil olabilir) “ana veya temel hizmet” olarak belirlemesi ve isteğe bağlı olmaksızın tüm kullanıcılara bunnu sunması daha doğru olacaktır. Bu sağlandıktan sonra, “tercihli veya isteğe bağlı hizmet” olarak çeşitli profiller (yetişkin, çocuk, kamu gibi), başvuruya bağlı olarak kullanıcıların hizmetine sunulabilir.

“Kısıtlılık” ölçütü bakımından Türkiye’de dikkate alınması gereken hususlardan birisi de, erişim engellemesi uygulamasının merkezinde bulunan TİB üzerindeki kamuoyu baskısıdır. TİB, kurulduğu günden bu yana üstlendiği görevler ve uygulamaları bakımından sürekli olarak eleştirilerin ve tartışmaların odağında yer almış bir kurumdur. Önce, “telekulak” ve “yasadışı dinlemeler”, İnternet Dairesi kurulduktan sonra ise, “site kapatmalar” ve “sansür” konularındaki tartışmalar ve eleştirilerde TİB hep hedefte olmuştur. Dolayısıyla TİB, tedirgin ve gerilimli bir atmosferde görevlerini ifa etmeye çalışmaktadır.

Nitekim, TİB, erişim engellemeye ilişkin uygulamalarında sürekli eleştirilmektedir. Bir kesim TİB’ni İnternete sansür uygulamakla itham ederken, bir kesim de sakıncalı içerikle mücadelede yetersiz kaldığı gerekçesiyle eleştirmektedir. Özellikle, Başkanlığı “sansürcülük” ile itham eden ve içlerinde uluslararası bazı kuruluşlarında bulunduğu belli bir kesim yaptığı yayınlar, düzenlediği kampanyalar, protesto gösterileri ve açtıkları davalar ile bilerek veya bilmeyerek TİB üzerinde sosyal ve psikolojik baskı oluşturmaktadır.

Doğal olarak TİB ve BTK'nın bu iklimden etkilenmesi mümkündür. Dolayısıyla, bu iklim, Kurumları içerik düzenleme ve özellikle erişim engellemeye ilişkin karar ve uygulamalarında azami ölçüde ihtiyatlı ve temkinli olmaya, şimşekleri üzerine çekmeme konusunda dikkatli davranmaya itebilmektedir. Bu nedenle TİB'nın erişim engellemeye ilişkin bazı karar ve uygulamalarında engellemeyi en aza indirecek ve dar kapsamda tutacak seçenekleri tercih etmesi mümkündür.

Sonuç olarak, Bambauer'in "kısıtlılık" ölçütüne göre Türkiye, açıkladığı yasadışı içerik türlerine karşı uyguladığı erişim engellemelerinin kapsamını bazen istemese ve kastı o olmasa da teknik sınırlılıklardan dolayı geniş turarken, bazen de gelebilecek tepkiler nedeniyle dar tutabilmektedir. Fakat, bu sapmalar mercek altına alındığında, kısmen anlaşılabilir ve makul gerekçelere sahip oldukları görülmektedir. Diğer yandan, "kısıtlılık" ölçütü ile ortaya çıkartılmaya çalışılan hususun, söz konusu sapmaların ifade özgürlüğü ve bilgiye erişim hakkı gibi alanlarda demokratik değerleri zedeleyecek sonuçlar doğurup doğurmadığının anlaşılması olduğunu kabul edersek, Türkiye uygulamasının bu konuda çok önemli soruna sahip olmadığını söyleyebiliriz. Nitekim, TİB'nın erişim engellemesi uygulamalarında, ilan edilen suç türlerine ait içerikler dışında kasıtlı olarak siyasi bir amaç gözetilerek gerçekleştirilen erişim engellemesi örneğine rastlanılmaması bu durumun bariz bir göstergesidir. Dolayısıyla, Türkiye uygulaması "kısıtlılık" ölçütü bakımından bazı erişim engellemeleri yönüyle görünürde geçer not alaması da, bu ölçüt ile test edilmek istenen konunun özü bakımından önemli bir soruna sahip gözükmemektedir.

Bambauer'in dördüncü ve son ölçütü olan "Sorumluluk" ile engelleme kararlarına katılım, yetki tanımlama, engellemeye karşı çıkma imkanı ve çoğunluğun tercihlerine aykırı sınırlama konuları test edilmektedir. Engelleme kararlarına katılım ile, vatandaşların ve kullanıcıların, engelleme karar ve uygulamalarına ilişkin talep ve görüşlerinin demokratik bir ortam içerisinde uygulamaları etkileyebilme düzeyi ölçülmektedir. Bu konuda en önemli ölçüt vatandaşların şikayetlerini alan ve değerlendiren ihbar merkezlerinin varlığıdır. Çünkü, bu merkezlerin, vatandaşların istek ve taleplerini en sağlıklı şekilde alma ve erişim engellemelerine ilişkin süreçlere katılım sağlama konusunda önemli bir mecra olduğu kabul edilmektedir.

Bu bakımdan Türkiye’de TİB Bilgi ve İhbar Merkezi’nin önemli bir işlev gördüğünü iddia edebiliriz. Çünkü, bu Merkez kısa bir sürede, her geçen yıl daha çok sayıda ihbar alarak dünyada en çok ihbar alan merkezlerden birisi haline gelmiştir. İhbar sayılarının artması aynı zamanda vatandaşın katılımının da artması anlamına geldiği için “sorumluluk” ölçütü açısından olumlu bir gösterge olarak değerlendirilmelidir.

“Sorumluluk” ölçütünün ikinci önemli yönünü ise, erişim engelleme sisteminde yer alan aktörlerin ve özellikle kamu kurum ve görevlilerinin yetki ve sorumluluklarının açıkça belirtilmesi oluşturmaktadır. Bu konu, engelleme uygulamalarının hukuki ve siyasi denetiminin yapılmasını sağlama açısından önemlidir. Bu yönüyle ülkemizin genel olarak iyi bir noktada olduğunu söyleyebiliriz. Çünkü, 5651 sayılı Kanun ve ikincil düzenlemeler, Türkiye’de engellemelere ilişkin usul ve esasları, uygulanacak sistemi, TİB’nin ve kamu görevlilerinin görev ve yetkilerini en ince ayrıntılarına kadar belirlemektedir. Dolayısıyla uygulamaya ilişkin olarak sorumlulukların belirlenmesi konusunda müphem kalan herhangi bir husus göze çarpmamaktadır. Bu nedenle, “sorumluluk” ölçütünün bu ikinci yönü açısından sorun bulunmamaktadır.

“Sorumluluk” ölçütünün üçüncü önemli yönü ise, erişim engelleme kararlarına itiraz yolunun açık olmasıyla ilgilidir. Nitekim, demokratik ülkelerin çoğu bağımsız mahkemeler aracılığıyla bu olanağı sağlamaktadır. Türkiye uygulamasında bu açıdan da önemli bir sorun gözükmemektedir. Çünkü, 5651 sayılı Yasa’ya göre, erişim engellemesine ilişkin kararı verecek mercilerin birisi yargı organlarıdır. Diğer yandan, bu konuda en çok eleştirilen TİB’nin re’sen verdiği erişim engelleme kararlarının idari işlem olduğu için yargı denetimine tabi olduğu da açıktır. Bu açıdan “sorumluluk” ölçütünün bu üçüncü yönüyle ilgili de bir sorun gözükmemektedir.

“Sorumluluk” ölçütünün dördüncü önemli yönü ise, erişim engelleme uygulamalarında azınlığın korunması ve çoğunluk tercihlerine karşı kısıtlamaların varlığıdır. Burada özellikle söz konusu edilen uygulamalar, azınlığın korunması ve ayrımcılığın önüne geçilmesine ilişkin olarak, azınlıklara ilişkin içeriklerin sansüre uğramamasıdır. Bu bakımdan Türkiye’nin notunun iyi olduğu söylenebilir. Nitekim, ülkemizde erişim engellemelerine konu içerikler içerisinde siyasi değerlendirmelerle

veya ayrımcılık saiki ile azınlıklara ait web sitelerinin engellendiğine ilişkin herhangi bir şikayet mevzuu olmamıştır.

Dolayısıyla, “sorumluluk” ölçütü bakımından değerlendirildiğinde Türkiye’nin erişim engelleme uygulamalarında önemli bir soruna rastlanmayacağını ifade edebiliriz. Keza, Bambauer’in ölçütlerine dayalı meşruiyet analizini Türkiye örneği üzerinden yaptığımızda ve sonuçları bir bütün olarak değerlendirdiğimizde; “kısıtlılık” ölçütünün kullanılmasıyla beliren olumsuz sonuçlar dışında erişim engellemesi uygulamalarımız açısından genel olarak önemli bir sorun gözükmemektedir. Dolayısıyla, Türkiye’deki erişim engellemesi uygulamalarının “kısıtlılık” konusu dışında ciddi bir meşruiyet sorununun olmadığı söylenebilir.

Sonuç olarak, 5651 sayılı Yasa’nın ve TİB uygulamalarının eleştirilebilecek bazı yönleri bulunmakla birlikte, dünya uygulamalarıyla karşılaştırıldığında olumlu birçok yönün bulunduğu görülmektedir. Dünyada birçok ülkede İnternet için özel bir düzenlemenin eksikliği devam ederken, kanunilik ilkesine uygun olarak Türkiye’de konuya özel yasa ve yönetmelikler ile İnternet aktörleri tanımlanmış, sorumlulukları netleştirilmiş ve içerik çıkarma “uyar-kaldır”, erişim engelleme usul ve esasları belirlenmiştir. Böylece, Anayasa’da yer alan temel hak ve özgürlüklere ait sınırlamaların yasa ile yapılması gerektiğine ilişkin uluslararası ilkeye uygunluğun ülkemiz adına sağlanmış olduğu söylenebilir (Berber ve Kaya, 2010: 16-17).

Keza, engellemeye ilişkin suç türleri sınırlı ve belirli hale getirilmiş; kamu düzeni ve genel ahlakın korunması, ulusal güvenlik ve kamu yararı gibi muğlak, geniş ve keyfî uygulamalara yol açacak genel engelleme sebepleri kapsam dışı tutulmuştur. Yine, demokratik Avrupa ülkelerinde dahi çokça örneklerine rastlanan, hangi içeriğe müdahale edileceği tamamen idari makamların yetkisine bırakmış uygulamalarla yürütülen şeffaf olmayan İnternet içerik politikalarına karşılık, 5651 sayılı Yasa ile daha demokratik ve şeffaf bir yaklaşım sergilenmiştir (Berber ve Kaya, 2010: 16-17).

Söyler de buradan hareketle Türkiye’nin İnternet düzenlemelerinin antidemokratik olmadığını, hatta birçok Avrupa ülkesinden ve ABD’den daha iyi durumda olduğunu

belirtmektedir. Bu ülkelerde içerikle ilgili işler herhangi bir düzenleme olmaksızın yapılıyor iken, Türkiye’de konunun 5651 sayılı Yasa ile hukuki güvenceye kavuşturulduğuna dikkat çekmektedir (Yasin Söyler ile kişisel iletişim, 01.08.2013).

Bu çerçevede, 5651 sayılı Yasa ve bu Yasa’nın uygulayıcısı olan TİB, süreç içerisinde bazı uygulamalarından dolayı eleştirilse de, içerik düzenlemeleri açısından Türkiye’nin attığı bu adım genel olarak olumlu görülmelidir. Zaman içerisinde bu Yasa’nın, uygulamadaki aksaklıklar göz önünde bulundurularak revize edilmesi mümkün ve gerekli olacaktır. Nitekim, süreç içerisinde bu Yasa’yla ilgili olarak kamu kurumları, STK’ları, sektör firmaları tarafından bir çok değişiklik çalışması, talebi ve teklifi yapılmış ve yapılmaktadır. Bu kapsamda, 2008 yılında Abant’ta, daha sonra 2010 yılında Kartepe’de çalıştaylar düzenlenmiş ve sonrasında erişim engellemelerle ilgili kriterler deklare edilmiştir.¹²⁸ Son olarak ise, İnternet Geliştirme Kurulu ve O’nun altındaki bazı çalışma grupları aynı konularla ilgili değerlendirme ve önerileri alarak, bu Yasa’da yapılması istenilen değişikliklerle ilgili bir taslak oluşturmuştur (İnternet Kurulu, 2010). Tüm bu çalışmalarda dile getirilen öneri ve görüşler Kurul’un İnternet sitesinde yayınlanmaktadır (İnternet Kurulu, 2013).

Türkiye’de bugüne kadar erişimi engellenmiş site sayısının 30 bin civarında olduğu tahmin edilmektedir (Engelliweb, 2013a). İnternet ortamında 252 milyon alan adı ve 717 milyon web sitesi bulunduğu (Verisigninc, 2013: 2; Netcraft, 2013) ve bunların %30’una yakınının pornografik içerik olduğu hatırlanırsa (OpteNet, 2010a), TİB’nin erişim engelleme politikası hakkında önemli bir ipucu elde edilmiş olacaktır. Bu tablo, erişim engellemeleri konusunda TİB’na yöneltilen yoğun “sansür” eleştirilerinin büyük oranda haksız olduğunu ortaya koymaktadır.

Freedom House adlı insiyatifin, BM Demokrasi Fonu için hazırladığı “İnternette Özgürlük 2011” adlı rapora göre Türkiye, İnternet kullanımını “kısmen özgür” bırakan ülkeler arasında sayılmıştır (Freedom House, 2011). Keza, OpenNet’in

¹²⁸ 18-19.06. 2008’de Abant’ta “5651 Kapsamındaki ve Dışındaki Site Erişime Kapatmaları Çalıştayı” düzenlenmiştir. Çalıştay dökümanları için bkz. <http://5651calistay.org/2008-abant/>; 20-22.04.2010’da Kocaeli-Kartepe de “İnternet İçerik Düzenleme Çalıştayı” yapılmıştır. Kartepe Kriterleri Sonuç Bildirgesi için bkz. <http://5651calistay.org/2010/04/22/kartepe-kriterleri-yayinlandi/> (08.12.2012)

dünyadaki İnternet sansürleriyle ilgili yayınladığı 2011 yılı raporuna göre Türkiye orta seviyede sansür uygulayan ülkeler sınıfında yer almıştır (Aru, 2012b).

Çin, İran, Suriye, Kuzey Kore gibi ülkelerde ise İnternet trafik çıkışı üzerinde devlet tarafından sansür kapsamında katı uygulamalar bulunmaktadır. Türkiye erişim engellemeler konusunda tam anlamıyla iki tarafta da bulunmamaktadır. Engelleme işleminin devlet tarafından yapılmasıyla Avrupa’dan, İnternete yaklaşım açısında Çin, İran, Suriye gibi ülkelere farklılaşmaktadır. Başka bir ifadeyle sui generis (kendine özgü) bir uygulama söz konusudur (Hürriyet, 09.02.2008).

Tezin onaltıncı alt hipotezi çerçevesinde Türkiye’nin İnternet içerik düzenleme politikaları ve uygulamaları bir bütün olarak değerlendirildiğinde, eleştirilebilecek bazı eksik yönleri bulunsada, Türkiye örneğinin, dünyada neredeyse bir benzeri bulunmayan kendine özgü karakteri ortaya çıkmaktadır. Türkiye çocukların, gençlerin ve ailelerin katalog suçları olarak belirlenmiş yasadışı ve zararlı İnternet içeriklerinden korunması için devlet eli ile mücadele etmektedir. Bu mücadelenin kuralları, kapsamı, yöntemi, uygulama şekli ve örgütsel yapısı, doğru ve yanlışlarıyla, büyük oranda ülkemize has özelliklere sahiptir. Bu yönüyle, Türkiye, ilginç ve örnek bir uygulama geliştirmektedir.

Çalışmanın bundan sonrasında “Genel Değerlendirme”, “Sonuç” ve “Öneriler” bölümlerine yer verilmiştir. Bu çerçevede, önce çalışmanın bütünlüğü içinde toparlayıcı bir özet yapılmış ve son kez hipotezler bu bütünlük içinde “genel değerlendirme” başlığı altında kısaca değerlendirilmiştir. Daha sonra, tez içinde ele alınan tüm hipotezlere ilişkin ulaşılan sonuçlar kısa açıklamalar ile “Sonuç” başlığı altında belirtilmiştir.

Bu son kısımda, hipotezlerin “Genel değerlendirme” ve “Sonuç” başlıkları altındaki karşılıklarının takibini kolaylaştırmak için hipotez numaraları, söz konusu başlıkların altındaki metinlerin hipotezle ilgili olan bölümlerine de yazılmıştır. Son olarak ise, konuyla ilgili Türkiye örneğine yönelik politika ve uygulama önerileri, “Öneriler” başlığı altında kayıt altına alınmıştır.

GENEL DEĞERLENDİRME ¹²⁹

1. Masuda ve Drucker'in 1990'larda kavramsallaştırdığı “bilgi toplumu”, insanlığın teknolojik gelişim tarihine göre “saban-tarım toplumu” ve “buhar makinası-sanayi toplumu” aşamasından sonra ulaştığı toplum aşamasını ifade etmektedir. “Bilgi ve iletişim teknolojileri” ve özellikle İnternetin başrol oynadığı bilişim devrimi dünyayı “sanayi toplumu”ndan “bilgi toplumu” aşamasına taşımış, bu durum geleneksel toplumsal, ekonomik, siyasal ve kültürel yapıyı etkileyerek insanların hayatında köklü değişimlere ve dönüşümlere neden olmuştur.

Bu yeni dönemde, sanayi toplumunun ekonomik, sosyal, siyasal, kültürel ve felsefi yapısı, üretim ilişkileri, tüketim alışkanlıkları, örgütsel yapıları değişmiş, sermaye küreselleşmiş ve bu dönüşümler, fordist üretimden postfordist üretime, ulus-devletler dünyasından küreselleşmiş dünyaya, modernist düşünceden postmodernist düşünceye, refah devletinden özelleştirme anlayışına, geleneksel kamu yönetiminden yeni kamu yönetimi yaklaşımına, temsili demokrasiden katılımcı demokrasiye geçilmiştir. Tüm bu değişimler “paradigma değişimi” olarak da nitelenmektedir.

Bu değişimler yeni yönetsel ve hukuksal sorunlar ortaya çıkarmaktadır. Teknoloji çok hızlı geliştiği için çoğu zaman hukuk ve yönetim boyutu teknolojinin gerisinde kalmakta, bu da sorunları daha da büyötmektedir. Dolayısıyla İnternet ve İnternetin sembolize ettiği bilgi toplumu olgusu hem yeni kurum, kavram ve ilişkileriyle hem de beraberinde getirdiği sorun ve problemlerle birçok yeni tartışmanın odağı olmaktadır. İnternet içerik düzenlemesi konusu ve sorunu da bu tartışmaların alt başlıklarından birisini oluşturmaktadır.

2. Alaeddin Şenel'in ifade ettiği gibi; her toplum biçiminin dayandığı bir “geçim biçimi”, geliştirdiği bir “yaşam biçimi” ve yaşam biçimiyle uyumlu bir “düşün biçimi” ve bunlarla da uyumlu bir “yönetim biçimi” vardır. Dolayısıyla, sanayi devrimi, sanayi toplumunu ve ona uygun kamu yönetimi anlayışını ortaya

¹²⁹ Bu bölümde önceki bölümlerin genel bir toparlayıcı özeti ve değerlendirmesi yapıldığı için daha önce metin içinde ilgili yerlerde gösterilen kaynaklar burada tekrar gösterilmemiştir. Sadece, ilk defa kullanılan atıflar için kaynak gösterilmiştir.

çıkartırken, bilgi ve iletişim teknolojilerindeki gelişmeler de bilgi toplumunu ve ona uygun yönetim yapısını meydana getirmiştir. Zira, sanayi toplumunda hakim olan ulus-devlet eksenli merkeziyetçi ve hiyerarşik düzeni yansıtan bürokratik kamu yönetimi yapılanması yerini, bilgi toplumunda, merkeziyetçilikten uzaklaşan, yerelliği, yerinden yönetimi, yatay örgütlenmeyi ve esnek uzmanlaşmayı öngören görev örgütlenmelerini gündeme getirmiştir.

Bu süreçte bilgi toplumunda devletin rolü ve sınırlarının yeniden sorgulandığına, siyasal sınırların ve ulusal egemenlik anlayışının eski katılığını kaybettiğine, bölgesel ve uluslararası örgütlenmelerin önem kazandığına, küresel sermayenin çizdiği etkinlik alanı içinde mal ve hizmet, teknoloji ve bilgi akışının hızlandığına, bireysel tercihlerin ve alt kimliklerin önem kazandığı yeni devlet anlayışının geliştiğine tanık olunmuştur. Keza, bilgi toplumu devleti, “Hukuka bağlı demokratik devlet”, “adem-i merkeziyetçi devlet”, “katılımcı devlet”, “açık-şeffaf devlet”, kamu görevlilerinin istihdamında bilgi ve becerinin, uzmanlığın esas alındığı “meritokratik devlet”, “sınırlı-çerçeve devlet”, doğrudan ekonomik faaliyette bulunmak yerine piyasayı düzenleyen ve gözetici “hakem devlet” olarak ortaya çıkmıştır.

Örgütlerin bilgi ve iletişim teknolojilerinden giderek daha çok yararlanmaya başlamasıyla bilginin işlenme hızı, kullanabilirliği, kullanım alanları ve veri hacmi artmış; planlama, uygulama ve denetleme kapasitelerini büyük ölçüde geliştirmiştir. Yeni teknolojilerle, işyeri ve mesai kavramı geleneksel anlamını yitirmiş, hizmet yöntemleri değişmiş, kamu hizmetlerinin ucuz ve daha kolay sunulması mümkün hale gelmiş, vatandaşların siyasal katılım imkanları artmıştır. Diğer yandan, bilgi toplumunda gelişen İnternet, web teknolojileri ve e-posta gibi yeni araçların kullanımının artmasıyla birlikte vatandaş-devlet ilişkisi de yeni bir boyut kazanmış ve şeffaf, vatandaş odaklı, daha ucuz ve daha iyi çalışan bir idari yapı oluşturmak için kamu yönetiminin iyileştirilmesi çabalarına da çare olacağı ümidiyle, “e-devlet” kavramı ve uygulamaları hız kazanmıştır.

Varacağı son nokta ve etkileri hala tam olarak kestirilemeyen bilgi toplumu sürecinden kamu yönetimi de derinden etkilenmektedir. Bu süreçte, “yönetim”in

klasik, yöneten ve yönetilen varsayımına dayanan içeriği boşalırken; konuyla ilgili ve karardan etkilenen tüm aktörlerin “birlikte”, “beraber”, “ortaklaşa”, “işbirliği” içerisinde kendilerini yönetmesi anlayışı doğmuş ve “yönetişim” kavramı ortaya çıkmıştır. Artık bu yeni dönemde, tüm siyasal ve toplumsal süreç, ilişki ve kararlar devlet, yerel yönetimler, özel sektör, STK’ları, meslek örgütleri, gönüllü kuruluşlar ve üniversiteler gibi aktörler arasında beraberce düzenleme, yönlendirme, üretim ve yönetim temelinde yapılandırılmaktadır. Sonuçta, sanayi toplumunun “kamunun yönetilmesi” olarak yapılanan “kamu yönetimi” anlayışı, bilgi toplumunda “kamunun yönetmesi” biçiminde kavramsallaşıp kurumsallaşmaya başlamıştır.

Bu süreçte, devletin daha etkili ve verimli bir işleyişe kavuşturulması amacıyla “kamu yönetimi reformları” gündeme gelmiş ve devletin kamu hayatındaki müdahale ve etki alanının daraltılmasını temin etmek için kullanılan en önemli araçlardan birisi olan deregülasyon uygulamaları, öncelikle Batı Avrupa ve ABD’de, daha sonra da diğer ülkelerde yaygınlık kazanmıştır. 1980’lerden sonra hız kazanan bu eğilim, daha çok özelleştirme politikaları ile kendisini göstermiştir. Yeni devletin tüm özellikleri ile ortaya çıkması 1990’lardan sonra regülasyon politikaları ile olmuştur. Bu çerçevede, ABD’de önceden beri var olan “düzenleyici kurullar”, kamu yönetiminin işleyişine hız ve etkinlik kazandırmak ve daha önce icracı rolü kaldırılan devlete aktif düzenleyicilik işlevi verilmesi için öncelikle İngiltere gibi Batı Avrupa ülkelerinde ve bu ardından Türkiye’de faaliyete geçirilmiştir.

Böylece, “bilgi toplumu”, “devlet/kamu yönetimi”ni dönüştürürken, “devlet/kamu yönetimi”nin “bilgi toplumu” ile ortaya çıkan İnternet ve İnternet içeriğinin düzenlenmesi gibi sorunlara çözüm bulma, gelişen yeni yapı ve yaklaşımları kendisine uyarlama yönünde iki yönlü işleyen bir etkileşim süreci geliştirmiştir. Bu da İnternet içerik düzenlemesi konusunda özellikle “yönetişim” ve bu çerçevede “düzenleyici kurullar” olarak kendini gösteren yönetsel yaklaşım ortaya çıkarmıştır.

3. Bunun yanında bilgi toplumu kuramına ilişkin ciddi eleştiriler bulunmaktadır. İlk eleştiri, bilgi toplumu kuramcılarının dünyanın bilgi toplumu aşamasında olduğuna yönelik iddialarının aksine, dünyaya egemen durumda olan ülkelerin dışında büyük

çoğunluğun bilgi toplumu aşamasında olmadığı konusundadır. Buna göre, bilgi toplumu olmayı belirleyecek dönüşümler, tüm toplumlarda aynı oranda ve düzeyde işlememektedir. Bu nedenle toplumların belli bir bölümü, sanayi sonrası dönüşümleri etkin bir şekilde yaşarken, geri kalan büyük çoğunluk, tarım, sanayi ve ileri sanayi toplumu aşamalarını yaşamaktadır. Bunun yanında azgelişmiş ülkeler ile bilgi toplumu seviyesine ulaşmış ülkeler arasındaki farkın giderek arttığı da görülmektedir. Bu nedenlerle, ancak küreselleşme bağlamında ele alındığında dünyanın bilgi toplumu aşamasında olduğunun iddia edilebileceği belirtilmektedir.

İkinci eleştiri ise, toplumların farklı tarihsel ve yapısal özelliklere sahip oldukları, dolayısıyla; Batılı toplumların kendi tarihsel ve toplumsal dinamiklerinin sonucu olarak yaşadıkları tarım, sanayi ve bilgi toplumu aşamalarının ortaya çıkardığı dönüşümlerin tarih, kültür, değerler sistemi ve siyasal yapıları farklı diğer toplumlar için anlamları ve etkilerinin farklı olacağı konusundadır. Bu yüzden, bu tür hazır formül ve modellerin farklı toplumların dokusuna uyum sağlayamayarak sorun oluşturabileceği unutulmamalı ve bilgi toplumu aşamasında bulunmayan topluluklar “geri kalmışlık” telaşı içine sokularak, kültürel-ideolojik dayatmalar yapılmamalıdır.

Bilgi toplumu kuramıyla ilgili üçüncü eleştiri ise, bilgi toplumunun kapitalizmde gelinen son nokta olduğuna ilişkin değerlendirmedir. Buna göre, kapitalizm, dönemsel olarak ve şartlar gereği kendisini iktisadi, siyasi ve ideolojik yapılarda yeniden yapılandırmaktadır. Bilgi toplumu işte bu son yapılandırmanın adıdır. Keza, bilgi toplumu kavramsallaştırması, kapitalizmin içinde bulunduğu yeni kriz şartlarını aşmak için bilgi iletişim teknolojilerinin dönüştürücü potansiyelinin devreye sokulduğu yeni dönemi anlatmaktadır. Dolayısıyla bilgi toplumunu, yeni bir toplumsal dönem olarak değil, kapitalizmin krizini aşmak için bilgi iletişim teknolojilerinin desteğinde yeni politikaları ve uygulamaları uluslararası bir meşruluk şemsiyesi altında hayata geçirme eylemi olarak tanımlamak gerekmektedir.

Bu yaklaşıma göre, bilgi toplumu, küreselleşen dünya ekonomisi içerisinde gelişmiş toplumların ticari-ekonomik rekabet güçlerini artırma hedeflerine ulaşması için daha çok olanak sağlamasına yönelik bir politikayı ifade etmektedir. Bu durum, gelişmiş

ülkelere, merkezleri bu ülkelerde bulunan çokuluslu şirketlerin önünü açmaya yarayan politikaları oluşturma ve uygulamaya koyma olanağı sunarken, azgelişmiş ülkeleri ekonomik kalkınma sorununun “bilgi toplumu olmakla” aşılabileceği umuduyla küresel kapitalist sisteme eklemlenmeye itmektedir. Nitekim, bu dönemi Castells “Enformasyonel Kapitalizm” olarak tanımlamaktadır.

Bilgi toplumu kuramına yöneltilen bu eleştirilerin yanı sıra, bilgi toplumunun neden olduğu veya beraberinde getirdiği bazı önemli sorunlar ve riskler de bulunmaktadır. Bunlardan birisi ‘Gözetim Toplumu’ olma riskidir. Orwell’in “1984” benzeri bazı kitaplara da atıf yapılarak dillendirilen bu risk; teknolojik gelişmelerin, toplumları giderek bir izleme ve gözetleme toplumu olmaya doğru götürmesi yanında, kitle iletişim araçları ve teknolojinin yönlendirici etkisi ve özellikle İnternet aracılığıyla toplumu kolayca manipüle etmek ve sıkı bir denetim altına almak isteyenlerin olabileceği endişelerini de içine alan bir kavramdır.

Bilgi toplumu ile ilgili gündeme gelen ikinci bir sorun ise “sayısal uçurum/sayısal bölünme” konusudur. Bilgi ve iletişim teknolojileri alanında ülkeler arasındaki ve ülkeler içindeki eşitsizlik olgusu uzun zamandır tartışılmaktadır. “Bilgi yoksulları/bilgi zenginleri”, “iletişim sahipleri/iletişim yoksunları” gibi kavramlar bu nedenle kullanılmaktadır. BM, G8, OECD ve Dünya Bilgi Toplumu Zirvelerinde de en çok tartışılan bu konu, halen önemini ve güncelliğini korumaktadır.

Bilgi toplumu olmanın beraberinde getirdiği diğer bir sorun ise “Güvenlik korkusu” ya da “Risk toplumu” olma kaygısıdır. Gelişen teknolojinin varlığı, insanın kişisel bağımsızlığını, mahremiyetini ve güvenliğini tehdit eden riskleri de beraberinde getirmektedir. “Risk toplumu”, bilgi toplumunun bir özelliğidir ve artık tehlikenin kaynağı cehalet değil bilgidir. Bilim ve teknoloji sorunlara çözüm bulmaya çalışırken yeni sorun/risk alanları oluşturmaktadır. Teknoloji modern yaşamın karmaşıklığını azaltma konusunda kolaylıklar sağlarken, beraberinde ekolojik riskler, sosyal riskler (ailelerin dağılması, ferdiyetçilik, toplumsal yozlaşma, yalnızlık, çocuk istismarı, pornografi, fuhuş, intihar, kumar, şiddet, ayrımcılık, madde bağımlılığı, terör, açlık ve kıtlık, işsizlik, sosyal adaletsizlik vb.), teknolojik riskler (kitle imha silahları, siber

saldırıları, manyetik kirlenme, özel hayatın gizliliğine tecavüzler vb.), kültürel riskler (kültür emperyalizmi, yerli toplum ve değerlerin yok oluşu vb.) oluşturmaktadır.

Diğer yandan, bilgi toplumunda tüketimin sembol olduğu gerçeğinden hareket eden sosyal bilimciler, tüketim toplumu ve yabancılaşma sorununa dikkat çekmektedir. Tüketim toplumu ve tüketim kültürü sunduğu bütün araç ve kolaylıklarla, geçmişe göre çok daha ince ve etkin yöntemlerle bireyi cendereye almakta, tüketime dayalı yaşam biçimlerini satın almaya zorlayan yanlış ve sahte ihtiyaçlar üretmektedir. “Piyasa ekonomisi”, toplumu, sınırları her gün genişleyen biçimde tüketici yapmak için başta reklamlar olmak üzere çeşitli pazarlama teknikleriyle, üretilen ürünün alınması gerektiğine, onsuz yaşanamayacağına inandırmaya çalışmaktadır.

Diğer yandan, bilgi ve iletişim teknolojileri formel ilişkilerdeki kolaylığın yanında insanlar arası sosyal ilişkilerde azalma ve topluma yabancılaşma, toplumdan kopma gibi sakıncaları da beraberinde getirmektedir. Yüz yüze yürütülen insan ilişkileri yerini makine-insan ilişkisine, gerçek yaşam yerini sanal gerçeklik uygulamalarına bırakmaktadır. Zamanının büyük bölümünü bilgisayar karşısında geçiren insanların en belirgin yönü, içe kapanma ve kendini soyutlama, yalnızlık ve yabancılaşmadır. İnternette istediği gibi sörf yapma, arzu ettiği hiçbir şeye İnternetin itiraz etmemesi, kişilerde sanal bir sınırsız özgürlük hissi oluşturmakta; gerçekte kendi arzularının kölesi haline getirerek, sınırsız ve keyfi gücün tutsağı yapmaktadır.

Bilgi toplumu olmanın maliyetlerinden birisi de “bilgi kirliliği” ve “enformatik cehalet”tir. Postmodern toplum bilgi yoksunluğu tehlikesine karşı geleceği bilgi teknolojilerinde görürken, “bilgi fetişizmi” tehlikesi ile karşılaşmaktadır. Bilgi toplumunda kişiler bireysel bazda, aşırı bilgi yüklemesi yaşamakta, enformasyon denizinde boğulmama savaşı vermektedir. Çünkü, bilgi enflasyonu yaşanmakta, doğrulanmamış çok sayıda bilgi ile karşılaşmakta, adeta bilgi çöplüğü içinde yüzülmektedir. Yani, “doğru” ve “yararlı” bilgiye ulaşmak bilgi toplumu fertleri için çoğu zaman önemli bir sorun haline gelmektedir. Bu durum “bilgi kirlenmesi” kavramını gündeme getirmektedir. Naisbitt’in, “enformasyon içinde yüzerken bilgi için açlıktan ölmek” olarak ifade ettiği bu durum, çok sayıdaki dağınık, çelişkili ve

bütünsellikten yoksun bilgi karşısında bireyin birikimini düzenlemek için harcadığı çaba ve zamanı gün geçtikçe artırmakta; verim ise aksine düşmektedir.

Bilgi toplumunda insanlar zamanlarının çoğunu, bilgi ve iletişim teknolojilerinin ürünü olan cihazların karşısında değerlendirilmektedir. Fakat buna rağmen içerikte büyük bir yozlaşma, anlayışta kısırlaşma yaşanmakta ve “enformatik cehalet” yaygınlaşmaktadır. Bilişim alanındaki yoğun gelişme ve ilerleme, enformasyon tüketimini artırırken, aynı oranda toplumsal ve bireysel bilgiyi sığlaştırma tehlikesine de kapı aralamaktadır. Dolayısıyla, bilgi toplumunun en ciddi sorunlarının başında, bu sığlaşma-düzeysizleşme-sıradanlaşma tehlikesi gelmektedir.

Diğer yandan, İnternetin iletişim, bilgi edinme, paylaşım, ticaret, kamu hizmeti alma gibi iyi amaçlarla kullanılması ve insanlığa hizmet sunmasına tanık olunurken, barındırdığı yasadışı ve zararlı içerikler, yanlış veya suçta araç olarak kullanımından kaynaklanan çeşitli toplumsal sorunlara, güvenlik ve mahremiyete ilişkin risklerin oluşmasına ve giderek yaygınlaşmasına neden olduğu görülmektedir. Bu sorunlar en başta çocuklar, gençler ve aileler olmak üzere tüm toplum kesimlerini etkilemektedir.

Bilgi toplumuna yönelik bu eleştiri ve sorunlar, bugün ve gelecekte bilgi ve iletişim teknolojilerinin son analizde insanlığa hizmet etmek yanında, onun sonunu hazırlama risk ve tehlikesini de içinde barındırdığını ortaya koymaktadır. Diğer yandan, bilgi toplumu olgusuna ilişkin olarak bahsi geçen risk ve tehlikelerin ortaya çıkmasında bilgi toplumunun itici gücünü oluşturan İnternetin önemli bir rolünün olduğunu da unutmamalıdır. Buradan hareketle, topluma yön veren siyasetçilerin ve kamu yöneticilerinin sözü edilen olgu ve sorunların farkında olarak, yeni teknolojilerin insanoğlunun özgürlüğü, refahı ve mutluluğu için kullanıldığını garanti altına alma sorumluluklarını yerine getirmeleri büyük önem taşımaktadır.

İnternetle ilgili konuları buraya kadar özet bir tasviri yapılan bu büyük fotoğraf ve gösterdiği gerçeklik bağlamında ele almak ve İnternet özelini, bu bütünlüğün içindeki yeri ve anlamı bakımından anlamaya çalışmak gerekmektedir. Yani, İnternete ilişkin olguları değerlendirirken bu büyük bilgi toplumu fotoğrafını olumlu

ve olumsuz yönleriyle birlikte sürekli hatırdâ tutmalıdır. Aksi takdirde, sorunların gerçek boyutları ile görülmesi mümkün olmayacak ve eksik veriler üzerine yapılan değerlendirme ve analizler yanlış sonuçlara ve eksik çözümlere götürecektir.

4. İnternet kaynaklı en önemli sorunlardan birisi, İnternet içeriklerinin önemli bir kısmını oluşturan yasadışı ve zararlı içeriklerdir. Bu tür içeriklerin başlıcaları; pornografi ve çocuk pornografisi, fuhşa aracılık, ırkçılık, ayrımcılık, kumar oynamaya ve uyuşturucu kullanmaya teşvik, şiddet, vahşet, nefret ve intihara yönlendirme içerikleri ile telif hakkı ihlallerine ait içeriklerdir.

Yasadışı ve zararlı İnternet içerikleri arasında en büyük yere sahip olan içerik türü pornografi ve çocuk pornografisi içerikleridir. Günümüzde bu tür içerikler dijital teknolojilerin ve özellikle İnternetin sunduğu imkanlarla, tüm dünyada çok hızlı bir şekilde artmakta, çoğaltılmakta ve paylaşılmaktadır. Keza, pornografinin, İnternette özgürce yer alması ve sınırsızca paylaşılabilmesi tüm dünyada eleştiri konusu yapılmakta ve bunlarla mücadele edilmesinin gerekliliği tartışılmaktadır.

Lakin, günümüzde, pek çok ülke, sadece çocuk pornografisini suç kapsamında değerlendirirken, yetişkin pornografisini ya hiç suç olarak kabul etmemekte veya sadece extrem pornografiyi bu kapsama almaktadır. Fakat, suç olarak görülse bile genellikle cezalar yetersiz kalmaktadır. Bu durumda, gerçek görüntüler yanında bilgisayar programları ile üretilmiş canlandırmaya dayalı materyallerle, hikaye tarzı metinlerden oluşan pornografik içerikler barındıran İnternet, gençler ve çocuklar için pornografiyle karşılaşmada ilk adres olmaktadır. Keza, İnternet, sadece en büyük ve zengin içerikli pornografi koleksiyonunu kullanıcıya sunarak pornografi endüstrisini teşvik etmekle kalmamakta, sürekli pornografik konuşmaların yapıldığı sohbet odaları kullanılarak genç erkek ve kızlara promosyonlar ve hediyeler verilerek birbirleriyle tanışmaları sağlanmakta ve bu piyasaya çekilmeye çalışılmaktadır.

Nitekim, İnternet pornografisi konusunda yapılan araştırmalardan elde edilen bazı veriler sorunun boyutlarını ortaya koymaktadır. Bu verilerden bazılarını hatırlayalım. İnternette yaklaşık 370 milyon pornografik web sayfası bulunmaktadır ve toplam

içeriğin %37'sini bu pornografik içerikler oluşturmaktadır. İnternette her gün pornografik içerik için 68 milyon arama yapılmaktadır. “Sex” kelimesi İnternette yapılan tüm aramaların 1/4'üne karşılık gelirken, en çok arama yapılan 200 sözcüğün 82'sinin pornografi ile ilişkili olduğu ve 24 yaş altı erkek kullanıcıların %70'inin bu tür sitelere girdiği tespit edilmiştir. İnternette indirilen içeriklerin %35'i pornografik temalıdır ve her gün 2,5 milyar civarında pornografik e-posta gönderilmektedir. Sanal pornografi meraklıların 1/3'ü kadındır. Ayrıca, pornografik içerikli web sitelerinin büyük bölümü kötü amaçlı yazılımlar barındırmaktadır.

İnternet, çocuk pornografisinin akıl almaz bir hızla gelişmesine neden olmuş, ticaretine küresel bir kimlik kazandırmış ve bir suç tipi olarak uluslararası alanda dünyayı tehdit eden önemli sorunlardan birisi haline getirmiştir. Çocuk pornografisi materyallerinin %85'inin İnternet aracılığıyla dağıtılmakta olduğu tespit edilmiştir. İnternet, çocuk pornocuları ve çocuk tacirlerine, birbirlerine ulaşma, yeni kurbanlar ve materyaller bulma gibi konularda, İnternet sayfaları, haber grupları, e-posta iletileri ve sohbet odaları ile büyük kolaylık sağlamaktadır. Ayrıca, tespit edilme riskini en aza indirmek amacıyla, çocuk pornocuları arasında değiş tokuş işlemleri için bire-bir (peer-to-peer) bağlantı yönteminin de tercih edildiği görülmektedir.

Uzmanlar, pedofillerin ilk başta yetişkin, daha sonra hayvan ve en son çocuk pornografisine yöneldiklerini tespit etmiştir. Bazen çok küçük yaştaki çocukların hatta bebeklerin yer aldığı, acımasızca ırza geçme, cinsel kölelik, hayvanlarla birlikte cinsel ilişki ve cinsel tacizin bütün çeşitlerini gösteren içerikler, çocuk pornografisinin iğrenç yüzünü ortaya koymaktadır. Nitekim, Telefono Arcobaleno'nun araştırmasında bu materyallerde yer alan çocukların %42'sinin 7 yaş altı, %77'sinin 9 yaş altı ve %19'unun 3 yaş altı olduğunun tespit edilmesi; Cybertip İhbar Merkezi'nin araştırmasında bu tür materyallerin %35'inde çocuklara tecavüze rastlanılması ve 8 yaşından küçük çocuklara ait materyallerin %69'unda çocuklara ekstrem taciz ve tecavüzlerin görülmesi; IWF araştırmasında, içeriklerin %72'sinde 0-10 yaş arası çocukların ciddi anlamda şiddet gördüklerine, %44'ünde cinsel işkence ve vahşete maruz kaldıklarına rast gelinmesi bu durumun bir kanıtıdır.

Diğer yandan, çocuk pornografisinin çocuklara karşı işlenen cinsel suçları beslemekte, teşvik etmekte ve kolaylaştırmakta önemli rol oynadığı bilinmektedir. Çünkü bu tür içeriklere ilgi duyan yetişkinler çoğu zaman söz konusu içerikleri izlemekle yetinmemekte, normal hayatta da bu davranışın akislerini sürdürmektedir. Nitekim yapılan araştırmalarda, çocuk pornografisi materyalleri alan-satan ve bulunduran kişilerin yaklaşık %80'inin bizzat kendisinin de aktif olarak çocuklara cinsel istismar ve şiddet uyguladıkları görülmüştür.

Keza, araştırmalar büyük bir pazar ve sektör haline gelen çocuk pornografisine olan ilginin her geçen yıl hızla arttığını göstermektedir. Nitekim, sektörün 2004 yılında bilinen geliri 20 milyar dolar iken, bugün 100 bini aşkın çocuk pornografisi sitesi bulunduğu, 2 milyon çocuğun bu sektörde seks kölesi olarak kullanıldığı, online suistimale uğrayan çocukların sayısının günde 20 bini aşmakta olduğu, sektörün yıllık cirosunun 80-90 milyar dolara ulaştığı tahmin edilmektedir.

Diğer yandan, çocukların cinsel istismarı içeriklerinin son derece pahalı olması nedeniyle dünyada giderek artan bir lüks tüketim haline geldiği, bu ürünlerin daha çok zengin ve eğitimli bir müşteri kitlesinin olduğu bilinmektedir. Bu nedenle, bu web siteleri barınmak için, yasal problemler ile karşılaşmamak amacıyla nispeten daha fakir ve bu konularda yasal düzenlemeleri olmayan ülkeleri seçmektedir. Keza, kapatılmamak ve erişilebilir kalmak için büyük çaba sarf etmekte, sık sık ülke ve IP adresi değiştirmektedir. Bazen de, ele geçirdikleri zombi bilgisayarlardan, sahibinden habersiz olarak bu içeriklerin dağıtımını yapmaktadırlar. Ayrıca, bu tür içeriklerin dağıtımında artık ağırlıklı olarak bedava barınma sağlayan servisler, sosyal ağlar, fotoğraf paylaşım siteleri ve ele geçirilmiş web siteleri de kullanılmaktadır. Dağıtıcılar yer sağlayıcı hizmetini daha karmaşık sistemleri olan, Kuzey Amerika, Avrupa ve Rusya gibi daha hızlı ve daha ucuz ülkelere almaktadırlar.

Görüldüğü gibi, çocukların cinsel istismarı ve çocuk pornografisi çok boyutlu ve küresel ölçekte güncel bir sorundur. Dolayısı ile bu alanda çok ciddi ve profesyonel mücadele gerekmektedir. Buna mukabil çocuk pornografisine karşı yürütülen ulusal ve uluslararası mücadelenin önünde bazı engeller vardır. Çocuk pornografisinin

tanımına ilişkin farklı anlayışlar, ülkelerin kanunlarında çocuk yaşı konusunda farklılıkların bulunması, yetişkin ile çocuk pornografisi arasında net bir ayrıma gidilememesi, ülkeler arasındaki yasal, sosyal ve kültürel farklılıklar ve ortak işbirliğinin sağlanamaması gibi nedenler bunların başlıcalarıdır. Bunun yanında, milyarlarca dolarlık gelirler söz konusu olunca bazı ülkelerin çocukların cinsel istismarı içerikleriyle mücadelede kafa karışıklığı yaşadıkları ve cılız tedbirlerle konuyu geçiştirdikleri görülmektedir.

Ayrıca, çocuk pornografisi, çocuk fahişeliği, çocuk seks turizmi ve insan kaçakçılığı arasında birbirini üreten, büyüten ve destekleyen yakın bir ilişki bulunmaktadır. Ne yazık ki, fuhuş ve porno için kullanılan çocukların daha çok dünyanın gelir düzeyi düşük, ekonomik sorunlar yaşayan, savaş, doğal afet, etnik çatışma vb sosyal ve siyasal çalkantıların yoğunlukta olduğu bölgelerde yaşayan mağdurlardan oluştuğu görülmektedir. Dolayısıyla, İnternet ortamındaki çocukların cinsel istismarı içerikleri, çocuk fahişeliği, çocuk seks turizmi ve insan kaçakçılığının asıl kaynağının gerçek hayat olduğu; dünyadaki gelir adaletsizlikleri, savaşlar, çıkar çatışmaları, ekonomik ve sosyal krizler son bulmadan, yani kaynak kurutulmadan bu tür sorunlarla mücadelenin sınırlı kalacağı açıktır.

Diğer yandan, bazı kesimler de ilginç bir şekilde bu tür içeriklerin serbest olmasını, “İnternet özgürlüğü” ve “İnternette ifade özgürlüğü” bağlamında değerlendirilmesi gerektiğini iddia etmektedir. Fakat, pornografiye erişim özgürlüğünün ifade özgürlüğü kapsamında değerlendirilmesi genel olarak kabul görmeyen bir görüştür. Zira, ifade özgürlüğünün ne zaman, nasıl ve hangi şartlarda sınırlandırılabilceği AİHS’nin 10. maddesinde belirlenmiştir. Burada zikredilen sınırlandırma konularından birisi de “genel ahlakın korunması”dır. Nitekim, AİHM de bir çok kararında, sınırlama veya müdahale için mevzuatın olması, sınırlamanın meşru bir amacının bulunması ve sınırlamanın demokratik bir toplum için gerekli olması ölçütlerine bağlı olarak söz konusu sınırlama ve müdahaleyi uygun görmüştür.

Ayrıca, pornografinin ulaşamadığı özgür alanlar olmasının da özgürlüğün bir parçası olduğu tüm dünyada yüksek sesle savunulmaya başlanmıştır. Buna göre, insanın

beden ve ruh sağığına zarar veren ve sosyal dokuyu zedeleyen pornografi konusu kişisel özgürlükler kapsamında değerdendirilmemelidir. Toplumun aleyhine bir özgürlük arayışının makul görölmesi mümkün değildir. Nasıl benzer gerekçelerle ‘Dumansız Hava Sahası’ uygulaması kabul görüyorsa, “ pornosuz İnternet sahası” uygulamasına da itiraz edilmemelidir.

Fakat, günümüzde, pornografik ürünlerin üreticileri ve dağıtıcıları yanında, bankaları, yazılımcıları, kredi kartı firmalarını, İSS’ları, kablolu yayıncılık yapan şirketleri ve otel zincirlerini de içini alan ve silsile olarak birbirine bağılı, trilyon dolarlık büyük bir pastayı paylaşan porno endüstri, toplumsal maliyeti ne olursa olsun, daha çok kazanmak ve kar elde etmek için var gücü ile çalışmakta ve pornografinin yayılmasının önündeki toplumsal, kültürel ve yasal tüm engelleri aşmaya, dirençleri kırmaya çaba göstermektedir.

Bu nedenle porno endüstrisi, toplumda pornoyla ilgili olumlu bir imajın oluşturulması, popüler kültüre entegrasyonu, kamu otoriteleri ve toplumca olağan ve normal görölmesi, yasal güvenceler elde edilmesi yönünde çok yönlü ve ciddi çalışmalar yapmaktadır. Pornografik içeriklerin İnternet ortamında serbestçe barınabilir, bulunabilir ve paylaşılabilir olmasını sağılamak için konuyu “İnternet özgürlüğü” ve “ ifade özgürlüğü” bağlamına ve alanına çekme çalışmaları da sektörün bu kapsamdaki uğraşı ve stratejilerinden birisi olarak görülebilir.

Bu stratejiye, aynı zamanda çocuk pornografisine de bu yolla bir özgürlük alanı açmaya çalışan çocuk pornografisi sektörünün de destek vermesi kuvvetle muhtemeldir. Çünkü, bu çevrelerin de benzer strateji ve yaklaşımlarla çocukların bir seks objesi olarak görölmesinin ve kullanılmasının kişisel bir tercih ve özgürlük konusu olduğunu, bunun doğal, olağan ve normal karşılanması gerektiğini savunarak, çocuk pornografisinin serbest bırakılmasını sağılamaya çalıştıklarına da rastlanılmaktadır. Nitekim pedofiller, yakın bir zamana kadar nasıl eşcinsellik bir sapkınlık olarak görölürken bugün bir bireysel tercih ve özgürlük konusu olarak kabul ediliyor ise, zaman içinde kendilerinin de bu kapsamda değerdendirilip kabul

göreceklerini ummaktadır. Keza, Hollanda ve İsveç gibi bazı ülkelerde çocuk pornografisinin yasallaşmasını savunan bazı siyasi oluşumlar dikkat çekmektedir.

Dolayısıyla bu çevrelerin, yetişkin pornografisi konusundaki toplumsal direncin ve muhalefetin “özgürlük” argümanı ile kırılması ve izale edilmesini, hedeflerine ulaşmak için bir adım olarak görmeleri doğaldır. Bu nedenle, bazı ülkelerin pornografik içeriklere erişimi engelleyen veya sınırlandıran uygulamaları, pornografi sektörünün gayretleri ile bir kısım sansür konusunda hasas olan özgürlükçü çevreleri de yanına alarak “Sansüre Hayır”, “Pornoya Özgürlük”, “Pornoma Dokunma” kampanyalarına konu olabilmektedir.

Diğer yandan, İnternette görülen şiddet, vahşet, nefret ve intihara yönlendirme içerikleri de diğer bir sakıncalı içerik türüdür. Şiddeti ve saldırganlığı özendirme, intihara teşvik etme, ırk, etnesite, cinsiyet, din, dil ve mezhep temelli ayrımcılık ve nefreti kışkırtma gibi içerikleri ile İnternet, özellikle çocukların ve gençlerin gerçeklik sınırlarını zorlamalarına, “aykırı yaşama” ve “şiddet” kültürünün etkisinde kalmalarına ve yanlış model oluşturmalarına, kendilerine ve yaşadıkları topluma zarar verecek düşünce, tutum ve davranışlara yönelmelerine neden olmaktadır.

Yine, İnternet barındırdığı içerikler ile her yaş grubundan kullanıcıları, özellikle çocukları ve gençleri kumar, bahis ve şans oyunları oynamaya teşvik etmekte ve imkan sağlamaktadır. Bu nedenle, İnternet üzerinden oynanan kumar, bahis ve şans oyunları büyük paraların döndüğü devasa bir sektör haline gelmiştir. Kumar ve bahis bağımlıları başta olmak üzere insanlar, günümüzde sayılarının on binlerce olduğu telaffuz edilen İnternet sayfaları aracılığıyla kumara, bahise ve şans oyunları oynamaya teşvik edilmektedir. Nitekim, Facebook’un kendi altyapısında geliştirdiği ve 200 milyon üyesi ile dünyanın en büyük oyun platformu olan Teksas Hold’em Poker adlı kumar oyunu bunun bir örneğidir.

Keza, sanal ortamda suç takibinin zor olması sebebiyle uyuşturucu ve uyarıcı madde kaçakçıları, bu tür maddelerin pazarlanmasının, satışının ve üretimin her aşamasında İnterneti kullanmaktadır. Bazı İnternet siteleri uyuşturucu ve uyarıcı madde türleri,

retim teknikleri ve retim iin hammaddelerin nasıl temin edilebileceğine ilişkin bilgilere yer verirken, bazıları da kişileri uyuşturuu ve uyarıcı madde kullanmaya alenen zendirecek sohbet odaları, forum, video vb. ierikler sunmaktadır.

Keza, İnternette grlen en nemli ierik sorunlardan birisi de telif hakkı ihlalleri konusudur. Fikir ve sanat eserlerinin izinsiz kullanımı İnternette en ok rastlanan ierik sorunlarındandır. Teknolojinin gelişimiyle birlikte kopyalama, kayıt ve taklit gibi eylemler kolaylaşmış, fikri mlkiyet haklarına tecavz de artmıştır. İnternetle birlikte, fikri mlkiyet haklarına ynelik sorunlar, ticari ve hukuksal boyutları ile karşı karşıya kalınan en karmaşık meselelerden birisi haline gelmiştir.

Bahsi geen yasadışı ve zararlı ierikler dıřında, gvenlik sorunu İnternetin getirmiş olduđu nemli olumsuzluklardan birisidir. Hızla gelişen ve yaygınlaşan İnternetin denetimden uzak yapısı, İnterneti, illegal pek ok iş ve oluşumun yeni buluşma alanı haline getirmektedir. İnternet, bilişim suçları olan; bilgisayar sistemlerine ve servislerine yetkisiz erişim, bilgisayar sabotajı, bilgisayar yoluyla dolandırıcılık, izinsiz yazılım kullanımı, bilgisayar yoluyla sahtecilik, telekomnikasyon hizmetleri hırsızlığı, bilgisayar sistemlerinin suç rgtleri tarafından kullanılması, tehdit ve gasp gibi suç eşitlerinin hayatımıza girmesine sebep olmuştur.

Teknolojik gelişme, terrn de siber ortama taşınmasına yardımcı olmuş, suç, kabuk değıřtirerek kendini siber ortamda gstermiştir. İnternet, suç rgtleri, terr grupları ve ayrılıkı gler iin organize olma, eđitim, iletiřim ve propaganda, yardım ve bađıř toplama aracı olarak kullanılabilir. Yine, İnternetin sađlamış olduđu imkanlarla ulusal veya uluslararası suç rgtleri, ekonomik, politik veya askeri amalarla siber saldırılar yapabilmektedir. Keza, son dnemde bu siber saldırıların lkeler arasında siber savařlara dnřtđ grlmektedir. lkeler siber savařlar iin hem savunma hem de saldırı amalı olarak siber ordular kurmakta ve kullanmaktadır.

Bu kapsamda, kresel İnternet firmaları ve kullanımları ok yaygın olan rnlerine ilişkin tereddtler olmuştur. zellikle popler arama motorlarının aynı zamanda iyi birer casus yazılımı olarak tm lkeler aısından riskler tařıdıđı belirtilmektedir.

Dünyada en çok tercih edilen arama motoru olan “Google”ı kontrol altında tutan ABD’nin bu yolla dünyanın bütün bilgisini topladığına dikkat çekilmektedir.

Yine, İnternet bağlantısına sahip bilgisayarların güvenlik önlemlerinin yetersiz olması veya yetersiz kalması nedeniyle, İnternet üzerinden gelebilecek başlıca dijital tehlikeleri casus yazılımlar, bilgisayar virüsleri, solucanlar (spamlar), truva atları (trojenler), phishing (oltalama), botnetler olarak sıralayabiliriz.

Devletlerin, bir takım güvenlik riskleri ve tehditlerini gerekçe göstererek kişilerin telefon ve İnternet iletişimini takip etmeyi, dinlemeyi ve izlemeyi istemesi, kişisel hakların ve mahremiyetlerin ihlali konusunu gündeme getirmektedir. Geline bu nokta, bilgi toplumunun en önemli tartışma konularından birisi olan özgürlük/güvenlik paradoksu sorununu ortaya çıkmaktadır. Devlet güvenliğini koruma ile bireylerin mahremiyetini koruma arasındaki çatışma yeni olmamakla birlikte; gelişen teknoloji ve özellikle İnternet teknolojisinin devlete bireyler hakkındaki özel bilgilere eskisinden daha fazla ulaşma imkanı vermesi, bilgi toplumunda, ulusal güvenliği korumak ile mahremiyetin korunması daha sık karşı karşıya gelmekte ve mahremiyet ihlalleri daha çok vuku bulmaktadır.

Bu çerçevede, İnternetin doğum yeri, merkezi ve büyük oranda hakimi olan ABD’nin güvenlik gerekçesi ile istihbari amaçlı olarak kişilerin özel bilgilerine ulaşma konusunda ciddi çalışmalar yaptığı bilinmektedir. Hatta, İnternette hizmet veren, ana serverları ve hostingleri ABD’de bulunan ABD menşeli birçok büyük şirketin (Microsoft, Facebook gibi), ABD istihbarat örgütleri ile işbirliği içinde bulunduğu sıkça dile getirilmektedir.

Diğer yandan İnternetin, güvenlik ve mahremiyet riskleri yanında, gerek bireylerin oluşturduğu aile yapısını, gerekse çocuk ve gençleri olumsuz yönde etkileyecek özelliklere sahip olduğu bilinmektedir. Nitekim, İnternetin toplumun temel taşı olan aile kurumu için önemli tehlike ve tehditler oluşturduğu; aile düzenin bozulması yönünde negatif bir etkisinin olduğu ifade edilmektedir. Bu kapsamda, İnternetin aile üzerindeki olumsuz etkileri, aşırı kullanımı durumunda aile içi ilişkilere ve iletişime

vermiş olduğu zarar, eşler arasında “aldatma”yı kolaylaştırması ve boşanmaların artmasına neden olması ve barındırdığı yasadışı ve zararlı içeriklerin genel olarak tüm aile bireylerini olumsuz yönde etkilemesi şeklinde üç noktada toplanmaktadır.

Özellikle pornografik içerik toplumun temel taşı olan aile kurumu için önemli bir tehdit haline gelmiştir. İnternetin bireyleri yeni cinsel arayışlara ittiği bilinmektedir. Porno izleyen erkekler eşlerini daha az heyecan verici bulmakta ve içeriklerde gördüklerini eşlerinden beklemektedir. Bu durum aile içi huzursuzlukların artmasına, evliliklerin riske girmesine neden olmaktadır. Araştırmalar, İnternet pornografisinin artan boşanma davalarının sebeplerinden birisi olduğunu göstermektedir. ABD’de yapılan bir araştırmada katılımcıların %62’si İnternetin boşanmalarda etkili olduğunu ve boşanma vakalarının %56’sının eşlerden birinin pornografik İnternet sitelerine olan takıntılı ilgisinden kaynaklandığını belirtmeleri bu duruma bir örnektir.

Diğer yandan, pornografinin erkeklerin kadınlar üzerinde kurmayı tahayyül ettikleri iktidar ve tahakküm arzusunu sömürmekte olduğu, zevk kölesi, hizmetçi, kurban rolünden hoşlanan kadın prototipleri ortaya koyarak, gerçek hayat ve kadın gerçeği hakkında yanlış düşüncelere kapılmalarına sebebiyet verdikleri dile getirilmektedir. Zira, pornografi kadınların kendilerine kötü davranılmasından, şiddetten, tecavüze uğramaktan, aşağılanmaktan aslında gizliden gizliye “memnun olduklarına” dair hastalıklı düşünceler uyandırmaktadır.

Kuşkusuz İnternet kaynaklı risk ve tehlikelerin en çok tehdit ettiği toplumsal kesimler çocuklar ve gençlerdir. Bu kapsamda çocuklar ve gençler İnternet ortamında pornografi ve cinsel istismarla, şiddet, vahşet, siber zorbalık ve ırkçılık içerikleriyle karşılaşabilmekte, sosyal ağlar, dijital oyunlar ve bağımlılıkla ilgili sorunlar yaşayabilmektedir.

İnternetin çocuklar ve gençler açısından risk oluşturan en önemli tehlikesi çocukların pornografik görüntülere maruz kalması ve cinsel istismarı gelmektedir. İnternette pornografik yayınların sınırsız olması, kolay erişilebilmesi ve denetimin zor olması gibi nedenlerle çocuklar ve gençler erken yaşlarda pornografik görüntülerle

tanışmakta ya da bazen cinsel istismara maruz kalabilmektedir. Bu çerçevede, İnternet ortamında giderek yaygınlaşan bir sorun da, İnternette kendini çocuk olarak tanıtır cinsel haz amacıyla çocukları hedef alan yetişkinlerin bu hedefe ulaşmak için yaptıkları faaliyetleri ifade eden “grooming”dir. Pedofil hastası yetişkinler İnterneti kullanarak çocukları kandırma veya tehdit etme yoluyla gerçek hayatta buluşmaya, tanışmaya zorlamakta ve sonrasında çocuğu sapkın cinsel emellerine alet etmektedir. Ne yazık ki, sohbet servisleri ve sosyal ağların yaygınlaşması tüm dünyada grooming olaylarının sayısında patlamaya neden olmuştur.

Çocukların ve gençlerin İnternet ortamında sıkça pornografik içeriğe ve tacize maruz kaldıklarını kanıtlayan birçok araştırma vardır. İngiltere’de yapılan bir araştırmada, İnternette gezinen çocukların %57’si çevrimiçi pornografiye rastladığını, %38’i başka bir şey yaparken önüne pornografik içerikli reklamın çıkıverdiğini, %36’sı başka bir şey ararken bir porno sitesine kazara girdiğini, %25’i ise pornografik mesaj sağanağına yakalandığını belirtmiştir. Keza, Kaiser Family Foundation’un hazırladığı bir raporda, 15-17 yaş arası gençlerin %70’i pornografik içeriklerin onlar istemeden karşısına çıktığını ve %23’ü bu olayın sıklıkla tekrarlandığını belirtmiştir. Yine, ITU’nun bir araştırmasında her yıl, İnternet kullanıcısı her 5 çocuktan 1’inin İnternet saldırganlarının veya pedofili hastalarının tacizine uğradığı tespit edilmiştir. Keza, Symantec’in araştırması, 7-14 yaş arası çocukların arama motorlarında ilk üç sırada YouTube, Google ve Facebook sözcüklerini aradıkları, ardından sex ve porno kelimelerinin geldiği görülmüştür. Başka bir araştırmada, İnternette ilk kez pornografiye maruz kalma yaşının ortalama 11 olduğu ve 8-16 yaş arası çocukların %90’ının çoğu ev ödevi yaparken online pornografiyle karşılaştığı tespit edilmiştir.

Çocukların ve gençlerin İnternet kullanımında önemli yer tutan konulardan birisi de dijital oyunlardır. Dijital oyunların etkileşimli ve son derece eğlendirici olmaları dijital oyun oynama alışkanlığı her yaştan birey için tutkuya dönüşürken, dünyada ekonomik açıdan hayli büyük yere sahip bir sektör haline gelmesinde etkili olmaktadır. Nitekim, günümüzde 1 milyarı geçen müşteri kapasitesi, krizlerden en az etkilenen ve katma değeri çok yüksek karakteri ile dijital oyun sektörü 2011 yılı itibarıyla 70 milyar dolarlık ciroyu aşmıştır. Dijital oyun oynama yaşı 5-6’ya

düşerken, dijital oyunların cazibesi, İnternet kullanımını da artırmaktadır. Yapılan araştırmalarda, İnternet kullanımının nedenleri arasında oyun oynamak daima ilk üç sebepten biri olmakta, çoğu kez yüzde 50'lik bir orana ulaşmaktadır. Bu nedenle, önemli bir kullanıcı sayısına sahip olan sosyal ağlar da İnternet ortamında oynanabilen oyunları desteklemekte ve pazarlamaktadırlar. Örneğin, Facebook kullanıcılarının 80%'i bu siteyi oyun oynamak için kullanılmaktadır.

KontROLSÜZ, amacı dışında ve bilinçsiz kullanılması halinde dijital oyunların çocuklar ve gençler üzerinde olumsuz etkiler meydana getirdiği bilinmektedir. Bu çerçevede, bağımlılık oluşturmada yanında, başka bir takım fiziksel ya da psiko-sosyal sağlık sorunlarına neden olduğu konuyla ilgili literatürde sıklıkla gündeme getirilmektedir.

Birçok bilgisayar oyununda gösterilen kötü karakterler, başkalarının hayatını ve duygularını önemsememe, yaşamak için yok etme, ahlaki değerlerin horlanması, karşısındakine değer vermeme, insanları kategorize etme gibi mesajlar çocukların ve gençlerin kişiliğinin gelişmesine olumsuz tesir oluşturmaktadır. Keza, şiddet başta olmak üzere, savaş, suç, soygun, gaddarlık gibi olguları normalleştirerek, saldırganlık, duyarsızlık, bencillik, açgözlülük, düşmanlık, hilekarlık gibi olumsuz davranışlara yönlendirmektedir. Nitekim, yakın zamanda, Norveç'te bir gençlik kampında katliam yapan aşırı sağ eğilimli Breivik'in mahkemedeki ifadesinde rol yapma oyunu türündeki savaş oyunlarından etkilendiğini söylemesi, dijital oyunlar ve şiddet arasındaki ilişkiye dikkat çekmektedir. Keza, ABD'de, 1997-2002 arasında dijital oyunlardaki şiddetin sebep olduğu düşünülen 16 benzer olay tespit edilmiştir.

Son zamanlarda İnternet'in gençler tarafından daha sık kullanılmaya başlanmasıyla gündeme gelen konulardan birisi de siber zorbalıktır. Siber zorbalık, e-posta, sohbet ortamları, sosyal ağlar ya da cep telefonları kullanarak kişileri sürekli rahatsız etme, alay etme, hakaret etme, isim takma, tehdit etme, korkutma, dedikodu yayma ya da kişinin rızası olmadan fotoğraflarını yayınlama gibi ilişkisel saldırı davranışlarını içermektedir. Siber zorbalığa maruz kalan çocuklarda, derslerde başarısızlık, disiplini bozma, okula gitmek istememek, depresif ruh hali, öfke/kızgınlık, çocuğun kendisine olan saygısını yitirmesi, diğer insanlarla ve ailesiyle ilişkilerinde bozulma gibi

fiziksel ve duygusal durumlardan biri ya da birkaçının görülebildiği belirlenmiştir. Yapılan araştırmalar, siber zorbalığın okullarda sıkça görülen bir tehdit unsuru haline geldiğini göstermektedir. Örneğin, Kanada’da yapılan bir çalışmada, çocukların %27,3’ünün e-posta yoluyla, %36,4’ünün ise iletişim ortamlarında siber zorbalıkla karşılaştığı, ABD’de yapılan bir çalışmada ise, sanal zorbalık olaylarının devlet okullarında %54, özel okullarda %34 oranında gerçekleştiği tespit edilmiştir.

İnternetin getirdiği diğer bir olumsuzluk ise, özellikle okul çağındaki gençlerde sık görülen, psikolojik ve bedensel gelişimlerini, sosyal ilişkilerini olumsuz yönde etkileyen “İnternet bağımlılığı”dır. Zevk, haz, risk, macera ve uzaklaşma duygularını kamçılayan birçok madde gibi İnternet de bağımlılık yapabilmektedir. İnternet bağımlılığının ortaya çıkmasında etkili olan konular ise cinsellik, flört, muhabbet, kumar, pornografi, sohbet, borsa oynamak, açık artırmalara katılmak, oyunlar ve saplantılı bir şekilde yeni bilgiler peşinde koşmak olarak sıralanmaktadır. Nitekim, ABD, Çin, Güney Kore, Tayvan İnternet bağımlılığı’nı ulusal bir problem olarak tanımlamışlardır. Lise öğrencilerinin haftada ortalama 23 saat bilgisayar oyunu oynadıkları ve 2.1 milyon lise öğrencisinin bağımlılık riski taşıdığı Güney Kore’de 140’ın üzerinde İnternet bağımlılığı tedavi kliniği hizmet vermektedir. Çin’de ergenlerin %13,7’sinin İnternet bağımlısı olduğu tespit edilmiştir.

Diğer yandan, İnternet konusunda son dönemin en önemli fenomenlerinden birisi sosyal ağlardır. Dünyayı bir çığ gibi etkisi altına alan sosyal ağlar kullanıcı sayılarıyla rekora koşmaktadır. Sosyal ağların en popülerlerinden biri olan Facebook, dünyadaki mevcut İnternet kullanıcılarının %34,73’ü tarafından kullanılmaktadır. EU Kids Online’ın araştırma sonuçlarına göre; 9-10 yaşındaki çocukların %24’ü, 11-12 yaşındakilerin %48’i, 13-14 yaşındakilerin %72’i ve 15-16 yaşındakilerin %81’i sosyal paylaşım sitelerinden birinde profilleri bulunmaktadır.

Sanal ortamda sosyal iletişim kurmaya yarayan sosyal ağların, çocuklar ve gençler için yaygın kullanım özelliği bir takım riskler taşımaktadır. Bu risklerden birisi, kontrolsüz bir şekilde kişisel bilgilerin ve özel fotoğraf, video benzeri görüntülerin paylaşılmasıdır. Ancak, daha büyük tehlike, yetişkin kişilerin çocukların veya

gençlerin kişisel bilgilerine ve fotoğraflarına erişmesi ve çocuk veya gençmiş gibi onlarla iletişim kurmasıdır. Bu ortamlarda kandırılan çocuklar; uyuşturucu, alkol, pedofili, organ mafyası, istismar, taciz ve şantaj gibi tehditlerle karşılaşabilmektedir.

Keza, sosyal ağların bir tür “gözetleme”, “teşhircilik” ve “gözetim kültürü” meydana getirdiği ve bunun giderek yaygınlaştığı da dile getirilmektedir. Bireyler İnternet ortamında “denetlenmekten/gözetlenmekten” haz alma anlamında “teşhirciliğe”, diğer yandan gözetlerken dahi “gözetleme/dikizleme” eyleminde bulunarak “röntgenciliğe” yönelmişlerdir. Bu da sosyal ağların toplumsal etkileri bakımından gelinen ilginç ve endişe verici başka bir noktayı işaret etmektedir. Nitekim, sosyal paylaşım sitelerinde, şimdiye kadar bize sorulmasından rahatsızlık duyacağımız pek çok özel bilgimizi sırf trend olduğu için veriyor ve bundan keyif duyuyoruz. Aynı şekilde biz de başkalarının paylaştığı bilgileri okumaktan, fotoğraflarına bakmaktan, videolarını izlemekten, 'tweet'lerini okumaktan zevk alıyoruz.

Buraya kadar bahsi geçen konular, bilgi toplumu ve İnternetin, birçok riskleri ve tehlikeleri de beraberinde getirdiğini ve yeni sorunlara kaynaklık yaptığını ortaya koymaktadır. Bu olumsuzluklar tüm toplumu tehdit ettiği gibi özel olarak çocukları, gençleri ve aile kurumunu hedef almaktadır. Dolayısıyla, bu olumsuzlukları en aza indirecek önlemleri ve mücadele şekillerini ortaya koyan İnternet düzenlemelerine ihtiyaç bulunmaktadır. Eldeki veriler yasadışı ve zararlı içeriklerin yüksek sosyal maliyetlerinin olduğuna işaret etmektedir. O nedenle, başta pornografi olmak üzere her tür yasadışı ve zararlı içerikle etkili bir mücadele yürütmenin gereği açıktır.

5. Coğrafi sınırlara bağlı olmayan İnternetin, içerik düzenlemesiyle ilgili sorunlarda dikkate alınması gereken en önemli parametrelerden birisi uluslararası yönetimi ve işbirliği boyutudur. E-ticaretin milyarlarca dolarlık bir hacme ulaşması, telif hakları, zararlı içeriğin denetimi, İnternet iletişiminin ulusal güvenliğin bir parçası olarak görülmesi, kültürel ve dilsel çeşitliliğin sağlanması gibi nedenlerle alan adları ve IP adreslerinin yönetimi büyük bir menfaat çatışması ve mücadeleye konu olmuş ve İnternetin uluslararası yönetimi önemli bir sorun haline gelmiştir. Öyle ki, İnternet üzerinde söz sahibi olma, İnternet alan adları ve IP numaralandırma politikalarını

belirleme ve kontrol etme sorunu sadece devletler ve özel sektör arasındaki bir ihtilaf olarak değil, devletlerarası bir menfaat ve ideoloji sorunudur.

Devletler, zamanla İnternetin sosyal, siyasal ve ekonomik hayatı yönlendiren etkili bir araç olduğunu görmüşler ve farklı iç dinamiklerle İnternet üzerindeki etkilerini ulusal ve uluslararası ölçekte artırma gayreti içine girmişlerdir. Fakat, siber uzayın mimarisi teknoloji geliştirici ve üretici devletlerin politikaları doğrultusunda şekillendiği için, büyük oranda, bu ülkelerin özel ve kamusal güçleri bu alanın sınırlarını ve kurallarını belirlemekte ve regüle edilmesinde en büyük baskın güç olmaktadır. Dolayısıyla, yeni uygulamalar, mimari tarafından izin verildiği ölçüde uygulanma imkanı bulurken, bu alanın düzenlenmesi için belirlenen kurallar, çoğu zaman diğer devletler ve kullanıcılar tarafından isteksiz de olsa kabul edilmektedir. Bu durumda, diğer devletler çoğu zaman, kendi başlarına yaptıkları düzenlemelerde egemen güç olma adına değil, ikincil uygulamaların belli yönde yapılmasını gözetken etkin olmayan bir denetleme organı olarak hareket etmektedirler.

Diğer yandan, İnternet üzerinden gerçekleştirilen hukuk ihlalleri, işlenen suçlar ve zararlı içerikler tüm toplumları etkileyebilme gücüne sahiptir. Bu konularla ilgili yapılacak mücadelede devletlerin rolü önemlidir. Her bir devletin İnternetle işlenen suçlarla mücadele etmesi ve kendi egemenlik alanında üzerine düşeni yapması gerekmektedir. Bu mücadele devletlerin olduğu kadar uluslararası toplumun da menfaatinedir. Aksi takdirde, bazı devletler İnternet suçları için odak haline gelerek İnternet güvenliği için tehdit oluşturmakta ve İnternete güveni zedelemektedir.

Ulusal çabalara ek olarak; bu sanal ortamın zararlı tesirlerinden korunmak, işlenen suçlarla mücadele etmek ve “serbest suç işleme bölgelerinin” oluşmasını engellemek için sıkı bir uluslararası işbirliği ve her ülke için geçerli olacak yeknasak kurallar gerekmektedir. Bu kapsamda, İnternetin kötüye kullanılmasını önlemeye çalışan ve yaptırım uygulamaya yetkili merkezi bir otoritenin bulunmaması, İnternetin küresel ve merkezi olmayan yapısının getirdiği en önemli sorunlardan birisidir.

Ayrıca, İnternet trafiğinin farklı ülkeler üzerinden geçerek akması, bu karmaşık yapı içerisinde bir noktadaki bir sorunun dünyanın farklı noktalarındaki trafiği olumsuz yönde etkileyebilmesi, İnternet içeriğini barındıran sunucuların dünyanın her tarafına yayılmış bulunması, genel veya bölgesel İnternet noktalarının kontrolü, bakımı, hatların artırılması gibi nedenler İnternetin işlerliğinin devamı için tüm devletlerin aktif katılımını, uluslararası işbirliği ve koordinasyonu gerekli kılmaktadır.

Tüm bu nedenler İnternetle ilgili uluslararası düzenlemeler yapılmasının gereğini ortaya koymaktadır. Lakin, mevcut durum bu beklentileri karşılamaktan uzaktır. Çeşitli ulusal ve uluslararası kuruluşların işbirliğinden oluşan karmaşık ilişkiler bütününden ve çok aktörlü bir yapıdan oluşan mevcut durum, ABD dışında İnternet ağının tamamını kontrol eden tek bir ulusal veya uluslararası merkezi bir otorite bulunmaması sonucunu doğurmuştur.

Nitekim, İnternetin uluslararası yönetimiyle ilgili en önemli kurum olan ve İnternet alan adları sisteminin teknik yönetimi, IP adres alanlarının tahsisi, protokol parametrelerinin belirlenmesini ve kök sunucu sistemi yönetimi işlevlerini koordine etmekle görevli ICANN, California Eyaleti hukukuna tabi olarak, ABD Ticaret Bakanlığı'nca belirlenen esaslar çerçevesinde faaliyet göstermektedir. ICANN'ın görevleri arasında, "İnterneti çalıştırmak", İnternet polisliği, sitelerdeki ihlaller, güvenlik veya içerik konusu yer almamaktadır.

ICANN'la ilgili; hukuki meşruiyetinin bulunmadığı, çok yavaş çalıştığı, sorunları çözmekte yetersiz kaldığı, çalışma süreçlerinin ve prosedürlerinin düzgün, kolay ve anlaşılabilir olmadığı, hükümet, endüstri ve İnternet toplumunun tüm paydaşlarını bir araya getiremediği, yeterli mali kaynaklara sahip olamadığı, İnternet toplumundan kopuk olduğu, işlemlerinin gizli olduğu şeklinde yoğun eleştiriler vardır.

Keza, dünyadaki İnternet protokol parametrelerinin düzenlenmesi ve koordine edilmesiyle görevli IANA da, bağımsız olarak faaliyet göstermek üzere ABD Ticaret Bakanlığınca yetkilendirilmiş bir kurumdur ve uluslararası katılım ve ABD etkisinde hareket etme sorunu IANA için de geçerlidir. Yine, tüm sorumluluğu ICANN'a ait

olan ve dünya İnternet trafiğini düzenleyen 13 kök sunucu üzerindeki ABD etkisi, uluslararası katılım eleştirilerini kök sunucu yönetimi için de geçerli kılmaktadır.

ICANN ve IANA, mevcut yapılanma şekilleri ve karar alma süreçleri bakımından İnternet politikalarının taraflı oluşmasına neden olmakta, bağımsız hareket edememekte ve ABD Ticaret Bakanlığı'nın bir parçası olmaktan kurtulamamaktadır. Bu durum, haklı olarak ICANN ve IANA'nın meşruiyetinin sorgulanmasına neden olmakta; hükümetlerin eşit olarak temsil edildiği uluslararası bir kuruluş olarak yapılandırılmamaları meşruiyetlerini sorunlu hale getirmektedir. Bu itibarla, ICANN'ın tek bir hükümetin kontrolünde gayriresmi yapısından kurtarılarak tüm yetkilerinin bağımsız bir uluslararası örgüt tarafından gerçekleştirilmesi talep edilmekte ve tüm hükümetlere açık uluslararası meşruiyeti olan bir kuruluşa dönüştürülmesinin gerektiği dile getirilmektedir.

Diğer yandan ABD, ICANN'ın yönetiminin teknik bir sorun olduğunu, özerk yapısının devam etmesi gerektiğini, başka devletlerin müdahalesinin gereksiz olduğunu savunarak, İnternet üzerindeki hakimiyetini sürdürmek istemektedir. Zira, ABD, askeri iletişim stratejisinin bir parçası olarak ortaya çıkardığı İnterneti, güvenlik stratejisinin bir parçası olarak benzer bir amaç için kullanmaya devam etmekte ve bu nedenle İnternet üzerindeki egemen konumunu korumayı ekonomik ve ulusal güvenlik menfaatleri için gerekli görmektedir. Halbuki, artık küresel hale gelen ve kullanıcılarının büyük çoğunluğu ABD dışında bulunan İnternetin, yönetim boyutuyla da küresel ölçekte düşünülerek, uluslararası hale getirilmesi ve hükümetlerin yönetim süreçlerinde yer almalarının sağlanması gerekmektedir.

Bu talepler üzerine, başta AB olmak üzere uluslararası toplum, İnternet üzerindeki ABD etkisinin kırılması ve katılımcı bir yapının oluşmasını sağlamak için çeşitli girişimlerde bulunmuş ve bu süreçte "İnternet yönetişimi" kavramı ortaya atılmıştır. Özellikle Dünya Bilgi Toplumu Zirvelerinde gündeme getirilen İnternet yönetişimi; İnternetin idaresinin hükümetler, özel sektör, STK'ları ve uluslararası örgütlerin katılımıyla çok taraflı, şeffaf ve demokratik bir biçimde gerçekleştirilmesini, adil bir

kaynak dağılımını, herkesin kendi dilinde erişiminin kolaylaştırılmasını ve İnternetin istikrarlı ve güvenli şekilde çalıştırılmasını kapsamaktadır.

İnternet yönetiřimi; telekomünikasyon altyapısı, genişbant erişim, teknik standartlar, alan adlarının, IP adreslerinin, kök sunucuların yönetimi, spam, siber güvenlik, siber suçlar, řebeke güvenlięi, bilgi sistemlerinin güvenlięi, kritik altyapının korunması, sınırlar arası koordinasyon, rekabet politikaları, özelleřtirmeler, telif hakları, e-devlet, e-ticaret, elektronik kimlik doęrulama, yasadışı içerik, tüketicilerin korunması, bilginin özgürce akması, kişisel verilerin korunması, evrensel hizmet, ulusal altyapıların geliştirilmesi, kiralık hatların maliyetleri, eğitim, insan kaynaęı nitelięinin geliştirilmesi, kültürel çeřitlilik gibi konuları kapsayan içerięi ile İnternetin uluslararası yönetimi bağlamında tartiřılmaya devam etmektedir. Bu tartiřmalarda genellikle, bu alanlara ilişkin sorunların çözümünde hükümetlerin karar alma süreçlerinde etkinlięinin mutlaka saęlanması talep edilmektedir.

Bu çerçevede, ICANN'ın görevlerinin, BM'ye baęlı uluslararası özel uzmanlık kuruluřu olan ITU'ye devredilmesi fikri ciddi destek görmektedir. Teknik ve idari birikime sahip, hükümet-endüstri-sivil toplum ortaklıęını kurmayı bařaran, oturmuř ve kolay anlařılabilen çalışma sistemi ve prosedürleri olan, ekonomik kaynaklara sahip ve en önemlisi meřruiyet sorunu olmayan ITU'nun bu görev için uygun adres olacaęı deęerlendirilmektedir. Böylelikle kullanıcılara ek maliyetler çıkarılmamıř olacaęı ve İnternet alan adlarının tahsisi ve dięer çalışmalardan elde edilecek gelirlerin az geliřmiř ve geliřmekte olan ülkelerde İnternetin geliştirilmesi ve yaygınlařtırılmasına kullanılabileceęi öngörülmektedir.

Tezin 5. alt hipotezinde de belirtildięi gibi; sonuç olarak, bu gün için henüz devletlerin İnternet yönetiřimi konusunda taleplerini tatmin edecek düzeyde bir yapılanmaya gidilebilmiř deęildir. ICANN, ABD'nin mevcut uluslararası sistemdeki egemen konumundan dolayı varlıęını hala sürdürmektedir. Mevcut yapının veya ICANN'ın radikal bir dönüşüme uğramasının ancak ABD'nin uluslararası sistemdeki bu konumunun deęiřimine baęlı olduęu bilinmekle birlikte, uluslararası baskıların zaman içinde köklü deęiřikliklere sebep olabileceęi beklenebilir.

6.,8. Dünyada İnternet içerik düzenlemesinin nedenleri ve konuları, uygulanan modeller, ölçütler, ülkelerin konuya yaklaşımları, hukuksal ve örgütsel yapılar ve bunların işleyişleriyle ilgili hususlar da tartışılmaktadır. Bu kapsamda, özellikle İnternet içeriğinin devlet eli ile düzenlenmesi sorunu tüm bu tartışmaların merkezinde yer almaktadır. Nitekim bu konu, İnternet içeriğine müdahalenin doğru olup olmamasından, bunun devlet eli ile yapılmasının uygunluğuna; hangi içeriğe kim tarafından ne kadar müdahale edilebileceğinden, bunun hangi yöntemle ve nasıl gerçekleştirilmesi gerektiğine kadar bir dizi sorunu içinde barındırmaktadır.

Günümüzde, İnternetin güvenli kullanımını sağlamak amacıyla ülkeler, giderek artan bir oranda siber suçlarla mücadele ederken, diğer yandan İnternet içerik güvenliğiyle ilgili bir takım “önlem” ve “müdahaleleri” kapsayan düzenlemeler yapmaktadır. Bu düzenlemelerin “yöntemi” ve “kapsamı” tartışmalara neden olmaktadır. Bu çerçevede tartışmalar iki temel soruya/soruna odaklanmaktadır. Bunlardan birincisi; düzenlemelerin hangi yöntem ve kapsam ile yapılması durumunda ifade ve bilgiye erişim özgürlüğünü de kapsayan “insan hakları ve demokrasi” ile bağdaşabileceği, ikincisi; düzenlemelerin hangi yöntem ve kapsamla yapılması durumunda İnternetin dağıtık ve dinamik özgün yapısına daha çok uyum sağlayacağı konusundadır.

“Yöntem” konusunda; içerik düzenlemelerinin nasıl bir yönetsel yaklaşımla ele alınması gerektiği, öngörülen önlem ve müdahalelerin kim/kimler tarafından, nasıl bir mekanizma ile yapılmasının uygun olacağı, “kapsam” konusunda; düzenlemelerin sınırlarının ne olacağı ve hangi konuları içereceği konuları tartışılmaktadır.

“Yöntem”e ilişkin temel görüş ayrılığı, içerik düzenlemelerinin doğrudan devlet eliyle mi, yoksa sivil inisiyatif tarafından mı, ya da her ikisinin birlikte mi yapmasının ve uygulamasının uygun olacağı noktasında ortaya çıkmaktadır. Bir kesim devlet eli ile yapılan her tür doğrudan veya dolaylı düzenlemeye kökten karşı çıkarken, bunun İnternetin özgürlükçü doğasına aykırı olacağını ileri sürmektedir. Bu görüşe göre, İnternetin kendine özgü yapısından ve teknik özelliklerinden dolayı devletler İnterneti düzenlemekte etkisiz ve yetersiz kalacaktır. Keza, İnternet içeriğine ilişkin

hükümetlerin yapacağı her tür düzenleme ifade, bilgi ve düşüncenin serbest dolaşımı, bilgiye erişim gibi özgürlüklere sınırlama getirme ve sansüre sebep olma riski taşır.

Ayrıca, her devletin İnterneti kendi yaklaşım ve önceliklerine göre düzenlemesi ve kontrol etmesi, ülke adedince farklı “İnternet” ortaya çıkaracağı için İnternetin küresel ağ olma özelliğini sona erdirecektir. Bu nedenle, konu kendi araçları ve kendi kuralları ile çözmek üzere tamamen kullanıcılara, sivil topluma ve sektörün öz düzenleme girişimlerine bırakılmalıdır. Bu yöntem, İnternetin kendine özgü doğasına ve teknik özelliklerine uyumlu uygulamalar geliştirecek, teknik ve operasyonel eksiklikleri en aza indirecektir.

Bu görüşün aksine, devletleri içerik düzenlemelerinin dışında tutmayı gerçekçi bulmayanlar; özgürlük fikrinin “kuralsızlık” anlamına gelmeyeceğine, bilakis özgürlüğün teminat altına alınmasının da kuralları gerekli kıldığına işaret etmektedir. Ayrıca, hükümetlerin ulusal çıkarları ve değerleri korumaları için düzenleme yapılması kaçınılmaz görülmektedir. Bu kapsamda, devletin öncelikli görevinin vatandaşların maddi ve manevi varlığını koruyabileceği ve geliştirebileceği ortamı hazırlamak olduğunu; dolayısıyla, İnternetin her türlü hukuka aykırı, zararlı ve sakıncalı içerikten arındırılması gerektiği dile getirilmektedir. Keza, devletin genel ahlakı ve aileyi koruma görevine de dikkat çekilmektedir.

Kimileri de bu alanın, kamu/sektör/sivil toplum ilgili tüm tarafların katılım sağladığı bir mekanizma ile ortaklaşa düzenlenmesi ve yönetilmesi görüşünü savunmaktadır. Bu yaklaşımda, içerik düzenlemelerinde devletin otoriter gücünün gerekliliği kabul edilmekle beraber, İnternetle ilgili problemlerin çözümünde İnternetin küresel ve merkezi olmayan, dağıtık ve dinamik yapısı nedeniyle devletin yetersiz kalacağı görüşü dile getirilmektedir. Bu yüzden, bir yandan ulusal ölçekte İnternet’in çok taraflı yönetimi anlayışıyla hareket ederken, diğer yandan ulusal düzeydeki politikaların geliştirilmesinde uluslararası yetki konularının dikkate alınması ve bu politikaların uluslararası düzeydeki gelişmeler ışığında birleştirilmesi ve koordinasyonunun sağlanması gerekmektedir.

İçerik düzenlemesinin “kapsam”ı konusun da ise; yasadışı ve zararlı olarak kabul edilerek mücadeleye konu edilecek içerik türlerinin neler olacağı ve özellikle erişim engellemeye veya filtrelemeye konu olan hususların sınırları tartışılmaktadır. Bu kapsamda, içerik düzenlemesinde çerçeveyi geniş tutma eğiliminde olan ve çok sayıda içerik türünü düzenleme konusu yapmayı savunan görüşler ve uygulamalar içinde olan devletler daha fazla “sansürcü” nitelemesine muhatap olmaktadır. Demokratik değerlere önem veren ülkelerin ise, genel çerçeveyi mümkün olduğunca sınırlı tutarak, sadece önemli gördükleri belirli birkaç hususu içerik düzenlemesine konu edindikleri belirtilmektedir. Nitekim, devlet düzenlemesini gerekli görenlerin bir çoğu sınırlı müdahaleyi özgürlükler ve demokratik değerler açısından en önemli gereklilik olarak öne sürmekte ve düzenlemelerde adil, hesap verebilir ve kamu yararına göre ölçülü ve gerekli olan en az müdahale öngörülmektedir.

Diğer yandan, “İnternet” olgusu karşısında kamu gücünü kullanan ulus devletlerin bir takım zorluklar yaşadıkları da bir gerçektir. Bu zorlukların en önemlisi de İnternetin, klasik ulusal egemenlik anlayışlarına meydan okuyan karmaşık, çok değişkenli, dinamik ve sınır tanımayan küresel yapısıdır. Vatandaşlık, ulusal sınır gibi kavramları hiçe sayan bu teknoloji, devletlerin klasik ulusal egemenlik yaklaşımlarını oldukça zorlamaktadır. Dolayısıyla, İnternet teknolojisi bugün “egemenlik” kavramını yeniden düşünmeye mecbur kılmakta ve İnternetin düzenlenmesi konusu “düzenleme” ve “devletin egemenlik yetkisi” kuramlarının temelden sorgulandığı bir mecraya doğru ilerlemektedir.

Fakat bu durum, uygulamada, devletlerin İnternete hiç müdahalede bulunmadıkları anlamına gelmemektedir. Altıncı alt hipotezimizde de belirtildiği gibi, ilk zamanlarda tamamen bir özgürlük alanı olarak görülen İnternet, günümüzde çeşitli sosyal, kültürel, siyasal, yönetsel veya ekonomik sebeplerle; doğu-batı, güney-kuzey, demokratik-totaliter, gelişmiş-az gelişmiş hemen hemen dünyadaki bütün devletlerin, hatta uluslararası kuruluşların giderek artan bir oranda değişik müdahalelerine ve düzenlemelerine muhatap olmaktadır. Bugün, İnternet yelpazesinin aşırı uçlarının kontrolü her devlet için büyük önem arz etmektedir.

Aynı şekilde, sekizinci alt hipotezde belirtilen; İnternet içerik düzenlemelerinin “ifade ve bilgiye erişim özgürlüğü” ve İnternetin çok yönlü/aktörlü ve dinamik özgün yapısıyla uyum içinde olması gerektiğine ve düzenlemelerde “sınırlı müdahale” nin tercih edilmesinin, bu iki kritere uygunluğu sağlama konusunda en elverişli yaklaşım tarzı olacağına ilişkin tespit, yukardaki değerlendirmelerden ortaya çıkan sonuç ile paralellik göstermektedir.

7. Dünya uygulamaları, ülkelerin ekonomik, teknolojik, kültürel gelişmişlik düzeylerine, sosyolojik ve siyasal kodlarına, inanç haritalarına göre İnternet politikalarının farklılık gösterdiğini ortaya koymaktadır. Başka bir deyişle, bazı ortak noktalar bulunmakla birlikte, ülkelerin kendilerine özgü özelliklerine göre, içerik düzenleme politikaları, kullanılan araçlar, yöntemler, teknikler ve kriterler, düzenlemelerin kapsamı, uygulamalara ilişkin süreçler farklılık arz etmektedir.

Nitekim, Avustralya, Türkiye ve Singapur gibi bazı ülkeler içerik güvenliğine ilişkin önlem ve müdahalelerini konuya özel genel kapsayıcı yasal düzenleme yaparak gerçekleştirirken, AB üyesi Almanya, Belçika, Yunanistan, İrlanda ve İspanya gibi bazı ülkeler de bunun yerine “gerçek hayatta suç olanın çevrimiçi ortamda da suç sayılması” prensibinden hareketle mevcut yasalarını İnternete uyarlayarak sonuç almaya çalışmaktadır. Ülkelerin büyük çoğunluğu ise, hem mevcut yasalarını İnternete içeriklerine göre revize ederek hem de belirli bir tür içeriğe özel yasalar çıkartarak parçalı ve değişik düzenlemeler yapmayı tercih etmektedir. Keza, ABD, Kanada, Brezilya, Japonya, Rusya, Güney Kore yanında, AB üyesi İngiltere, Fransa, İtalya, Danimarka, Hollanda ve Finlandiya bu ülkelerdendir.

Devletleri bu alanda düzenleme yapmaya bazen ulusal güvenlik konularında duyulan endişeler (terörizm, ırkçılık ve ayrılıkçılık vb.), bazen ise, İnternette yer alan kimi içerikler karşısında toplumların ve devletlerin, kendi geleneksel, tarihsel, kültürel, sosyal, siyasal, dinsel ve ahlaki değerlerine ilişkin taşıdıkları kaygılar itmektedir. Kimi zaman da İnternetteki devletle ilgili değer yargılarına yönelik hakaret içeren ifadeler, rejim, resmi ideoloji aleyhtarlığı yapılması gibi kurulu siyasal sisteme ve siyasi istikrara zarar verecek içeriklerden duyulan rahatsızlıklar etkili olmaktadır.

Söz konusu nedenlerle dünyadaki birçok ülke farklı konularda içerik düzenlemesi gerçekleştirmiştir. Ülkeler ve uluslararası kuruluşlar, bazı istisnalar dışında, genelde ortak görüş olarak çocuk pornografisi ve cinsel istismarı ile telif haklarına ait içerikler yanında çocukların pornografik içerikten korunması konularında uzlaşmaya varmış gibi gözükmektedir. Bunlar dışında en çok düzenlemeye konu edilen içerik türleri ise ekstrem pornografi (ensest, ölü sevicilik, hayvan vs.), ırkçılık ve ayrımcılık, nefret ve şiddet içerikleri, online kumar, intihara ve uyuşturucu kullanmaya teşvik gibi konulardan oluşmaktadır. Genellikle de devletler ülke vatandaşlarını özellikle çocukları ve gençleri bu tür içeriklerden korumak amacıyla söz konusu içeriklerle mücadele etme yoluna başvurmaktadır.

Nitekim, diğer bir çok ülkenin yanında AB üyesi İngiltere, Almanya ve Fransa ekstrem pornografiyi yasak içerik kapsamında değerlendirirken, Avustralya, Japonya, Güney Kore, Çin, Suudi Arabistan ve İran gibi bir çok ülke her tür müstehcen ve pornografik içeriği yasadışı olarak kabul etmiştir. Son dönemde AB’nde ve özellikle İngiltere ve İzlanda gibi bazı üye ülkelerde yetişkin pornografisi konusunda politika değişikliğine gitme yönünde bazı işaretler görülmektedir. Önce, İzlanda’da başlayıp diğer üye ülkelere yayılan ve sonunda AB’nin karar organlarına taşınan pornografinin özellikle kadınları “cinsel özne” olarak kullandığı, cinsiyet ayrımcılığını körüklediği ve kadına yönelik cinsel şiddeti artırdığı yönündeki tartışmalar, bu tür içeriklere karşı tedbir alınmasını gündeme getirmiştir.

İrkçı ve ayrımcı, nefret ve şiddet içerikleri de özellikle başta Almanya, İngiltere, Fransa, Avusturya olmak üzere birçok AB üyesi ülkelerde ve Avustralya, Brezilya ve Rusya’da yasadışı içerik düzenlemelere konu edilmiştir. Keza, online kumar, bahis ve şans oyunları ABD, Avustralya, Fransa, Almanya ve Güney Kore yanında Çin, İran ve Suudi Arabistan’da yasaktır. Yine, uyuşturucu kullanmaya teşvik içerikleri; Avustralya, İspanya, İtalya, Bulgaristan, Rusya, Japonya, Güney Kore, Çin, İran ve Suudi Arabistan’da, intihara yönlendirme içerikleri; Almanya, İtalya, Rusya, Yunanistan, Bulgaristan, Japonya, Güney Kore, Çin, İran ve Suudi Arabistan gibi ülkelerde yasadışı olarak kabul edilmiştir.

Bunlar dışında ülkelerin ulusal güvenlik ve terörizm ile mücadele gerekçesiyle anti-terör yasaları çıkartarak içeriklere müdahale ettikleri veya İnternet trafiğini izlemeye aldıkları görülmektedir. Bu çerçevede ABD'nin sadece ülkesindeki değil, tüm dünyadaki telefon ve İnternet trafiğini takip ettiği ve müdahalede bulunduğu bilinmektedir. Keza, İngiltere, Fransa ve Rusya kendi vatandaşlarına yönelik olarak benzer faaliyetler gerçekleştirmektedir. Yine, bazı devletlerin bir takım siyasal kaygılarla yaygın filtreleme yaptıkları ve İnternet içeriklerini kontrol altına almaya çalıştıkları da görülmektedir. Örneğin, Çin, komünizme karşı tehdit olarak gördüğü içerikle, Suudi Arabistan, İran ve Suriye rejim aleyhtarı içerikle, Güney Kore, Kuzey Kore propagandasına ait içerikle mücadele etmektedir.

Bununla birlikte kimi ülkelerin kendilerine özel bazı gerekçelerle farklı içerik türlerine karşı önlem geliştirdikleri de görülmektedir. Örneğin, Brezilya eşcinsel düşmanlığı, hayvanlara kötü muammele ve insan kaçakçılığı içeriklerini zararlı ve yasadışı olarak kabul etmiştir. Keza, Çin ve Güney Kore İnternette spekülasyon bilgisi ve haber yaymayı yasaklamıştır. Yine İran; İsrail veya ABD'yi iyi gösteren veya öven, ateistliği teşvik eden, İslami kurallara zarar veren, lüks ve savurganlığı teşvik eden yayınları, Arabistan; alkol ve büyücülük içeriklerini engellemektedir.

Ayrıca, Güney Kore ve Singapur'da seçim yasalarıyla seçim dönemlerindeki İnternet yayınları için özel düzenlemeler getirilmiştir. Bu kapsamda, Güney Kore Seçim Yasası, seçim dönemlerinde politikacıların ve kampanyaların karalanmasını yasaklamak amacıyla, bilgi ve iletişim ağları üzerinden yapılan kampanya aktivitelerine kısıtlamalar getirmektedir. Singapur'da ise, seçim dönemlerinde web sitelerin siyasi parti reklamlarını yayınlamaları, aday tanıtımında bulunmaları ve her türlü seçim anketi yapmaları yasaklanmıştır.

Diğer yandan, bazı uluslararası kuruluşların da İnternet kaynaklı kullanım ve içerik güvenliği sorunlarına karşı bir takım uluslararası belgeler yayınladığı görülmektedir. Avrupa Konseyi Siber Suç Sözleşmesi bunlardan birisidir. 2001 tarihli Sözleşme, daha sonra yapılan ek protokol de dahil olmak üzere telif hakkı ihlalleri, bilgisayarlarla ilişkili sahtecilik fiilleri, çocuk pornografisi, ırkçı ve yabancı düşmanı

eylemler ve ağ güvenliği ihlallerine ilişkin hükümler getirmiştir. Siber Suç Sözleşmesi, İnternet ve diğer bilişim ağları aracılığı ile işlenen suçlara yönelik ilk ve tek uluslararası sözleşme olması nedeniyle tarihsel öneme sahiptir.

Keza, AB de İnternetteki zararlı ve yasa dışı içeriklerle mücadele konusunda aktif bir yaklaşım sergilemektedir. Bu çerçevede bir yandan üye ülkelere yol gösterecek konuya ilişkin çerçeve kurallar oluşturmaya çalışırken, diğer yandan İnternetin kendine özgü niteliklerini göz önünde bulundurarak esnek, uygulanabilir ve sonuç almaya yönelik içerik düzenleme politikaları geliştirmeyi amaçlamaktadır. AB hukuka aykırı ve zararlı içeriğe müdahalede belirli koşullar altında ifade hürriyetini korumaktan daha baskın bir kamu yararı olduğunu kabul etmektedir.

Bu bağlamda AB, İnternet ortamındaki sakıncalı içeriği “hukuka aykırı” ve “zararlı” içerik şeklinde ikiye ayırmaktadır. Birlik, çocuk pornografisi ve cinsel istismarına, ırkçılığa ve teröre dair içerikleri hukuka aykırı içerik olarak kabul ederek suç kapsamına almakta ve cezai düzenleme yapılmasını istemektedir. Zararlı içerik ise, yayınlanması suç olmamakla birlikte, 18 yaşından küçüklerin pornografik veya şiddet yer alan içeriğe ulaşmalarının engellenmesi gibi bazı kısıtlayıcı hükümler getirilmiş olan içeriği ifade etmektedir. AB, zararlı olarak kabul edilen içeriklere ilişkin mücadeleyi gerekli görmekle birlikte cezai bir düzenleme yapılmasını üye devletlerin inisiyatifine bırakmıştır. Diğer yandan, AB, e-ticaret ve bilgi güvenliği ile telif hakkı ihlallerine ilişkin yasal düzenlemeler öngörmektedir.

BM ise, 1989 tarihli Çocuk Haklarına Dair Sözleşme’den sonra çocukların cinsel istismarı ve sömürülmesi konusunda daha etkin olunması için 25.05.2000 tarihinde Çocuk Haklarına Dair Sözleşmeye Ek Çocuk Satışı, Çocuk Fahişeliği ve Çocuk Pornografisi İle İlgili İhtiyari Protokol’ü kabul etmiştir. Protokolün temel amacı çocuk satışı, çocuk fahişeliği ve çocuk pornografisini önlemektir. Bu çerçevede, Protokolü kabul eden devletlerin bu fiilleri iç hukuklarında suç olarak kabul etmelerini zorunlu kılmakta ve suçların tanımı, bu suçlarla mücadeleye ilişkin uluslararası işbirliği, devletlerin yargılama yetkisi, suçluların iadesi ve ceza yargılamasına ilişkin temel ilkeler gibi konuları düzenlemektedir.

Sonuç olarak, yedinci alt hipotezde savunulduğu gibi, bazı ortak noktalar bulunmakla birlikte, tarihsel, sosyal, siyasal özellikleri, demokratiklik düzeyleri, ekonomik ve teknolojik gelişmişliklerine göre; önlem alınan içerik türü, gerekçeleri, yöntemi, ölçütleri ve sonuçları bakımından ülkeler oldukça farklı uygulamalara sahiptir.

9. İnternet içeriğinin düzenlenmesi konusunda dünyada farklı yönetsel yaklaşımlar uygulanmakta ve bu yaklaşımlar değişik boyutları ile tartışmalara konu olmaktadır. İçerik düzenlemesine ilişkin temel yönetsel yaklaşımlar, devlet düzenlemesi (government regulation), kendi kendine/öz düzenleme (self-regulation) ve birlikte/ortak düzenleme (co-regulation) olarak sıralanabilir.

Devlet düzenlemesi yaklaşımında kamu otoritesi, konuyla ilgili düzenleme yapma yetkisini tekeline alarak, yetki verdiği bazı kamu kurumları eli ile söz konusu içeriklerle kamu gücünü kullanarak doğrudan mücadele etme yöntemini tercih etmektedir. Bir takım eleştirilere neden olsa da, İnternet içeriğinin bu nevi doğrudan ve aktif devlet müdahalesiyle kontrol altına alınmaya çalışılması ve farklı amaçlarla İnternetin kısıtlanması sıkça görülen bir uygulamadır.

Bu yönetsel yaklaşımda devletlerin farklı yöntemler ve uygulamalar geliştirdikleri göze çarpmaktadır. Bazı devletler temel prensip olarak İnternet içeriğine doğrudan müdahale etmeksizin vatandaşların hukuki veya cezai sorumluluğunu esas alırken, bazıları ise içeriğe müdahale etmeyi ön plana çıkarmaktadır. Bu çerçevede, her devlet farklı sorumluluk esaslarına göre İnternet kullanıcıları, içerik, yer ve erişim sağlayıcıları ve diğer aktörlerin hukuki ve cezai sorumluluklarını düzenlemektedir.

Yöntemi ne olursa olsun, devlet düzenlemelerinin uygulanabilir, inanılır, açık ve saydam olması, düzenleyici kuruluşlara sınırlı takdir yetkisi vererek keyfiliği önlemesi gerekmektedir. Nitekim, Rusya, Çin, Güney Kore, İran ve Suudi Arabistan gibi ülkeler yanında diğer bazı üçüncü dünya ülkeleri ve özellikle Asya kıtasında görülen, doğrudan devlet otoritesinin egemen olduğu kurumların yönetiminde gerçekleştirilen içerik düzenlemesi uygulamalarında, genellikle katı bir müdahale yönteminin tercih edildiği ve kapsayıcı önleyici tedbirlerin alındığı görülmektedir.

Kendi kendine/öz düzenleme, genel olarak her iş dalı veya sektörün kendi kural ve davranış ilkelerini kendisinin belirlemesi, kendi kendini düzenlemesidir. Burada hem öz denetim hem de davranış kuralları sektör içindeki firmalarca belirlenmektedir. Öz düzenleme, zorunlu olmamakla birlikte, bu ortak kurallara uymaya karar veren sektör mensuplarının getirilerini katılanların paylaştığı bir “gönüllülük” hareketidir.

İnternet ortamının kurallarını belirleme ve önlem alma eğilimi, bazı ticari kaygılar ve beklentiler nedeniyle, İnternet sitelerini ve sosyal ağları yöneten birçok büyük firma, İSS’lar, yer ve erişim sağlayıcılarca da benimsenmektedir. Bu yüzden, bu aktörler gönüllülük esasına göre örgütlenmekte ve öz düzenlemenin temel araçları olan içerik filtreleme, derecelendirme ve ihbar merkezi uygulamalarını hayata geçirmektedir.

Nitekim, AB’nin içerik düzenlemesine ilişkin yayınladığı belgelerde “öz düzenleme” vurgusu göze çarpmaktadır. Bu kapsamda Avrupa ülkelerinde genelde filtreleme ve erişim engellemesi, öz düzenleme çerçevesinde, konuya ilişkin açık bir mevzuat düzenlemesi olmaksızın sivil toplum, polis ve İSS işbirliği ile “gönüllülük” esasına göre yapılmaktadır. Fakat, hükümetlerin, sektör temsilcilerini, içerik düzenlemeleri ile ilgili “zorunlu gönüllü” işbirliği yapma konusunda gayriresmi oluşturdukları baskılar ile zorladıkları da bir gerçektir. Hükümet temsilcilerinin, “gönüllülük” esasını tesis edilemediği taktirde başka yaptırımların uygulanacağına yönelik beyanları, İSS’ları gerekli tedbirleri “zorunlu gönüllü” olarak uygulamaya itmektir.

Keza, böylece, gerçekte birçok ülkede farklı şekillerde ve genellikle şeffaf olmayan yöntemlerle erişim engellemesi uygulandığı, bu uygulamaların genellikle idari birimler tarafından oluşturulan kara listelerin erişim sağlayıcılara gönderilmesiyle gerçekleştirildiği görülmektedir. Örneğin, İngiltere’de çocuk pornografisi ve ırkçılıkla mücadele eden IWF’un üst düzey yöneticilerini emekli emniyet mensupları oluştururken, bünyesinde hiçbir hukukçu barındırmamasına rağmen oluşturduğu kara listeler, İngiltere’deki tüm erişim sağlayıcılar tarafından “gönüllü” olarak kullanılmaktadır. Benzer şekilde Kanada, Avustralya, Rusya, Almanya, Fransa, Danimarka, İsveç, Finlandiya ve Norveç’te İSS’lar, Polis teşkilatları veya ilgili idari birimlerin sağlamış oldukları kara listelere erişimi engellemektedir.

Keza, ABD’de de İnternet ortamında işlenen çocukların cinsel istismarı gibi belirli suçlara yönelik önleyici tedbirler alınması amacıyla, farklı adlarla da olsa sektörün içinden aktörlerin öz düzenleme yaklaşımıyla oluşturdukları yapıları teşvik etmektedir. Bu yapılar, genelde bağımsız ve özerk, fakat dolaylı olarak hükümetlere bağlı olarak içerik düzenlemesi faaliyetleri yapmaktadırlar.

Özellikle çocukları İnternetin zararlı içeriğinden korumak için İnternet sitelerine etiket vermek suretiyle derecelendirmesini sağlayan İnternet derecelendirme sistemi, siteleri kategorilere ayrılmakta ve ebeveynlerin site erişimlerine ilişkin kararlarına kaynaklık etmektedir. Kategorizasyon genellikle, değerlendirme (örneğin; çıplaklık, cinsel içerik, şiddet) ya da işaretler (farklı abonelerin ilgi ve uğraşlarına göre içeriğin belirlenmesi) gibi farklı bilgi tiplerine dayanmaktadır. Bu yönüyle yapılan işlemin, İnternet sitelerini düzenlemek ve İSS’ların müdahalesi olmaksızın içeriğin kontrol edilmesini sağlamak şeklinde önemli bir görev üstlendiği söylenebilir.

AB’inde İnternet İçerik Seçimi Platformu ve dijital oyun sektöründe Pan-Avrupa Oyun Danışma Kurumu öz düzenleme uygulamasıdır. ABD’de ESRB, İngiltere’de ise Birleşik Krallık İnteraktif Eğlence Ortaklığı, dijital oyun sektörünün öz düzenleme kuruluşu olarak oyunları içeriklerine göre sınıflandırmaktadır. Avustralya’da ise tüm yayın türlerini düzenleyici kurum olan Sınıflandırma Kurulu tarafından değerlendirilmektedir. Almanya’da da BpJM, Rusya’da Roskomnadzor, Güney Kore’de Medya Derecelendirme Kurumu bir kamu kurumu olarak içerikleri endekslemekte, kategorizasyon, derecelendirme ve işaretleme yapmaktadır.

İhbar merkezi uygulaması, öz düzenleme yaklaşımında kullanıcıların şikayetleriyle İnternet içeriğinin denetlenmesini ve yasa dışı içeriğin sunuculardan kaldırılmasını sağlayan önemli bir araçtır. Nitekim, 1999 tarihli İnternet Eylem Planı gereği hem AB nezdinde hem de her ülke kendi bünyesinde içerik takip eden ve sakıncalı içeriğe ilişkin ihbarlar alan merkezler kurulmuştur. Yine, bazı STK’ları ve devletlerin işbirliğiyle, dünya genelinde faaliyet gösteren ihbar merkezleri arasında iletişim ve işbirliği sağlamak maksadıyla INHOPE gibi ana ihbar merkezleri kurulmuştur.

Birlikte düzenleme olarak adlandırılan yönetim modelinde ise, kamu kurumları, sektör temsilcileri ve STK'ları işbirliği yaparak, birlikte kuracakları bir mekanizma ile İnternet içeriğini düzenlemektedir. Böylece, “devlet” ve öz düzenlemenin birlikte uygulanabileceği ve birbirini destekleyebileceği bir ortak zeminde her iki yaklaşımın tek başına uygulanmasından kaynaklanan dezavantajlar bertaraf edilecek ve avantaja çevrilecektir. Birlikte düzenleme konusunda iki farklı yaklaşımdan bahsedilmektedir. İlkinde, özel sektör tarafından oluşturulan öz düzenlemenin devlet tarafından kontrol edilmesi ve onanması şekliyle bir birlikte düzenleme öngörülürken, diğerinde, özel sektör ile devletin sorumluluk paylaşımına giderek kendi alanlarında kurallar oluşturması usulüyle bir birlikte düzenleme anlayışı söz konusudur.

Nitekim, ABD ve AB ülkeleri de dahil olmak üzere İngiltere, Fransa, Almanya, Brezilya ve Japonya gibi bir çok demokratik ülkenin öz düzenleme uygulamalarına önem vermekle birlikte gerçekte daha çok birlikte düzenleme yöntemine göre hareket ettiği görülmektedir. Örneğin, AB içerik düzenlemesi uygulamalarında göze çarpan “zorunlu gönüllülük” gerçeği, AB’nin konuya ilişkin genel yönetimsel yaklaşımının öz düzenleme yönünde olduğu şeklindeki görüşü zayıflatmaktadır. Belki şekilsel olarak öz düzenlemeye uygun bir yapı var gibi gözükse de, arka planda kamu kurumlarının doğrudan veya dolaylı olarak etki ve yönlendirmede bulundukları, hatta ince yollu tehditlerle istikamet belirledikleri bu tür yapıların öz düzenleme yaklaşımının ruhuna ve özelliklerine uygun düşmeyeceğini söylemek mümkündür.

Sonuçta, sakıncalı İnternet içeriğiyle ilgili olarak devletlerin tek başlarına yeterli düzenlemeler yapmaları mümkün gözükmemektedir. Özellikle, yasal düzenlemeler her ne kadar var olan sorunların çözümünde en önemli belirleyici faktör olsa da, çağın gereği, bu alanda devletin tek başına düzenleme yapması yerine; daha demokratik yaklaşımlarla hareket etmesi, işbirliği, koordinasyon, danışma, birlikte düzenleme ve öz düzenleme gibi yeni konulara da önem vermesi gerekmektedir.

Keza, İnternet gibi “ele avuca sığması” zor olan bir varlığın doğuracağı riskleri sadece tek bir aktörle, yani devlet eliyle yönetilmesinin mümkün olmayacağı bilinmektedir. Çözümün, kurumlarıyla beraber başta devlet olmak üzere aile, ilgili

STK'ları, özel sektör kuruluşları ve okul/üniversite gibi diğer tüm paydaş aktörlerin İnternetin doğurduğu risk ve tehditleri yönetmede sorumluluk alması, katkıda bulunması ve işbirliği geliştirmesiyle mümkün olacağı görülmektedir.

Bu perspektifle ele alındığında, dokuzuncu alt hipotezde ortaya konulan hususun doğruluğu açığa çıkmakta; İnternet içeriğinin düzenlenmesi ve yasadışı ve zararlı içerikle mücadele konusunda, birlikte düzenleme yöntemini de içine alan yönetim modelinin sonuç alma noktasında en etkili yönetsel araç olduğu görülmektedir.

10.,11.,12. Ülkeler, İnternetin güvenli kullanımı ve yasadışı ve zararlı içeriklerle mücadele etmeye yönelik faaliyetlerinde farklı yöntemler kullanmaktadır. Bu yöntemleri filtreleme ve erişim engelleme yöntemleri ile bunların dışında kalan uyar-kaldır, özel anlaşmalar yapma, bilinçlendirme ve İnternet etiği çalışmaları ve pozitif içerik oluşturma yöntemleri olarak sayabiliriz.

Devletlerin suç algılaması, ekonomik ve teknolojik gelişmişliği, insan hakları, demokrasi ve hukuk devleti konusundaki hassasiyetleri içerik politika ve uygulamalarının çerçevesini belirlediği gibi, müdahalenin yöntemi ve kapsamını da değiştirebilmektedir. Bu etkenlere bağlı olarak, İnternet erişimini engellemede kullanılan teknikler, engelleme süresi, engelleme öncesi ve sonrası takip edilen süreçler, engelleme kapsamı devletten devlete değişmektedir. Bazı devletler bir tek yöntem kullanırken, bazıları birden çok yöntemi kombine şekilde kullanabilmektedir. Hatta bazıları hukuk dışı müdahale ve yöntemlere dahi başvurabilmektedir. Örneğin, adına “Siber Çin Setti” de denilen filtreleme sistemiyle Çin, tüm İnternet sitelerinin filtrelenmesinin kapsamlı ve karmaşık bir uygulamasını yapmaktadır.

Başlıca erişim engelleme yöntemlerini, genel olarak engellemenin kapsamı ve kullanılan teknikler bakımından ikiye ayırabiliriz. Engellemenin kapsamına göre, engelleme, İnternet ağı içerisinde bulunan İnternet omurgası, İSS'lar, kurumlar ve kişisel bilgisayarlar üzerinde yapılabilmektedir. Devletler, web sitelerine erişimi İSS'lar nezdinde engelleyebileceği gibi ana İnternet omurgası üzerinden tek aşamada tüm ülke genelinde de engelleyebilirler. Devletlerin bu konudaki tercihlerini, coğrafi

büyüklikleri, ülkede faaliyet gösteren İSS'ların sayısı, telekomünikasyon sektörünün özel sektöre açık olup olmaması gibi etkenler belirlemektedir.

Engellemede kullanılan tekniğe göre yaygın olarak kullanılan başlıca yöntemler şunlardır: IP'den engelleme, alan adından engelleme, URL'den engelleme, Proxy engellemesi, içerik engellemesi, DDOS atakları, alan adı iptaliyle engelleme, fiziksel sunucu müdahalesi yoluyla engelleme ve ağ hatası gösterme yoluyla engelleme.

Bunlar dışında devletler, bazı nedenlerden dolayı doğrudan filtreleme ve engelleme yapmak yerine, bir takım başkaca sosyal ve ekonomik yöntemler kullanarak erişimi fiilen zorlaştırmakta veya kullanıcıların oto-sansür uygulamalarını sağlamaktadır. Bireysel davranışlar üzerinde etkinlik kurularak sonuç alınmaya çalışıldığı için bu yöntemler sosyal teknikler olarak adlandırılmaktadır. Örneğin Çin ve Güney Kore bu yöntemi en iyi kullanan iki ülkedir.

Erişim engellemeye ilişkin kullanılan her bir tekniğin kendi içinde güçlü ve zayıf yönleri bulunmaktadır. Örneğin basit ve maliyetsiz olmakla birlikte IP ve alan adı engellemesi, istenmeyen içerik yanında masum içeriklere de otomatik olarak engelleme sonucunu doğurmaktadır. Çünkü, IP veya alan adı engellendiğinde o IP'den veya alan adından yayın yapan tüm içerikler engellemeye uğramaktadır. Bu durum cezada şahsılık ilkesinin ihlaline neden olmaktadır. Buna mukabil, erişimi engellenen içeriği barındıran sunucun değiştirilmesi veya alan adındaki küçük bir değişiklik engellemeyi aşmaya yeteceği için çokta kullanışlı bir yöntem değildir.

Bu tür mahzurların giderilebilmesi için sadece ilgili sayfayı engellemeyi esas alan URL yoluyla engelleme daha kullanışlı gözükmemektedir. Fakat, bu yönteminde bazı dezavantajları vardır. İnternet trafiğini yavaşlatmakta ve ekstra yatırım yapmak ve fazladan insan kaynağı ayırmak gibi mali külfetler getirmektedir. Ayrıca, bir sunucu üzerinden yayınlanan yasaklı URL adresinin birkaç saniye içinde değiştirilerek erişim engellemeden kurtulabilmesi bu yöntemin etkinliğini azaltmaktadır.

Bu ve benzeri nedenlerle giderek artan eğilim, birkaç yöntemi birlikte daha sofistike ve kombine teknikler kullanarak daha fazla yerde ve daha fazla engelleme yapmak

yönündedir. Fakat bu durumda dahi filtreleme ve erişim engellemede yüzde yüz başarılı bir teknik bulunamamıştır. Dünyanın en gelişmiş filtreleme ve erişim engelleme sistemlerine sahip olan Çin ve S. Arabistan devletleri bile birçok içeriği engellemede başarısız olmaktadır. İnternet içeriğinin hızla değişmesi ve değişik web sitelerine yayılması çoğu zaman engellemeyi olanaksız kılmaktadır. Keza, her bir teknik engelleme ilgisiz web sitelerini engelleyebileceği için aşırı engelleme veya tam aksine ilgili web sitelerini engelleyememe nedeniyle de etkisiz engelleme riski taşımaktadır. Bu nedenlerle devletler kullandıkları teknolojinin mükemmel olmasından ziyade etkili olmasına önem vermektedir.

İnternette filtreleme ve erişim engellemeler yaygın hale geldikçe, bunları aşabilmeyi sağlayan araçların geliştirilmesi ve kullanılması da hız kazanmıştır. Dolayısıyla, erişim engelleme teknolojileri ne kadar hızlı geliyorsa, engellemeleri aşacak teknolojiler de aynı hızda gelişmekte; web sitelerinin erişimleri değişik teknikler kullanılarak engellenirken, engellemelerin aşılmasında da bunlara mukabil farklı teknikler uygulanmaktadır. Yine, engelleme yöntemleri kombine şekilde kullanıldığı gibi engellemeleri aşma yöntemleri de kombine olarak kullanılabilir.

Erişim engellemesini aşmada, temel prensipleri hedefi ve paketin içeriğini gizlemeyi içeren pek çok teknolojik yöntem kullanılmaktadır. Bu yöntemlerin en önemlileri, IP değiştirme yöntemi, alan adı sunucusu değiştirme yöntemi, URL gizleme yöntemi, proxy kullanma yöntemi, içerik aldatması yöntemi, kopya içerik kullanımı yöntemi ve önbellek kullanımı yöntemi'dir.

Diğer yandan, erişim engellemelerini aşma gayretleri, İnternet kullanıcılarının demokratik mücadelelerini ve politik baskıya karşı bilgi alışverişinde bulunmalarını desteklemek açısından sempatik gelse de, kullanıcıların çocuk pornografisi, ırkçılık, ayrımcılık, şiddet, kumar, uyuşturucuyu ve intiharı teşvik gibi içeriklere ulaşmasını sağlamaya yönelik olunca oldukça rahatsız edici olmaktadır. Zira, ülkelerin haklı gerekçelerle mücadele ettiği ve engellediği bu tür içeriklere erişimi sağlayan söz konusu tekniklerin kullanılmasını her zaman ve her şartta yerinde ve meşru görerek sansüre karşı yürütülen özgürlük mücadelesi gibi savunmak doğru olmayacaktır.

Nitekim, bilişim şirketlerinin katı sansür uygulayan ülkelere İnternet içeriğini filtreleyen ürün ve hizmetler sunması eleştirildiği gibi, meşru sınırlar içerisinde filtreleme ve erişim engellemesi yapılan ülkelere, o ülkenin kullanıcılarına, kısıtlamaları aşma fırsatını sağlayacak araçların dağıtımını gerçekleştiren şirket, şahıs ve kurumlar da aynı şekilde eleştirilmektedir. Bu işi yapanların, erişim engellemesi uygulayan ülke vatandaşlarına engellemeleri aşma fırsatı vermeden önce, söz konusu devletin engelleme rejimini değerlendirmesinin gerekliliğine vurgu yapılmaktadır.

Filtreleme ve erişim engelleme dışında sakıncalı İnternet içeriği ile mücadelede daha sempatik yöntemler de bulunmaktadır. Uyar-kaldır yöntemi bunlardan birisidir. Bu yöntemde sakıncalı içeriğin kaldırılmasına yönelik bildirimler önce içerik veya erişim sağlayıcıya iletilmekte ve içeriğin kaldırılması istenilmektedir. Belirlenen süre içerisinde kararın gereği yerine getirilmezse erişim engelleme kararı uygulanmaktadır. Nitekim, ABD, uyar-kaldır sistemini yasal düzenlemeye kavuşturmuş ilk ülkedir. Brezilya, Avustralya, Japonya ve Singapur yanında, AB'nin e-Ticaret Direktifi gereği İngiltere, Almanya, Avusturya, İsveç, Norveç, Danimarka, Finlandiya ve İtalya gibi AB üyesi ülkelerin birçoğunda bu yöntem uygulanmaktadır.

Yasadışı ve zararlı İnternet içeriği ile mücadelede kullanılan diğer bir yöntem de özel anlaşmalar yapılmasıdır. Bu yöntemde ülkeler, küresel arama motorları, sosyal ağlar ve video paylaşım siteleri ile belli içeriklerle karşılaşıldığında şikayet etme ya da engelleme imkanları getiren özel anlaşmalar yapmaktadırlar. Aynı zamanda ilgili ülkeye özel içerik sunulması da bu özel anlaşmalar ile mümkün olabilmektedir. Örneğin, Jugendschutz ile Youtube yaptıkları özel bir anlaşma ile Nazi içeriklerinin çıkarılması veya Almanya'dan erişiminin engellenmesi konusunda anlaşmışlardır. Brezilya'da Google ile Brezilya Federal Cumhuriyet Savcılığı çocukların cinsel istismarı içeriklerinin Google'ın sosyal ağı Orkut'tan çıkarılması veya filtrelenmesi konusunda anlaşmışlardır. ABD Federal hükümeti Youtube ile yaptığı özel bir anlaşma sayesinde terörizm videolarını hızlı bir şekilde siteden kaldırmaktadır. Bu şekildeki anlaşmalar sayesinde Youtube 20'den fazla ülkede o ülkelere özel yerel kopyalar ile hizmet vermektedir. Dünyanın önde gelen 18 sosyal paylaşım sitesi ile

AB arasında “AB için güvenli sosyal ağlar prensipleri” metni imzalanmıştır. Bu uygulama tüm dünyada giderek yaygınlaşmaktadır.

Yine, yasadışı ve zararlı içerikle mücadelede neredeyse her ülkede kullanılan yöntemlerden birisi de bilinçlendirme faaliyetleridir. İnternetin güvenli kullanımı konusunda en uzun ve en kalıcı önlem olarak ön plana çıkan bilinçlendirme faaliyetleri, zor ve uzun bir süreç gerektiren ancak en az eleştiri alan bir yöntem olarak dünyada yaygın olarak kullanılmaktadır. Bilinçlendirme faaliyetlerinin en temel hedef kitlesi çocuklar ve gençler olmakla birlikte, eğiticiler ve ailelere yönelik bilinçlendirme faaliyetleri de yapılmaktadır. ABD, AB ülkeleri, Avustralya, Rusya, Arjantin ve Brezilya bu konudaki faaliyetleri ile ön plana çıkan ülkelerdir.

İnternetin neden olduğu sorunlara çözüm bulma kapsamında gündeme getirilen konulardan birisi de İnternet etiğidir. İnternet toplumunda, içerik ve yanlış kullanımından ortaya çıkan sorunların birçoğunun aslında aynı zamanda etik sorunlar olduğundan hareketle etik anlayış, İnternet alanında da insanlık değerleri için bir takım tehlikelerle mücadele etmek, korumacılık ve düzenleme anlamında duyulan ihtiyaca cevap verebilecek bir imkan olarak görülmektedir. Nitekim, bu türden ihtiyaçları karşılamak için İnternette “netiquette” olarak adlandırılan ve bizzat kullanıcıların gönüllülük temelinde kendi kendini düzenleme ve denetlemelerini amaçlayan çalışmalar yapılmaktadır. Bu konuda özel çalışma yapan Güney Kore ve Brezilya gibi ülkeler de bulunmaktadır. Diğer yandan, öz düzenleme, bilinçlendirme ve İnternet etiği çalışmalarını birbirinin tamamlayıcısı ve destekleyici unsurları olarak ele almanın ve uygulamanın daha doğru olacağına dikkat çekilmektedir.

İnternetin zararlarından korunmak, yasadışı ve zararlı içeriğin önlenmesi gibi İnternet hakkında olumsuz bir algı oluşturan yaklaşımın değiştirilmesi amacıyla, İnternetin sempatik yönünü ortaya çıkarmak için yeni bir içerik düzenleme yöntemi olarak pozitif içerik oluşturulması konusu yakın dönemde gündeme gelmiştir. Bu çerçevede, AB’nin ve OECD’nin İnternetin risklerinin azaltılmasında, pozitif içerikler ve çocuklara özgü güvenli alanlar oluşturma yaklaşımını ayrı bir önlem olarak ajandasına aldığı görülmektedir. Bu kapsamda, bütçeler ayrılmakta, çocuklara

yönelik web siteleri ve arama motorları ile çocukların yaşlarına uygun içeriklere erişebilecekleri kapalı ortamlar oluşturulmaktadır. Bu süreçte, kamu kurumları, STK'ları ve özel şirketler yer almaktadır.

İçerik düzenlemesinde kullanılan yöntemlerle ilgili olarak gelinen noktada, tezin onuncu alt hipotezinde savunulan hususların doğrulandığı görülmektedir. Zira, hipotezde belirtildiği gibi, filtreleme ve erişim engelleme yöntemleri yasadışı ve zararlı içeriklerle etkili bir mücadele yürütmede etkisiz kaldığı gibi, bir çok sakıncalı durumun oluşmasına da neden olmaktadır. Bunun yerine uyar-kaldır, pozitif içerik oluşturma, büyük firmalarla özel anlaşmalar yapma, bilinçlendirme ve etik çalışmaları gibi daha etkili ve sakıncasız pozitif düzenleme yöntemlerinin tercih edilmesinin daha doğru olacağı ortaya çıkmıştır.

13. İnternet dünyasının en önemli aktörleri olan ABD ve AB'nin hangi tür içeriklere karşı hızlı bir şekilde düzenlemelere gittiğini ve etkin/etkili bir mücadele yürüttüğünü analiz ettiğimizde ilginç bir durumla karşılaşmaktayız. Görülmektedir ki, bu ülkelerde İnternet içerik düzenlemelerinin asıl belirleyici unsuru büyük oranda sermaye, yani para ve piyasa olmaktadır. Nitekim, sınırsız bir özgürlük alanı olarak görülen İnternetin, tüm eleştirilere rağmen, en hızlı ve etkin/etkili şekilde düzenleyici kurallarla kontrol altına alınan/alınmaya çalışılan içerik konularının, büyük sektörlerin menfaatlerini ilgilendiren içerik türlerine ait olduğuna tanık olunmaktadır.

Örneğin, müstehcenlik ve pornografi, hatta çocuk pornografisi gibi özellikle çocuk ve genç kullanıcıların güvenliği ve korunması gerekçesine dayanan içeriklerle ilgili önlem alınmasına yönelik karar alma süreçleri yavaş ve tartışmalı bir şekilde ilerleyip, gevşek uygulamalara konu edilirken, telif hakkı ihlalleri ile online kumar ve bahis gibi ilgili sektörlerin menfaatlerine zarar veren ve sermaye ve rekabetçi piyasanın korunması gerekçesine dayanan içerik düzenlemeleri ve önlemlerine ilişkin kararlar hızla alınıp, katı bir şekilde uygulamaya geçilebilmektedir.

Benzer şekilde devasa boyutlara ulaşan dünyadaki pornografi ve çocuk pornografisi sektörünün bu içeriklerle mücadele edilmesine yönelik etkin/etkili önlemlerin

alınmasına engel olmaya veya bu yönde alınan önlemleri etkisiz ve geçersiz kılmaya çalıştığı ve bunda büyük oranda başarılı olduğu da bilinmektedir. Yani, pornografi piyasasının düzenleme süreçlerine tersinden etki ederek sonuç aldığı söylenebilir. Dolayısıyla, içerik düzenlemelerine ilişkin politika oluşturma, karar verme ve uygulama süreçlerinin küresel kapitalist sistemin kurallarına göre işlediği ve bu süreçleri büyük oranda ilgili piyasa oyuncularının belirlediği iddia edilebilir.

Diğer yandan, piyasanın ve sektörün etkili olduğu bu siyasal ve sosyal yapı içerisinde, içerik düzenlemesi kapsamında hayata geçirilen filtreleme, erişim engelleme, bilinçlendirme, ihbar merkezi, sınıflandırma vb. tedbir ve uygulamalara ilişkin bütçelerin etkili sonuçlar almaya ne kadar yeterli olduğunu da sorgulamak gerekmektedir. Zira, yüz milyar dolarlarla ifade edilen pornografi ve çocuk pornografisi sektörü karşısında milyon dolarlarlık mütevazı bütçelerle bu içeriklere karşı önlem almak ve etkili mücadele yürütmek pek mümkün gözükmemektedir.

Nitekim, ABD’de çocuk istismarı ve pornografisi ile mücadele eden en önemli ve etkili örgüt olan NCMEC’in 2010 yılı bütçesi 52 milyon dolar, AB’nin 1999-2002 “İnternet Eylem Planı” bütçesi 25 milyon ECU, 2005-2008 “Safer Internet Plus Programı” bütçesi 45 milyon Euro ve 2009-2013 “Daha Güvenli İnternet Programı” bütçesi 55 milyon Euro’dur. Yine, 37 ülkeden 43 ihbar merkezi üyesi bulunan INHOPE’un 2012 yılı bütçesi 556.019 Euro’dur. Ne kadar iyi niyetli, gayretli ve efektif girişim ve çalışmalar olursa olsun bu bütçeler ile İnternetteki yasadışı ve zararlı içeriklerle etkin/etkili bir mücadele vermek mümkün değildir.

Keza, bazı uzmanlar, ABD ve Avrupa’da dahil olmak üzere diğer bir çok ülkede yürütülen ihbar merkezli ve bilinçlendirme odaklı güvenli İnternet çalışmalarının İnternette yer alan sakıncalı içeriklerle gerçek anlamda “mücadele etmek” değil de “ediyormuş gibi gözükmek” için yapıldığını iddia etmektedir. Bu iddiaya göre, on milyonlarca site sayısına ulaşan bu içeriklere karşı en fazla yılda binlerle ifade edilen ihbarlarla,¹³⁰ 8-10 çalışanı bulunan ihbar merkezleri ile,¹³¹ göstermelik olarak yılda

¹³⁰ Bkz: ACMA ihbar merkezi, 2011 yılında, 6.043 ihbar almıştır. Bunların 2.123’ü hakkında işlem yapılmıştır. (ACMA, http://www.acma.gov.au/WEB/STANDARD/pc=PC_90105 (9.8.2012);

birkaç yüz siteyi kapatmakla veya basılı ve görsel bilinçlendirme materyallerini yaygınlaştırarak gerçek manada bir mücadele gerçekleştirilemez. Aslında devletler de pekala bunun farkındadırlar fakat, sadece bir şeyler yaptıkları görüntüsü vererek kamuoyu baskısını azaltmayı tercih etmektedirler. Bu nedenle, pornografinin her türü başta olmak üzere İnternetteki yasadışı ve zararlı içerikler her geçen yıl hızla artarken, bu içeriklerin sektörel hacimleri ve ciroları her yıl katlanarak büyümektedir.

Diğer yandan, başta ABD ve AB ülkeleri olmak üzere dünyadaki birçok ülkede ihbar ve bilinçlendirme merkezlerini ve bu tür faaliyetler yürüten yasadışı ve zararlı içeriklerle mücadele eden STK'larını finansal ve teknik olarak en çok destekleyen ve işbirliği yapan özel sektör kuruluşlarının ABD merkezli küresel İnternet firmaları (Microsoft, Yahoo gibi) olduğu görülmektedir. Bu durum bir açıdan, bu firmaların yasadışı ve zararlı içeriklerle mücadele konusundaki iyi niyetli yardımları olarak değerlendirilebilir. Fakat, başka bir açıdan, bu firmaların bu finansal ve teknik destek ve işbirliği girişimleri üzerinden bahsi geçen içeriklerle mücadeleyle ilgili çalışmalarını dolaylı olarak yönlendirme, kontrol ve denetim altında tutma çabası olarak da yorumlanabilir. Yani, bu tür yardımlar ve işbirlikleri, sektörün sakıncalı içerikle ilgili mücadelede ön alma, etkin ve belirleyici olma girişimleri olarak değerlendirilebilir.

Keza, birçok ülkedeki İnternet sektörünün öz düzenleme girişimlerini de bu kapsamda değerlendirmek mümkündür. Böylece, sektörün, ticari menfaatleri için bu mücadeleyi bloke ederek, devletlerin daha ciddi ve etkili mücadele yöntemleri geliştirmesi ve katı düzenlemeler yapmasının önüne geçmeye çalıştığı düşünülebilir.

Almanya, FSM 2000-2009 yılları arasında 10 bini aşkın ihbar almıştır.(FSM, 2012k, http://www.fsm.de/de/Statistiken_2010 (11.05.2012); Avusturya Stopline, 2011 yılında toplam 3.548 ihbar almıştır.(STOPLINE, http://www.stopline.at/fileadmin/stopline.at/content/dateien/Annual_report-2011.pdf(08.05.2012); Kanada Cybertip, 2002 den 2012 yılına kadar 50 bin ihbar almıştır.(CYBERTIP, http://www.cybertip.ca/app/en/federal_mandatory_reporting (08.05.2012); Fransa, Point de Contact'a, 2010 yılında 8.196 ihbar yapılmış, bunların 424'üne erişim engellemesi uygulanmıştır. (POINTDECONTACT, http://www.afa-france.com/wa_files/CP_20AFA_20Bilan_20PDC_20janvier_202011.pdf (10.05.2012)

¹³¹ Bkz: Japonya INTERNETHOTLINE İhbar merkezi 13 personelden oluşmaktadır.(INTERNETHOTLINE, http://www.internethotline.jp/statistics/index_en.html (15.05.2012); Hollanda, MELDPUNKINDERPORNO İhbar merkezi 3 yönetici ve 7 uzman personel ile faaliyetlerini sürdürmektedir.(MELDPUNKINDERPORNO, http://www.meldpunt-kinderporno.nl/over_ons.htm (16.05.2012).

Diğer yandan, tüm dünyada İnternetin izlenmesi, denetlenmesi ve kontrol altına alınması ve bu kapsamda özellikle merkezi filtreleme ve erişim engelleme uygulamalarına karşı mücadele veren büyük organizasyonların genellikle ya büyük küresel şirketlerin bizzat organize ettikleri veya teknik ve finansal destek sağladıkları girişimler olarak ortaya çıkması da bu çerçevede değerlendirilebilir. Nitekim, söz konusu organizasyonlar, ülkelerin İnterneti denetim altına almaya çalışan politika ve uygulamalarına karşı anti sansür işbirlikleri geliştirmekte ve hatta sansürü aşma konusunda ülke kullanıcılarına ücretsiz program desteği sağlamaktadır.¹³²

Örneğin, aralarında Google, Microsoft ve Yahoo gibi dünya bilişim devlerinin de bulunduğu, çoğunluğu ABD merkezli üniversiteler, STK'ları ve şirketlerden oluşan "Global Network Initiative" bunlardan birisidir. Bu girişim, tüm dünyada, bilgi ve iletişim teknolojileri sektörünün karşı karşıya olduğu ve uluslararası insan hakları ve ifade özgürlükleri ile çatıştığını düşündükleri yerel kanunlar ve uygulamalara uyma konusundaki hükümetlerin baskılarına karşı işbirliği oluşturmak ve sektördeki ifade özgürlüklerini korumak amacıyla çalışmalar yapmaktadır.¹³³

Bu tür girişimler, İnternette erişim özgürlüğünün sağlanması konusunda faydalı ve gerekli görülmekle birlikte, söz konusu şirketler ve ABD ekonomisi açısından, İnternetin yaygınlaşması, sınırsızca kullanımının önündeki engellerin kaldırılması ve dolayısıyla, sektörün daha da büyümesi ve karlı hale gelmesini sağlamaya yönelik girişimler olarak da görülebilir. Yani, sektörün genel bir yaklaşım olarak, ulusal ve uluslararası ölçekte farklı neden ve konular kapsamında yasadışı ve zararlı içeriklere karşı yürütülen mücadeleleri ve İnterneti içerik yönüyle regüle etme girişimlerini ticari çıkarlarına tehdit olarak gördüğünü iddia edebiliriz. Bu nedenle, İnternete

¹³² Open Net Initiative İnternet'te sansürlü sitelere girilebilmesini sağlamak için "Psiphon" isimli bir program geliştirmiştir. İlk versiyonu 2006 yılında yayınlanan programın amacı İnternet kullanıcısının sansürlenmiş sitelere proxy'ler aracılığıyla ulaşmasına imkan vermektir. Programın kurduğu bağlantının gelişmiş yöntemlerle şifrelenmesi sayesinde bilginin ilk anda okunması gelişmiş bilgisayarlar için bile uzun zaman almakta ve böylece kullanan kişinin yakalanması epeyce zorlaşmaktadır. Açık kaynak kullanan "Psiphon", "psiphon.civisec.org" adresinden ücretsiz yüklenebilmektedir. ("İnternet sansürüne karşı küresel savaş", 11.01. 2008, <http://www.hurriyet.com.tr/e-yasam/8005276.asp?m=1>)

¹³³ Geniş bilgi için bkz. <http://www.globalnetworkinitiative.org> (14.02.2013)

sınırsız özgürlük isteyen bahsi geçen girişimleri sadece ve sadece tüm ülkelerde insan haklarının tesis edilmesini amaçlayan çabalar olarak görmemek gerekmektedir.

Keza, küresel sermayenin sakıncalı içeriklerle ilgili tavrının temel motivasyonunu “ticari kar” saikinın oluşturduğunun en önemli göstergelerinden birisi de sektördeki büyük firmaların İnternete sansür uygulayan ülkelere sağladıkları teknik destek ve işbirliğidir. Nitekim, CISCO, Yahoo, Google, Microsoft gibi şirketlerin Çin benzeri devlet sansürü uygulayan ülkelere teknik destek sağladığı ve çeşitli düzeylerde işbirliği yaptığı bilinmekte ve eleştirilmektedir. Yani, İnternetin küresel şirketlerinin sakıncalı içeriklerle mücadele ve bu kapsamda devlet sansürü uygulamaları konusunda ilkesel bir tavrı bulunmamaktadır. Ülkelerdeki mevcut konjonktüre göre, ticari çıkarlarını ön planda tutan bir yaklaşım içinde hareket etmektedirler.

Diğer yandan, dünyada birçok ülkedeki İnternetle ilgili düzenleyici üst kurulların mevcut yaklaşım, görev, konum ve yapılarının, küresel İnternet sektörünün ülkelerin içerik politikalarında belirleyici olma girişimlerine elverişli bir vasat sağladığı da söylenebilir. Bu kapsamda, bu düzenleyici kurulların özellikle sakıncalı içerikle gerçek anlamda etkili bir mücadele yürütülmesine uygun olmadığı görülmektedir.

Zira, liberal politikalar gereği, tam rekabetçi piyasa şartlarının hakim olmasını, sektörün büyümesini, daha karlı hale gelmesini ve bu çerçevede teknik bakımdan regüle edilmesini sağlamaya yönelik olarak faaliyet gösteren düzenleyici kurullarda, genellikle İnternetin riskleri ve tehlikeleri, yasadışı ve zararlı içeriklere karşı önlem alınması gibi bir bakış açısı gelişmemiştir. Çünkü, bu bakış açısının İnternet sektörüne ekonomik olarak zarar vereceği, kullanımı sınırlandıracağı, içerik düzenlemelerine kapı aralayacağı ve yeni hukuki ve mali yükümlülükler getireceği öngörülmektedir. Dolayısıyla, İnternet piyasasını büyütme endeksli yaklaşımlar, içeriklerin risk ve tehlikelerini görmeye engel olabilmektedir.

Görüldüğü ve onüçüncü alt hipotezde belirtildiği gibi, küresel İnternet sermayesi, doğrudan veya dolaylı olarak içerik düzenlemelerinin yönünü, politikalarını, yasadışı içeriklerle mücadelenin kapsamını ve yöntemini büyük oranda belirlemektedir.

14. Son olarak, ülkelerin filtreleme ve erişim engelleme uygulamalarının normatif olarak değerlendirilmesine imkan tanıyacak yöntemlerden bahsedilebilir. Zira, son dönemde söz konusu uygulamaların meşruiyetini normatif olarak değerlendirmede faydalanılacak elverişli, tutarlı ve isabetli bazı ölçütlerin belirlenmesinin gerekliliği gündeme getirilmiştir. Bambauer’ın “açıklık”, “şeffaflık”, “kısıtlılık” ve “sorumluluk” olarak belirlediği bu ölçütlerin, devletlerin filtreleme ve erişim engelleme uygulamalarının normatif olarak değerlendirilmesi için alternatif ve süreç odaklı bir çerçeve sunmaya yarayacağı, bunun yanı sıra bu sürece ilişkin kurumsal işlemlerin analizine olanak vereceği ve böylece, devletlerin İnternet kısıtlamalarının meşruiyetini ölçmeye yönelik analitik bir yöntemin ortaya çıkacağı düşünülmektedir.

Nitekim, bu ölçütlerden “açıklık”; devletlerin filtrelemeyi kabul edip etmediğini ve bu engellemenin gerekçesini açıkça belirtip belirtmediğini, “şeffaflık”; engelleme tipleri ve kategorileri ve engelleme kriterlerinin ne kadar şeffaf olduğunu, “kısıtlılık”; erişim engelleme uygulamalarının engellemeye ilişkin beyanlarla belirtilen sınırlar içerisinde yapılıp yapılmadığı, uygulamaların dar ve geniş kapsamlı olup olmadığını ve “sorumluluk” ise; vatandaşların engelleme kararlarına ne oranda katıldığı, yetkili kişi ve kurumların görev ve sorumluluk alanlarının belli olup olmadığını, engellemeye karşı çıkma imkanı ve azınlığın korunma durumunu ölçmektedir.

Bambauer’ın bir örnek model geliştirdiği bu konu, ondördüncü alt hipotezde belirtildiği gibi, ülkelerin içerik düzenlemesi politika ve uygulamaları için sübjektiflik ve keyfilikten uzak, nesnel ve normatif ilke ve ölçütlerin belirlenmesi ihtiyacını ortaya koymaktadır. Bu yolla, ülke uygulamalarının meşruiyetini test etmeye yarayacak uluslararası geçerliliği olan bir analitik analiz yönteminin geliştirilmesi mümkün olacaktır. Eğer bu gerçekleştirilebilirse, bu alanda faaliyet gösteren sivil ve kamu otoritelerinin öznel ve keyfi yorumlarının önüne geçilmiş ve özellikle, İnternetin hakim güçleri olan ülkelerin bu konuyu suistimal ederek diğer ülkeler üzerinde baskı kurması büyük oranda engellenmiş olacaktır.

15. Konunun Türkiye boyutuna bakılacak olursa, öncelikle Türkiye’deki İnternet kullanıcılarının profilini ve kullanım özelliklerini dikkate almak gerekmektedir.

İstatistiki veriler ülkemizde İnternet kullanımının sayısal, oransal ve kullanım miktarı ve süresi bakımından hızla arttığını ortaya koymaktadır. İnternetworldstats.com'un verilerine göre Türkiye'de 2000 yılında yaklaşık 2 milyon İnternet kullanıcısı varken, bu sayı 2012 Haziran'ı itibariyle 36 milyonu aşmıştır. Türkiye, İnternet kullanıcı sayısı bakımından Dünyada 15. sırada gelmektedir. Avrupa'da ise, 5. sıradadır.

Ülke nüfusunun genç olması ve gençlerin de teknolojiye daha yatkın olmalarının da etkisiyle İnternet kullanıcılarının çoğunun genç olduğu ve trendin bu yönde devam edeceği görülmektedir. İnternet kullanımının yüksekliğinde erkek ve eğitilmiş olma karakteri ön plana çıkmaktadır. Ülkemizde kullanıcılar daha çok evlerinden veya cep telefonları ile İnternete bağlanmayı tercih etmektedirler.

Türkiye'deki İnternet kullanım özelliklerini ortaya koyan araştırmalar ise, Türkiye'de İnternetin Facebook, Google ve Hotmail gibi batılı platformların egemenliği altında olduğunu ve kullanıcıların da İnterneti bu platformların sundukları imkanlardan yararlanarak daha çok eğlenme, vakit geçirme, haber okuma ve iletişim kurma amacıyla kullanmakta olduklarını göstermektedir. Keza, İnternette en çok yapılan aktiviteler sörf yapma, sanal sohbetler, sosyal ağ faaliyetleri, video seyretme, oyun, müzik, film, görüntü, yazılım indirme, oyun oynama, çevrimiçi haber, gazete veya dergi okuma, spor ve sağlık sitelerini gezme, blogları ziyaret, e-posta gönderme/alma ve görüntülü/sesli görüşme yapmak olarak belirmektedir. Ayrıca, çok olmamakla birlikte, eğitim amaçlı olarak, araştırma ve inceleme yapmak için, e-ticaret, sanal alışveriş, İnternet bankacılığı, e-devlet hizmetlerinden yararlanma, mal ve hizmetler hakkında bilgi alma gibi maksatlarla İnternetin kullanıldığı görülmektedir.

Öte yandan, tüm dünyada olduğu gibi Türkiye'de de teknolojik gelişmeler insan hayatını kolaylaştırırken diğer yandan sosyal, kültürel, ekonomik, psikolojik ve hatta sağlık alanlarında bazı sorunlara neden olmaktadır. Zira, bilgi toplumu bağlamında ele alınan "gözetim toplumu" olma korkusu, sayısal uçurum, güvenlik korkusu, tüketim toplumu haline gelme ve yabancılaşma ile bilgi kirliliği gibi sorunlar bugün ülkemiz için de geçerlidir. Bir çok açıdan dünyanın artık global bir köy haline geldiği düşünülürse, Türkiye'nin de bu sorunlardan kaçması mümkün gözükmemektedir.

Nitekim, diğer gelişmiş ve İnternet kullanımı yüksek ülkelerde görülen toplumsal sorunların benzerlerinin ülkemizde de görülmeye başlandığına şahit olmaktadır. Bu çerçevede, İnternetin aile içi ilişkilere ve iletişime vermiş olduğu zarar, eşler arasında “aldatma”yı ve boşanmaları artması ile barındırdığı zararlı ve sakıncalı içeriklerin, özellikle de pornografik içeriğin, genel olarak tüm aile bireyleri için tehlike oluşturmaları boyutlarıyla ilgili sorunlar ülkemiz için de söz konusudur.

Keza, İnternet, barındırdığı cinsel istismar ve pornografi içerikleriyle Türkiye’deki kullanıcıların büyük çoğunluğunu oluşturan çocuklar ve gençler için önemli bir risk ve sorun kaynağıdır. Nitekim, Türkiye’nin Google arama motoru istatistiklerinde “seks” ve “child porno” terimin aranmasında dünya üçünlüğüne, “porno” teriminin aranmasında dünya dördüncülüğüne sahip olması, BTK’nın 2012 verilerine göre Türkiye’deki kullanıcıların 60 saniyelik zaman kesiti içerisinde yaptıkları aktiviteler içerisinde en dikkat çekici verilerden birisini iki milyon kullanıcının çevrimiçi porno izlediğini gösteren rakamın oluşturmaları, TİB’nin yaptığı teknik değerlendirmelerde Türkiye’deki İnternet kullanıcılarının içerik bakımından %73 oranında müstehcen siteleri ziyaret ettiklerinin tespit edilmiş bulunması, ne yazık ki, bu tür içeriklere merak ve ilginin çok büyük boyutlarda olduğunu göstermektedir. Dolayısıyla, bu durumun meydana getirdiği ve getireceği olumsuzluklar ve sorunlar önemli bir tehlike olarak bugünüümüzü ve geleceğimizi tehdit etmektedir.

Türkiye’de siber zorbalık konusunda yapılan araştırmalar da bu sorunun ülkemizde giderek yaygınlaştığını göstermektedir. Nitekim değişik araştırmalar ortaokuldan üniversiteye kadar siber zorbalığa maruz kalan öğrencilerin toplam içindeki oranının %30-50 arasında olduğunu ortaya koymaktadır. Yine, İnternette yer alan şiddet, nefret ve intihara yönlendirme içerikleri ülkemizde en çok çocukları ve gençleri olumsuz yönde etkilemektedir. Nitekim, İnternetteki kavga, çatışma, işkence, savaş, cinayet, infaz, yaralama gibi vahşet ve şiddet içerikleri ülkemizde de yaygın olarak rağbet görmekte, izlenmekte ve paylaşılmaktadır. Türkiye’deki kullanıcıların İnternette video izleme konusunda dünyada ilk sırada yer almasında; video izlemenin tüm İnternet trafiğinde bandı en çok meşgul eden aktivite olarak ön plana çıkmasında; Youtube’un uzun süre yasaklı olmasına rağmen 2004’ten bu yana

Google'dan yapılan aramalarda Facabook'tan sonra en çok aranan ikinci kelime olmasında bu ilginin ve merakın izleri bulunabilir.

Benzer şekilde yabancı düşmanlığı, ırk, cinsiyet, din ve mezhep ayrımcılığı ve nefreti teşvik etme ve kışkırtmaya yönelik İnternet içerikleri de başta gençler olmak üzere tüm toplumsal kesimler üzerinde olumsuz etkiler meydana getirmekte ve toplumsal barışı ve huzuru tehdit etmektedir. Nitekim, bir araştırma sonucunda, Türkiye'deki kullanıcılar bakımından İnternet'te demokratik bir tartışma kültürünün olmadığı; ırkçı, mezhep ayrımcı, cinsel kimliği aşağılayan ve küçük düşüren nefret söyleminin var olduğu, kullanıcıların gerçek yaşamdaki kimliklerine yakın hatta benzer kişilerle iletişim kurdukları ve farklı olana tahammülsüzlük gösterdikleri tespit edilmiştir. Keza, Türkiye'de özellikle de sosyal medya ve haber sitelerinin okuyucu yorumları nefret söyleminin giderek yükseldiği alanlar olarak dikkat çekmektedir.

İnternet, tüm dünyada olduğu gibi ülkemizdeki her yaş grubundan kullanıcıları ve özellikle çocukları ve gençleri kumar, bahis ve şans oyunları oynamaya, uyuşturucu ve uyarıcı madde kullanmaya teşvik etmekte ve imkan sağlamaktadır. Nitekim, Türkiye'de 1.5 milyon kişinin İnternet üzerinden kumar ve bahis oynadığı, online kumar işletmelerinin yıllık cirolarının 1 milyar doları aştığı tahmin edilmektedir. Keza, Google'ın yayınladığı arama trendlerinde "Facebook Holdem Poker" in 2012 yılı aramalarında Türkiye Endonezya'dan sonra ikinci sırada yer almıştır.

İnternet bağımlılığı konusunda da Türkiye kötü sinyaller vermektedir. Bazı araştırma sonuçları bu durumun ipuçlarını vermektedir. Örneğin, bir araştırmada ilköğretim ikinci kademe ve lise öğrencilerinin 10 üzerinden 6,36'sı "bilgisayar ve İnternetsiz", 5,69'u "cep telefonsuz" bir hayat düşünemediğini bildirmiştir. Keza, Youth Insight'ın liseli ve üniversiteli gençleri kapsayan araştırmasında gençlerin 1/3'ü İnternetin "yokluğunda yaşayamayacakları bir şey" anlamına geldiğini belirtmiştir.

Diğer yandan, Türkiye'de özellikle çocuklar ve gençler arasında, dünyadaki gelişme trendlerinin çok daha ötesinde ilgi gören, neredeyse bir sosyal ağ ve özellikle Facebook çılgınlığı göze çarpmaktadır. Nitekim, 2012 Mayıs'ı itibariyle

Facebook'un Türkiye'deki kullanıcı sayısı 32 milyonu geçmiştir. Ülkemizdeki toplam İnternet kullanıcılarının %88,13'ü aynı zamanda Facebook kullanıcısıdır. Bu oranın aynı tarihler için Dünyada %34,73, Avrupa'da %48,39 olduğu düşünülürse Türkiye'de nasıl bir Facebook çılgınlığı yaşandığı daha iyi anlaşılacaktır. Başka bir araştırmada, genel olarak çocukların %47'sinin sosyal paylaşım sitelerinde hesabı bulunurken bu çocukların da 1/3'nün sosyal ağlara üyelik için alt sınır olan 13 yaşından küçük olduğu belirlenmiştir.

Türkiyeli İnternet kullanıcısı çocuklar ve gençler açısından dijital oyunlar da potansiyel sorunlara gebe dir. Ülkemizde İnternetin oyun amaçlı kullanımının yaygın olduğu bilinmekte ve 20 milyon civarında dijital oyun kullanıcısının bulunduğu, bunların 15 milyon kadarının Facebook'da oyun oynadığı tahmin edilmektedir. Diğer yandan, Türkiye'de İnternet kafe kullanımı giderek azalsa da, çocuklar ve gençler için özellikle dijital oyun oynama mekanları olarak halen cazibesini kaybetmemiştir. İnternet kafelerin yanlış amaçlarla ve bilinçsizce kullanılması sonucunda özellikle çocukların çeşitli tehlikelerle, psiko-sosyal ve fiziksel gelişimlerini olumsuz yönde etkileyecek istenmeyen durumlarla karşılaşılması mümkündür.

Sonuç olarak, onüçüncü alt hipotezde de belirtildiği gibi, ülkemiz açısından İnternetin çocuklar, gençler, aile ve toplum için oluşturduğu riskler ve tehditlerin gerçek boyutları ile ortaya konulması gerekmektedir. Fakat bu konularda elimizde yeterli bilimsel veriler bulunmamaktadır. Ülke genelinde bilişim teknolojileri ve özellikle İnternet kullanımına, bunların etkilerine ve sonuçlarına, bu nedenle oluşan sosyal risklere ve tehditlere ilişkin geniş ve derinlikli alan araştırmalarına ihtiyaç vardır. Bu tür araştırmaların hem zamanla tekrar edilmesi hem de etkin kullanıcıya odaklanan çalışmaların çeşitlendirilmesinde fayda vardır.

1993 yılında Türkiye'de kullanılmaya başlanan İnternete 2001 yılına kadar önemli bir müdahalede bulunulmamıştır. Ancak, zaman içinde İnternetin suçta araç olarak kullanılmasına ilişkin olaylar yaşanmaya başlanması ve bu tür olayların nitelik ve nicelik olarak suç olgusunda değişikliğe neden olması, bu alanın bir takım yeni hukuki düzenlemelerle disipline edilmesi ihtiyacını ortaya çıkarmıştır. Bu ihtiyaçlar

doğrultusunda, İnternet yoluyla oluşan sorunların çözümü için zaman içinde farklı yasal düzenlemeler, kurumsal yapılar ve uygulamalar gündeme gelmiştir.

İnternetin ortaya çıkardığı sorunların giderilmesi amacıyla başlangıçta mevcut kanunlara çeşitli eklemeler yapılması yolu tercih edilmiştir. Bu çerçevede, sırasıyla TCK, FSEK, Basın Kanunu, RTÜK Kanunu ve Tüketicinin Korunması Hakkındaki Kanunu’nda değişiklikler yapılmıştır. Bunlar içerisinde özellikle RTÜK Kanunu’nda yapılan değişiklik, İnternete sansür yolunun açılacağı iddiasıyla bazı STK’larca tepki ve eleştirilere neden olmuştur.

Bu süreçte yasal düzenlemelere paralel olarak İnternete ilişkin bazı kurumsal yapıların oluşturulduğu da görülmektedir. Bu çerçevede, Ulaştırma Bakanlığına İnternet konusunda danışmanlık hizmeti sunmak üzere İnternet Kurulu ihdas edilmiş, telekomünikasyon ve dolayısıyla İnternet sektörünü de ilgilendiren, yetkilendirme, denetleme, teknik düzenlemeye ilişkin görevleri yerine getirmek ve sektördeki serbest rekabeti sağlamak üzere, idari ve mali özerkliğe sahip TK kurulmuştur. TK’nun kurulması, IMF ve Dünya Bankası’nın da zorlamasıyla o dönem tüm dünyada revaçta olan deregülasyon ve sektörlerin tam rekabetçi hale getirilmesi için düzenleyici ve denetleyici bağımsız üst kurullarca yönetilmesi politikalarının ülkemizdeki uygulamalarından birisidir.

Türkiye’de İnternetin düzenlenmesi konusuyla ilgili yürütülen çalışmaların diğer bir mecrası “bilgi toplumu” çalışmalarıdır. 2003 yılında ilan edilen e-Dönüşüm Türkiye Projesi ile belirli bir bütünlüğe kavuşturularak yürütülmeye başlanan bilgi toplumuna yönelik çalışmalar kapsamında, DPT’nin koordinasyonu ile, sırasıyla 2003-2004 Kısa Dönem Eylem Planı, Bilgi Toplumuna Dönüşüm Politikası Belgesi, 2005 Eylem Planı ile 2006-2010 Bilgi Toplumuna Stratejisi ve Eylem Planı belgeleri hazırlanmış ve uygulanmıştır. Bu süreçte, söz konusu belgelerin hazırlanmasında ve uygulanmasında E-Dönüşüm Türkiye İcra Kurulu, e-Dönüşüm Türkiye Danışma Kurulu, Dönüşüm Liderleri Kurulu gibi kamu kurum ve kuruluşları ile STK’lar, üniversiteler ve özel sektör temsilcilerinin ortaklaşa çalışmasını sağlamaya yönelik yönetim mekanizmaları kurulmuş ve işletilmiştir.

Türkiye'nin bilgi toplumuna ve İnternete bakışını ve İnternet politikalarının ana eksenini oluşturan e-dönüşüm Türkiye Projesi ve bu Proje kapsamında hazırlanan ve uygulanan bilgi toplumu belgelerinde temel yaklaşımın ekonomi ve teknoloji merkezli olduğu görülmektedir. Onun için bu belgelerde daha ziyade ekonomik kalkınma, refah devleti olma, teknolojinin yaygınlaştırılması, üretimde ve kullanımda teknolojik gelişmişliği yakalama, e-devlet uygulamaları ile devleti dönüştürme ve hatta demokratikleştirme konularının ön plana çıktığı gözlemlenmektedir. Keza, birazda yaşanan dönemin iklimine uygun olarak, bilgi toplumuna dönüşme ve bilgi ekonomisine geçme hedefi büyük bir ideal olarak benimsenmiş ve belgelere yansımıştır. Konunun, bilgi toplumuna yöneltilen eleştiriler, bilgi ve iletişim teknolojilerinin ve özellikle İnternetin taşıdığı potansiyel riskler, yanlış kullanımının neden olduğu sorunlar, yasadışı ve zararlı içeriklerin durumu, sosyal maliyetler gibi olumsuz yönleri özellikle başlangıçta çok fazla ön plana çıkartılmamıştır.

Bu iyimser yaklaşımın benimsenmesinde, başlangıçta İnternet kullanımının düşük olması nedeniyle güvenlik ve toplumsal sorunlarla henüz fazlasıyla tanışılmamış olmasının etkisi bulunmakla beraber, ülkenin ekonomik, sosyal ve siyasal iç dinamikleri açısından bu tür sorunların dile getirilmesinin ekonomik kalkınma ve teknolojinin yaygınlaştırılması hedefleri açısından risk ve engel oluşturabileceği endişesinin de etkili olduğu düşünülebilir. Bu kapsamda, henüz gelişmekte olan bilişim sektörünün ürkütölme korkusu, İnternet düşmanı ilan edilme kaygısı, AB ile olan ilişkilerin yara alması endişesi gibi birçok sebep de akla gelebilir.

Bu temel yaklaşımın ve endişelerin, en azından bir kısmının, yoğunluğu azalsa da halen geçerliliğini sürdürdüğü iddia edilebilir. Nitekim, bilgi toplumu belgeleri için başlangıçta oluşturulan tema ve kurgu sonraki yıllarda çok fazla değişmemiştir. O nedenle belgelerde yer alan strateji, eksen ve parametreler kısmen güncellenerek değişime uğrasa da bilgi toplumuna yönelik bu iyimser yaklaşım ve bunun üzerine inşa edilen idealleştirilmiş hedefler ve öncelikler büyük oranda korunmuştur.

Bununla birlikte, belgelerde bu temel eksik yaklaşım göze çarpsa da, zaman içinde, önce bilişim suçlarından başlamak üzere, İnternet kaynaklı sorun alanlarının ve bu

alanlara yönelik çözüm eylemlerinin belgelere girmiş olduğu görülmektedir. “Güvenli İnternet” bağlamında yasadışı ve zararlı içerikle mücadeleyi de öngören eylemlerin daha sonraki belgelerde yer almasını bu kapsamda değerlendirebiliriz. Biraz geç kalınmış ve yetersiz olsa da, bu ve benzeri konuların belgelere girmiş olmasını, sorunların varlığının ve süregelen eksik yaklaşımın zimmen kabul edilmesi ve daha dengeli bir yaklaşımın geliştirilmesi çabası olarak görülebiliriz.

Diğer yandan, Türk hukukunda, 5651 Sayılı Yasa’dan önce İnternet içeriğine müdahale, İnternet suçlarının cezalandırılması ve erişim engellemesi uygulamaları farklı kanun hükümlerine dayanılarak gerçekleştirilmiştir. Buna göre, İnternetin araç olarak kullanılmasıyla meydana gelen ifade suçları, özel hayatın gizliliğini ihlal veya kişilik haklarına saldırılar, telif hakkı ihlalleri, TSK’ya hakaret, yolsuzluk söylentileri, Türklük karşıtı veya terörist propaganda gibi nedenlerle mahkemelere intikal eden davalar, mevcut yasalarla sonuçlandırılmaya çalışılmıştır. Bu kapsamda, mahkeme kararı ile İSS’lar tarafından birçok sitenin erişime kapatıldığı görülmüştür. Erişim engellemeler içerisinde en çok ses getireni ise, YouTube’un engellenmesidir.

Diğer yandan, çocukların, ailenin ve kamu düzeninin korunması için İnternet ortamında bulunan yasadışı ve zararlı içerikle mücadele edilmesi ve bu konuda yasal düzenleme yapılmasının gerekliliği e-Dönüşüm Türkiye Projesi kapsamında yayınlanan 2006-2010 Bilgi Toplumu Stratejisi Eylem Plan’ında yer almaktaydı. Plan’ın 10. eylemi, “güvenli İnternet” için “gereklilik” ve “ölçülülük” kıstaslarına bağlı kalarak yasal düzenlemelerin yapılmasını ve İnternet üzerinde çeşitli denetim ve yasakların uygulanmasını öngörüordu.

Keza, 2006-2007’de yoğun bir şekilde devam eden çocuk pornosu operasyonları, İnternetin pornografik içeriğe erişimi çok kolaylaştırması, intiharı körükleyen Satanist içerikler, İnternet kafelerde yaşanan olumsuz hadiseler, çocuklarda görülen oyun tutkunluğu, Atatürk’e, milli ve manevi değerlere hakaret içeren YouTube videoları konusundaki şikayetler ve bu konuların sık sık basında yer bulması, İnternet’in düzenlenmesi taleplerini daha yoğun bir şekilde gündeme getirmiştir. Bu talepler, hükümet ve Meclis’i, İnternet içeriğinin düzenlenmesi için yeni bir kanun

yapılması amacıyla harekete geçirmiş ve İnternet içeriğine müdahale amacıyla farklı neden ve yöntemleri öngören iki kanun tasarısı ve bir kanun teklifi hazırlanmıştır. 5651 sayılı Kanun, bu tasarı ve teklifler üzerinde gerçekleşen tartışmalar ve yürütülen çalışmalar ile şekillenerek vücut bulmuş ve bugünkü halini almıştır.

Bu çerçevede ilk olarak Adalet Bakanlığı hem içerik hem de bilişim suçlarını düzenleyen bir kanun tasarısı hazırlamıştır. Tasarıyla; içerik, yer, erişim ve toplu kullanım sağlayıcıların sorumlulukları ile “düzeltme ve cevap hakkı” düzenlenirken, içerik ve bilişim suçlarının türleri, soruşturulma ve kovuşturulmalarına ilişkin esas ve usuller AB normlarına uyumlu olacak şekilde belirlenmek istenmiştir. Tasarı, sadece çocuk pornografisi ve devletin güvenliğine ve kamu barışına karşı işlenen suçları içerik suçu olarak kabul etmiştir. Bu kapsamda hazırlanan taslak, hakkında görüş alınmak üzere üniversiteler, mahkemeler ve ilgili bakanlıklar ve barolar dahil 100’den fazla kurum ve kuruluşa gönderilmesine rağmen yeterince kamuoyu ile paylaşılmadığı gerekçesiyle eleştirilmiştir.

Bu yasa tasarısı tartışılırken, bilişim ağlarının ortaya çıkardığı hukuki sorunları çözmeye matuf yeni bir yasa teklifi TBMM’ye sunulmuştur. Teklif, Adalet Bakanlığı Tasarısı’ndan çok daha kısa ve doğrudan İnternet aktörlerinin ve İnternet kafelerin yükümlülük ve denetimleriyle özellikle çocuk istismarı ve şiddet içerikli yayın, sahtecilik ve kumar gibi suçların İnternet üzerinden işlenmesine tedbir almayı amaçlayan bir metin olarak ortaya çıkmıştır. Nitelik olarak Adalet Bakanlığı’nın hazırlamış olduğu metinden fazlaca bir farkı bulunmayan bu Teklif, daha sonra TBMM Adalet Komisyonu kararı ile 5651 sayılı Kanun Tasarısı ile birleştirilmiştir.

Bu iki metin dışında Ulaştırma Bakanlığı bilişim suçlarının önlenmesi amacıyla yeni bir kanun tasarısı hazırlamış ve 12.02.2007’de TBMM’ye sunmuştur. 5651 sayılı Yasanın esasını oluşturan bu Tasarı, suçun ve suçlunun gelişen bilişim teknolojilerini kullanarak, Anayasa’nın, özel olarak korunmasını öngördüğü, başta aile, çocuklar ve gençler olmak üzere belirli sosyal kesimlere yönelik suçların kolayca işlenmesini önleyici “özel bir kanun” niteliğindedir. Tasarı, Avrupa Siber Suç Sözleşmesi ve Almanya Tele Hizmetler Yasası hükümlerinden yararlanılarak oluşturulmuştur.

Tasarı hızlı bir yasalaşma süreci geçirerek 04.05.2007 tarihli Genel Kurul’da görüşülerek kabul edilmiş ve 5651 sayılı “İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun” olarak, 23.05.2007 tarihli Resmi Gazete’de yayımlanarak yürürlüğe girmiştir. Tasarı, Adalet Komisyonu görüşmelerinde büyük değişikliklere uğramıştır. Genel Kurul’da sadece, Komisyon aşamasında metinden çıkartılan “İnternet Kurulu”na ait düzenleme yeniden metne alınmıştır.

Gerek Adalet Komisyonu ve gerekse Genel Kurul aşamasında olsun, Tasarı ile ilgili en çok tartışma katalog suçlarının kapsamının genişletilmesi konusunda yaşanmıştır. Anamuhalefet Partisi CHP, 5816 sayılı Atatürk Aleyhine İşlenen Suçlar Hakkında Kanun’da yer alan suçlar ile TCK’nın 302. maddesinde yer alan Türk Devleti’nin ve ülkenin bölünmez bütünlüğünü bozma suçu ve Anayasa’nın 174. maddesinde güvence altına alınan İnkılap Kanunları’na ve özellikle laiklik ilkesine karşı işlenecek suçların da erişim engelleme sebepleri arasına alınmasını önermiştir. Bu önerilerden sadece Atatürk’e hakaret suçlarından bir kısmı İnternet ortamındaki yayın yoluyla da işlenebileceği değerlendirmesiyle Komisyon aşamasında katalog suçları kapsamına alınmıştır.

Türkiye’nin İnternet tarihinde 5651 sayılı Kanun bir milat sayılabilir. İçerik düzenlemesi konusuna özel olarak hazırlanan bu Kanun getirdiği yeni hükümler ve uygulamaları ile yeni bir dönemi başlatmıştır. 5651 sayılı Kanun’un iki temel amacından birisi; içerik, yer, erişim ve toplu kullanım sağlayıcılara ait "yükümlülük ve sorumlulukları belirlemek", diğeri ise; bu İnternet aktörleri üzerinden “İnternet ortamında işlenen belirli suçların önlenmesine ilişkin esas ve usullerin belirlenmesi”dir. Keza düzenleme ile, TCK’nda yer alan “İntihara yönlendirme (madde 84)”, “Çocukların cinsel istismarı (madde 103, birinci fıkra)”, “Uyuşturucu veya uyarıcı madde kullanılmasını kolaylaştırma (madde 190)”, “Sağlık için tehlikeli madde temini (madde 194)”, “Müstehcenlik (madde 226)”, “Fuhuş (madde 227)”, “Kumar oynanması için yer ve imkan sağlama (madde 228)” ve “5816 sayılı Atatürk Aleyhine İşlenen Suçlar Hakkında Kanun’da yer alan suçlar”ın İnternet ortamındaki olumsuz etkilerinin önlenmesi için idari ve yargısal koruma tedbiri olarak iki çeşit

yöntem öngörülmektedir. Kanun ile içerik denetiminin nasıl ve hangi kurum tarafından yapılacağına ilişkin düzenlemeler yapılmıştır.

Kanun, öncelikle içerik, yer, erişim ve toplu kullanım sağlayıcılarını tanıtıcı bilgilerini kendilerine ait İnternet ortamında kullanıcıların ulaşabileceği şekilde ve güncel olarak bulundurmakla yükümlü tutarak bu aktörlere kolay erişimi sağlamaya çalışmıştır. Daha sonra, her bir aktöre yaptığı işin niteliğine göre farklı yükümlülükler getirmiştir. Buna göre, içerik sağlayıcılar kullanıma sunduğu her türlü içerikten sorumlu tutulurken, bağlantı sağladığı başkasına ait içerikten sorumlu tutulmamıştır. Ancak, sunuş biçiminden, bağlantı sağladığı içeriği benimsediği ve kullanıcının söz konusu içeriğe ulaşmasını amaçladığı açıkça belli ise, genel hükümlere göre sorumluluğa sahiptir.

Yer sağlayıcılar ise, yer sağladığı içeriği kontrol etmek veya hukuka aykırı bir faaliyetin söz konusu olup olmadığını araştırmakla yükümlü değildir. Fakat, haberdar edilmeleri ve teknik olarak imkan buldukları ölçüde yer sağladıkları hukuka aykırı içeriği yayından kaldırmakla yükümlüdür. Keza, erişim sağlayıcılarda erişim sağladığı içerikten sorumlu değildir ve bunların hukuka aykırı olup olmadıklarını ve sorumluluğu gerektirip gerektirmediğini kontrol etmekle ilgili yükümlülükleri yoktur. Fakat, hukuka aykırı içerikten, haberdar edilmeleri durumunda ve teknik olarak engelleme imkanı bulundukları ölçüde erişimi engellemekle yükümlüdürler. Ayrıca, erişim sağlayıcılara, sağladığı hizmetlere ilişkin olarak; trafik bilgilerini saklamak ve bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini sağlamak yükümlülüğü getirilmiştir.

Kanun, ticari amaçla toplu kullanım sağlayıcıların denetimi mahalli mülki amirlere verirken, aynı merciden izin belgesi almaları yükümlülüğü getirmiştir. Ticari amaçla olup olmadığına bakılmaksızın tüm toplu kullanım sağlayıcılara ise, konusu suç oluşturan içeriklere erişimi önleyici tedbirleri alma yükümlülüğü verilmiştir.

Kanun, erişimin engellenmesi kararının, soruşturma evresinde hakim, kovuşturma evresinde mahkeme tarafından verilebileceğini, soruşturma safhasında, gecikmesinde

sakınca bulunan hallerde Cumhuriyet savcısı tarafından da erişimin engellenmesi kararının alınabileceğini hükme bağlamıştır. Katalog suçlarını oluşturan yayınların içerik veya yer sağlayıcısının yurt dışında bulunması halinde ise, TİB'na erişimin engellenmesi kararını re'sen verebilme yetkisi tanımıştır. Yasa, içerik veya yer sağlayıcısı yurt içinde bulunsa bile, içeriği çocukların cinsel istismarı ve müstehcenlik suçlarını oluşturan yayınlara ilişkin olarak da TİB'na aynı yetkiyi vermiştir. Başkanlığa ayrıca, verilen erişimin engellenmesi kararının konusunu oluşturan yayınları yapanların kimliklerinin belirlenmesi durumunda, Cumhuriyet başsavcılığına suç duyurusunda bulunma yükümlülüğü getirilmiştir.

Kanun, içerik düzenlemesiyle ilgili verilen görevleri yerine getirmek üzere, TK bünyesinde bulunan TİB'nda İnternet Daire Başkanlığını ihdas etmiştir. Kanun ayrıca, İnternet Kurulu oluşturulmasını öngörürken, Başkanlığa bu Kurul ile gerekli işbirliği ve koordinasyonu sağlama görevi vermiştir.

5651 sayılı Kanun katalog suçları diye bilinen belirli suç tiplerine ait içeriklerle mücadeleyi benimsemiş olmakla birlikte, zaman içerisinde değişik ihtiyaçlardan ve gerekçelerden dolayı yeni erişim engellemesi sebepleri ortaya çıkmakta ve farklı yasal düzenlemeler söz konusu olmaktadır. Örneğin, DİB Kanun'unda 2010 yılında yapılan değişiklikle hatalı ve noksan olarak basıldığı veya yayımlandığı Kurul tarafından tespit edilen mushaf ve cüzler ile sesli ve görüntülü Kur'an-ı Kerim yayınlarının mahkeme kararı ile toplatılıp imha edileceği düzenlendikten sonra, bu kapsama giren yayının İnternet ortamında yapılması haline söz konusu yayınlara ilgili olarak erişimin engellenmesi kararının verilmesi ve bu kararın TİB tarafından uygulanması hüküm altına alınmıştır.

Bilahare 5651 sayılı Kanun'un uygulamasına yönelik olarak üç farklı yönetmelik hazırlanarak yürürlüğe konulmuştur. Bu düzenlemelerden ilki olan erişim ve yer sağlayıcılara faaliyet belgesi verilmesi konusundaki Yönetmelik ile, söz konusu İnternet aktörlerini kayıt altına alarak yasadışı ve zararlı içerikle mücadelede kontrol edilebilir ve denetlenebilir bir zemin oluşturulmuştur. İkincisi olan İnternet toplu kullanım sağlayıcılarına yönelik Yönetmelik ise, İnternet kafelere hukuki bir statü

kazandırırken, biraz karışık bir yapı öngörmekle birlikte, denetim ve kontrol altına alınmalarıyla ilgili önemli bir düzenlemedir. İnternet ortamında yapılan yayınların düzenlenmesine dair üçüncü Yönetmelik ile, söz konusu İnternet aktörlerinin sorumluluk ve yükümlülükleri detaylandırılarak, bunlar üzerinden katalog suçları ile mücadele edilmesinin uygulamasına yönelik usul ve esaslar belirlenmiştir.

Türkiye’de genel olarak İnternet, özel olarak ise İnternet içeriğinin düzenlenmesi ile doğrudan veya dolaylı ilgili kurumların başlıcaları UDH Bakanlığı, BTK, TİB, İnternet Geliştirme Kurulu, Çocuk ve Aile Profil Kriterleri Çalışma Kurulu, Çocukları Muzır Neşriyattan Koruma Kurulu, Sinema Genel Müdürlüğü Değerlendirme ve Sınıflandırma Kurulu, RTÜK, Bilgi Toplumu Dairesi Başkanlığı ve Aile ve Toplum Hizmetleri Genel Müdürlüğü’dür.

Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, hukuki ve kurumsal yapısı itibarıyla bilgi-iletişim alanlarında hem politika belirleme, kural koyma, düzenleme ve denetleme, hem de ana hizmet birimlerinin proje ve faaliyetlerini yerine getirme bakımından önemli ve kapsamlı görev ve yetkilere sahiptir. Bakanlık ile ilişkili bağımsız üst kurul olarak oluşturulan BTK, Bakanlığın doğrudan İnternete yönelik görevlerinin önemli bir kısmını üstlenmiştir.

İdari ve mali özerkliğe sahip özel bütçeli bir kamu kurumu olan BTK, Türkiye’de İnternet özelinde en yetkili kurumdur. Nitekim, Elektronik Haberleşme Kanunu BTK’ya İnternetle ilgili birçok görev ve yetki vermiştir. Bunlardan Kurum’a verilen kamu güvenliği, kamu sağlığı ve benzeri kamu yararı gereklerinden kaynaklanan sebeplerin tespiti halinde, şirketlerin elektronik haberleşme alanında faaliyete geçmelerini veya elektronik haberleşme sağlamalarını gerektiğinde Bakanlığın görüşünü de alarak engelleyebilme yetkisi dikkat çekmektedir.

Elektronik Haberleşme Kanunu’yla Ulaştırma Bakanlığı’na verilen ve daha sonra BTK’ya görev ve yetki olarak tevdi edilen İnternetle ilgili düzenlemelerden birisi de İnternet alan adlarının tahsis ve yönetimi konusudur. Nitekim, BTK’nın hazırladığı “İnternet Alan Adları Yönetmeliği” 2010 yılında yürürlüğe girmiştir.

Yakın zamanda BTK'yı ilgilendiren diğer bir İnternet düzenlenmesi konusu da “siber güvenlik”tir. Siber Güvenlik Kurulu'nun kurulması, başkanlığının UDHB'na verilmesi ve Bakanlığın siber güvenlikle ilgili görevlerini BTK ve diğer kamu kurum ve kuruluşları aracılığı ile yerine getirmesine karar verilmesinden sonra BTK ulusal siber güvenliğin sağlanmasıyla ilgili çalışmaların odak kurumu haline gelmiştir. Bu süreçte Siber Güvenlik Kurulu, Siber Güvenlik Strateji Belgesi ile Eylem Planı'nı onaylamış ve bu belgeye istinaden USOM'nin kurulmasına karar verilmiştir.

BTK, Kurul ile Başkanlık teşkilatından oluşmaktadır. Kurul, Kurum'un karar organıdır ve biri başkan yedi üyeden oluşmaktadır. Başkan ve Kurul üyeleri Bakanlar Kurulunca beş yıllık süre için atanmaktadır. Üyelerin ikisi telekomünikasyon sektörünü temsilen işletmecilerin göstereceği adaylar arasından, birisi de tüketicileri temsilen atanmaktadır. Başkan ve diğer üç üye kamudan gelmektedir. Dolayısıyla, BTK'nın yönetim ilkesini esas alarak yapılandırıldığı söylenebilir. BTK, İnternet içeriğinin düzenlenmesine yönelik temel yetkilerini ise 5651 sayılı Kanun vesilesiyle bünyesinde bulundurduğu TİB'na verilen yetki ve sorumluluklardan almaktadır.

Yasadışı dinlemelerin önlenmesini sağlamak amacıyla kurulan TİB, 2006 yılında faaliyete başlamıştır. 5651 sayılı Kanun ile TİB'na, Kanun'da sayılan İnternet ortamı ve bu ortamda işlenen bazı suçlarla mücadeleyle ilişkin görevler verilmiştir. TİB bünyesinde İdari, Hukuk, İnternet, Teknik İşletme ve Bilgi Sistemleri Daire Başkanlıkları bulunmaktadır. Son dönemde TİB'na siber güvenlikle ilgili görevler de tevdi edilmiştir. Siber Güvenlik Strateji Belgesi ile Eylem Planı'nı öngördüğü USOM, 2013 yılı Mayıs sonunda TİB bünyesinde faaliyete başlamıştır.

Türkiye'de İnternetle ilgili kurumlardan birisi olan ve 2011 yılında kurulan İnternet Geliştirme Kurulu'na; Bakanlığa, görev alanına giren konularla ilgili olarak çalışmalarda bulunma, araştırma, inceleme ve değerlendirme yapma görevleri verilmiştir. Kurul, Başkan da dahil dört STK temsilcisi, BTK Başkanı, Haberleşme Genel Müdürü ve bir akademisyen olmak üzere yedi üyeden oluşmaktadır ve sivil kanadın ağırlıkta olduğu yapısı ile yönetim yaklaşımının bir ürünüdür.

Ülkemizde içerik düzenlemesiyle ilgili olarak yakın zamanda oluşturulan diğer bir yapı ise Çocuk ve Aile Profil Kriterleri Çalışma Kurulu'dur. Kurul, Güvenli İnternet Hizmetinde yer alan Çocuk ve Aile Profil listelerinin oluşturulmasına ilişkin kriterleri belirlemektedir. BTK koordinasyonunda onbir üyeden oluşan Kurul'da, biri başkan olmak üzere BTK'dan iç, Aile ve Sosyal Politikalar Bakanlığında iki, İnternet Kurulu'nun sivil toplum temsilcisi üyelerinden iki, Türkiye Dijital Oyun Federasyonu'ndan bir ve psikoloji, pedagoji, sosyoloji, hukuk gibi ilişkili alanlarda uzmanlığı olan kişiler arasından BTK tarafından seçilen üç üye bulunmaktadır.

Bir tür "içerik sınıflandırma ölçütleri" belirleme işlevi de gören ve sivil kökenli üyelerin çoğunlukta olduğu Kurul'da, İnternetin tarafı olan tüm kesimlere söz hakkı tanınması amacıyla, konunun bağımsız uzmanları ile STK temsilcilerine de yer verilmesi oldukça önemlidir. Bu yaklaşım da, regülasyon çalışmalarının yönetim ilkesine göre "birlikte düzenleme" anlayışıyla yapılmasına yönelik beklentilere uygun düşmektedir. Aksi takdirde, Güvenli İnternet Hizmeti kapsamındaki profillerin içeriğinin hangi kriterlere göre, kim tarafından oluşturulacağı konusu çok daha büyük eleştirilerin ve tartışmaların yaşanmasına neden olacaktır.

Türkiye'de, Çocuk ve Aile Profil Kriterleri Çalışma Kurulu, Küçükleri Muzır Neşriyattan Koruma Kurulu, Sinema Genel Müdürlüğü Değerlendirme ve Sınıflandırma Kurulu ile RTÜK, "yayın içeriklerini değerlendirme ve sınıflandırma" benzeri işler yapmaktadır. Dolayısıyla, yapıları, yöntemleri ve yaklaşımları farklı olsa da, çalışma alanları büyük ölçüde örtüşen dört farklı kamu kurumunun varlığından bahsedilebilir. O halde, yayın içeriklerini değerlendirme ve sınıflandırma amacına yönelik faaliyetler gösteren bu kadar farklı kurum yerine, tüm bu kurumların mevcut görevlerini kapsayacak şekilde, her tür yayın içeriğini değerlendirip sınıflandırmasını yapacak ihtisaslaşmış bir "Sınıflandırma Kurumu" nun yönetim modeline göre oluşturulması daha faydalı olacaktır.

Diğer yandan, tüm dünyada ve ülkemizde haberleşme ve bilgi teknolojilerinin sayısal yayıncılığa yakınsaması sürecinin yaşanmakta olmasından dolayı, bu alanla ilgili denetim ve düzenleme görevi yürüten iki kurum olan RTÜK ve BTK arasında iç içe

girmiş olan yetki ve görevler konusunda bazı sorunların ortaya çıkması ihtimali bulunmaktadır. Bu gün için, mevcut mevzuat her iki Kurumu da ilgilendiren teknik ve idari konularda yetki ve görev paylaşımını düzenleyerek sorunun önüne geçmiş gibidir. Fakat, yakın gelecekte yakınsama teknolojilerinin daha da gelişmesiyle özellikle içerik denetimine ilişkin sorunların daha da karmaşık ve girift bir hale gelmesi muhtemeldir. O zaman, şu an iki kurum arasında işbirliği ile çözülen yayıncılık alanına ait sorunların içinden çıkılmaz bir noktaya ulaşması mümkündür. Bu nedenle, iki kurumun tek çatı altında görev yapması en uygun çözüm olacaktır.

İnternet içerik düzenlemesiyle ilgili bir diğer önemli kurum; Türkiye’de e-Dönüşüm Türkiye Projesi’nin koordinasyonunu yürüten ve bilgi toplumu dönüşümüne ilişkin politika, hedef ve stratejilerin belirlenmesi görevini üstlenen Bilgi Toplumu Dairesi’dir. Nitekim, Proje kapsamında geçmişte hazırlanan ve uygulanan strateji belgeleri ve eylem planları ile bundan sonra yapılacak plan ve strateji belgelerinin Türkiye’deki İnternet politikalarına yön veren ve verecek temel metinler olması nedeniyle hem bu belgeler, hem de Bilgi Toplumu Dairesi Başkanlığı’nın yapmış olduğu çalışmalar büyük öneme sahiptir.

Türkiye’de İnternetle ilgili kurumlardan birisi de ATHGM’dür. Aile yapısının ve değerlerinin, aileyi oluşturan bireylerin korunması kapsamında kötü alışkanlık ve bağımlılık, aile içi şiddet ve istismar, intihar ve benzeri sorunlarla ilgilenmek ve bu konularda inceleme ve araştırma yapmak, bunların önlenmesine ve sorunların çözümüne yönelik, aileyi destekleyici ve eğitici programlar hazırlamak ve uygulamak gibi birçok görevleri bulunan ATHGM, çalışmaları arasına aileyi ve çocukları İnternet’in olası zararlarından korumayı da almıştır. Bu konuda, geçmişte bazı faaliyetler gerçekleştiren ATHGM’nin yakın gelecekte İnternetin sosyal boyutu, çocuk ve aile üzerindeki etkileri ve ortaya çıkan sosyal problemler konusunda daha proaktif bir politika izlemesi beklenmelidir.

Türkiye’de içerik düzenlemesi bakımından 5651 sayılı Kanun’un yürürlüğe girmesi yeni bir dönemi başlatmıştır. Yasa’nın uygulamasından sorumlu kurum olarak TİB, bu kapsamda birçok iş ve işlem tesis etmiştir. Bunlardan birisi olan Bilgi İhbar

Merkezi, faaliyete başladığı 2007 yılından bu yana katalog suçlarıyla mücadele konusunda Türkiye’de önemli bir aktör haline gelmiştir. Merkez’in 2012 yılı sonuna kadar toplamda 558 bin ihbar sayısına ulaşarak dünyadaki benzerleri arasında en fazla ihbar alan birkaç merkezden birisi durumuna gelmesi bunun bir göstergesidir. Bu rakam, ülkedeki İnternet kullanıcılarının içerik düzenlemeleri konusunda aktif olduğu ve katılım sağlamaya çalıştığı şeklinde de yorumlanabilir. Fakat, Merkeze yapılan ihbarların %25’nin katalog dışı içeriklere ait olması dikkat çekicidir. Söz konusu şikayetlerin ayrıca analiz edilip değerlendirilmesi gerekmektedir.

Bilgi İhbar Merkezi intikal eden ihbarları, teknik ve hukuki açıdan değerlendirmekte ve sonuçlandırmaktadır. Merkez, şeffaflığı sağlamak için yapmış olduğu iş ve işlemlere, bağlı bulunduğu mevzuata ve uygulamalarına ilişkin bilgileri kısa ve öz bir şekilde web sitesinde yayınlamaktadır. Ayrıca, İnternet ortamında kişisel hakları ihlal edilen veya dolandırılan kişiler için kısa yönlendirmeler de bulunmaktadır. Diğer yandan Merkez, 2011’de INHOPE’a üye olduktan sonra özellikle çocuk pornografisi ile ilgili uluslararası işbirliği ve bilgi paylaşımı imkanına da kavuşmuştur.

5651 sayılı Yasa’nın uygulamasında TİB’nin en çok eleştiriye maruz kaldığı konu erişim engellemeleridir. Bu Yasa’ya göre Cumhuriyet savcılıkları, ceza mahkemeleri ve TİB belirtilen katalog suçlar kapsamında erişimin engellenmesi kararı verebilmektedir. Fakat, TİB’nin bu kararı verilebilmesi için İnternet sitesinin içerik veya yer sağlayıcısının yurt dışında bulunması gerekmektedir. Yurt içi yayınlarda sadece çocukların cinsel istismarı ve müstehcenlik suçunda hakim onayına sunmak şartıyla TİB engellenme kararı verebilmektedir. Ama, her halukarda verilen erişim engellemesi kararlarının uygulamasını TİB gerçekleştirmektedir. Bu durum, TİB’ni ve erişim engellemesi uygulamalarını sansüre dönüştüğü/dönüşeceği noktasında birçok tartışma ve eleştirilerin odağı haline getirmektedir.

Bu kapsamda; müstehcenlik kavramının belirsizliğinden, sakıncalı içerik yanında sitenin tamamına engellenmesi nedeniyle suç ve cezada orantısızlık bulunduğu, TİB’nca re’sen kapatılan sitelerle ilgili yetki tartışmalarına, yasaklar konusunda

ihtisas mahkemelerinin bulunmamasından, kapatılan sitelere ilişkin bilgi verilmemesi ve savunma hakkı tanınmamasına kadar birçok eleştiri dile getirilmektedir.

Söz konusu eleştirilere karşılık TİB, adli mercilerden gelen talepler ile ihbarlar veya idari tedbir gereği re'sen şüpheli gördüğü içerikleri Yasa'da yer alan usul ve esaslara göre ön inceleme, teknik inceleme ve hukuki değerlendirme işlemlerinden geçirmekte ve bu süreçte, yargı içtihatları yanında, Türkiye'den erişim yoğunluğu ve özellikle çocukların tesadüfen ve doğrudan içeriğe ulaşması gibi kriterleri de göz önünde bulundurarak engelleme kararı verdiğini deklare etmektedir. TİB, bu süreçte verilen kararlarda temel hak ve özgürlüklerin kısıtlanmasının sınırı olarak ortaya konulan “ölçülülük ilkesi”ne uygunluğu gözetmekte olduğunu ve önceliği “uyar-kaldır” mekanizmasını işletmeye verdiğini belirtmektedir. Keza, resen erişimin engellenmesi kararlarını, tamamıyla yasal olmayan içerik barındıran ya da suç unsuru içerikleri çıkarmamakta direnen sitelere uygulamakta olduğunu ifade etmektedir.

TİB, erişim engellemede kullandığı IP'den engelleme yönteminin bazı durumlarda masum içerikleri de engelleme gibi sakıncalarının farkında olduğunu, bu nedenle çocukların cinsel istismarı içerikleri ile ilgili hususlar dışında IP'den engelleme yöntemini çok sıkı şartlar altında, sınırlı olarak tercih edildiğini belirtmektedir. Fakat, TİB'nin daha çok tercih ettiğini duyurduğu alan adı üzerinden erişim engelleme yönteminde de, IP engellemeye göre daha sınırlı olsa da, benzer bir sakınca ortaya çıkmakta; bazen engellenen alan adı içerisinde tek bir sayfada bulunan yasadışı içerik nedeniyle alan adındaki tüm içerik engellemeye uğrayabilmektedir. Bu sakıncanın giderilebilmesi için, URL tabanlı erişim engelleme yöntemi kullanılmalıdır. Lakin, bu sistemin maliyetinin yüksekliği ve İnternette bir takım teknik sorunlara sebep olma potansiyeli, çok daha kolay ve masrafsız olan alan adı üzerinden erişimin engellenmesi yönteminin tercih edilmesine neden olmaktadır. Nitekim, TİB, 2008 yılı Haziran'ında URL tabanlı erişim engelleme konusunda İSS'lar ile çalışmalara devam edildiği yönünde bir açıklama yapmış fakat arkası gelmemiştir.

TİB, yönetimde şeffaflığın sağlanması adına bazı uygulamalar geliştirmiştir. Buna göre, web sitesinde engellemelerle ilgili mevzuat, yapılan işlemler, kararı kimlerin

vereceđi, engellenen site ile ilgili ne yapılabilceđi, erişim engelleme yöntemleri gibi konularda kullanıcılara ve ilgililere kısa bilgiler sunmaktadır. Bunun yanında, engelleme kararlarına karşı itirazda bulunulabileceđini hatırlatarak, ilgili siteye erişimin olup olmadığının sorgulanması için “eekg.tib.gov.tr” adresinden sorgu imkanı sağlamaktadır. Sitede ayrıca, web siteleriyle ilgili özet ve hızlı bilgi elde edilebilmesi için ayrı bir “Site Bilgileri Sorgu Sayfası” oluşturulmuştur.

Bunun yanında TİB açıkça, İnternetin dağıtık ve düzenlenemeyen yapısı nedeniyle kesin bir engellenmenin söz konusu olamayacağını; bunun ancak içeriğın yayından çıkarılmasıyla mümkün olacağı, bunun dışında yapılan her türlü işlemin, erişimi zorlaştıracı tedbirlerden ibaret olacağını dile getirmektedir. Nitekim, Türkiye’de yasaklı olmalarına rağmen bir çok İnternet sitesinin ciddi görüntülenme rakamlarına ulaşmaları ve ktunnel.com, vtunnel.com ve tunnel.com gibi engellemeyi aşmaya yönelik yöntemler sunan tünel web sitelerinin ülkemizde oldukça rağbet görmeleri bu gerçeğın bir kanıtı olarak değeriendirilebilir.

Diğeri yandan, TİB’nın, 2009 yılından bu yana adli mercilerce veya re’sen engellenen İnternet sitelerinin sayısı ve isimleri hakkında bilgi vermemesi eleştirilere konu olmaktadır. Başkanlık, erişim engelleme sayılarına ait bilgileri; kamuoyu tarafından “negatif veya yanlış yorumlanacak” düşüncesiyle, engelli sitelerin isimlerini de; yasadışı içerikle mücadeleyle ilişkin yöntemin ve bu sitelerin isimlerinin deşifresine yol açabilme ihtimalini ve İnternetin doğası geređi söz konusu sitelerin erişiminin tamamen sağlanamayacağı için bu sitelerin adlarının yayınlanmasının adeta suç işlenmesini teşvik etmek anlamına geleceđi gerekçeleriyle açıklamamaktadır.

Engelli sitelerin isim ve sayılarının yayınlanmasıyla ilgili dünya uygulamaları incelendiğinde, ilgili kurumların ve devletlerin genellikle bu tür bilgileri kamuoyu ile paylaşmadıkları görölmektedir. Engelli sitelerin sayılarının yayınlanması konusunda istisna birkaç uygulama dışında, özellikle yasaklı siteler ve filtrelemeye konu kara listeler, TİB’nın taşıdığı endişe ve kaygılara benzer nedenlerle, tüm dünyada genel bir politika olarak gizli tutulmaktadır. Bu bağlamda, TİB’nın, engelli sitelerin isimlerini yayınlama konusundaki endişe ve kaygılarını makul görmekle birlikte, ileri

sürülen tüm gerekçelere rağmen, bu sitelerin sayısal verilerinin yayınlanmasının açıklık politikası ve şeffaf yönetim açısından daha doğru bir tercih olacağı açıktır.

Buna mukabil TİB yayınlamasa da, “Engelliweb.com” gibi bazı İnternet siteleri erişime engellenmiş İnternet sitelerini listelemekte ve istatistiklerini yayınlamaktadır. Buna göre, Türkiye’de 2013 yılı Mayıs ayına kadar, 26 bini re’sen olmak üzere toplam 30 bin sitenin erişimi engellenmiştir. “Engelliweb.com” gibi web siteleri hakkında TİB’nin herhangi bir idari veya hukuki girişimde bulunmaması ve web sitesinde “eekg.tib.gov.tr” adresinden engellenen sitelerin sorgulanmasına imkan sağlaması, TİB’nin bu konuda katı bir tutum içerisinde olmadığını göstergesidir.

Diğer taraftan, TİB, katalog suçları kapsamında re’sen engellediği içeriklerin suç türlerine göre oransal dağılımını “www.guvenliweb.org.tr”de yayınlanmaktadır. Buna göre, başlangıcından 2013 Mart ayına kadar re’sen erişimi engellenen sitelerin dağılımı dikkate alındığında müstehcenlik, çocukların cinsel istismarı ve fuhuş suçları tüm engellemelerin %98,36 gibi büyük bir çoğunluğunu oluşturmaktadır.

5651 sayılı Kanun’un yürürlüğe girmesinden sonra Yasa’ya ve TİB’na ilişkin en yoğun tartışma Atatürk’e hakaret sebebiyle Youtube’un engellenmesiyle ortaya çıkmıştır. 5651 sayılı Kanun’dan önce de mahkeme kararı ile erişimi engellenen Youtube, bu Kanun’dan sonra da mahkemelerce verilen kararlar gereği TİB’nca erişime kapatılmıştır. Türkiye Youtube’u engelleyen tek ülke olmasa da, Youtube’un kapatılması içte ve dışta büyük yankı uyandırmıştır. Başlangıçta TİB, Youtube’la yaptığı birçok görüşmeden sonuç alamasa da, ilerleyen süreçte, kısmi bir uzlaşuya varılmış ve her bir erişim engellemesinden sonra Youtube’un söz konusu içerikleri kaldırmasıyla erişimi tekrar sağlanmıştır.

Youtube’un engellenmesi dışında, dünyaca ünlü alibaba.com, Richard Dawkins sitesi, Google’nin blogger.com ve blogspot.com servisleri, Geocities, Wordpress, myspace.com ve dailymotion.com engellenmeleri Türkiye’de ve dünyada çeşitli tartışmalara ve sansür eleştirilerine neden olmuş ve TİB eleştirilerin hedefi haline gelmiştir. Halbuki, tarafsız olarak incelendiğinde, bu erişim engellemelerinin

tamamının mahkeme kararı ile gerçekleştirilmiş olduğu ve Geocities sitesinin engellenmesi dışında diğer engellemelerin doğrudan ilgili İSS tarafından TİB'nin haberi olmaksızın mahkemenin talebi ile yapıldığı görülmektedir.

Dolayısıyla, uygulamada 5651 sayılı Yasa dışında, telif hakkı ihlalleri, özel yaşamın gizliliği, kişilik haklarını ihlal, Türklüğe hakaret ile terör ve PKK lehine propaganda yapmaktan dolayı mahkemelerin erişim engellemesi kararları vererek doğrudan ilgili erişim sağlayıcılar aracılığıyla bu kararları uygulattıkları görülmektedir. Bu nedenle, Türkiye'deki erişim engellemelerini "5651 sayılı Kanun kapsamındaki engellemeler" ve "5651 sayılı Kanun dışındaki mevzuata göre yapılan erişim engellemeleri" olarak ikiye ayırmaksızın, toptancı bir anlayışla hepsiyle ilgili olumsuzlukları ve eleştirileri 5651 sayılı Kanun'a ve TİB'na yöneltmek doğru olmayacaktır.

5651 sayılı Yasa'nın yürürlüğe girmesinden sonra en çok eleştirilen konulardan birisi de, TİB'nin re'sen uyguladığı erişim engellemeleridir. Bu bağlamda, Anayasa'ya göre haberleşme özgürlüğü ve özel yaşamın gizliliğine müdahaleye ancak bir mahkeme tarafından karar verilebileceği; bu nedenle yapılan idari işleme ilişkin olarak idare mahkemelerine itiraz yolu açık dahi olsa, ortaya çıkan bu Anayasal eksikliğin giderilemeyeceği iddia edilmektedir. Nitekim, bu nedenle bazı STK'ları, 5651 Sayılı Yasaya istinaden çıkartılan yönetmeliklerin iptali için Danıştay'da dava açmıştır. Fakat henüz Danıştay'dan herhangi bir iptal kararı gelmemiştir.

Diğer yandan, yasadışı ve zararlı içerikle mücadele kapsamında, idari kurumların kararlarıyla doğrudan veya yönlendirmeleriyle dolaylı olarak "öz düzenleme" çerçevesinde "zorunlu gönüllük" şeklinde ya da sektördeki büyük şirketlerle özel anlaşmalar yapma yoluyla, erişim engelleme veya filtreleme yapılmasına ilişkin uygulamaların tüm dünyada yaygın olarak kullanıldığına dair örnekler bir hayli fazladır. Nitekim, AB üyesi İngiltere, Almanya, Fransa, Finlandiya, Danimarka, İsveç ve Norveç'te bu kapsamda birçok uygulama göze çarpmaktadır.

Türkiye'de erişim engellemelerinin hukuksal boyutu üzerindeki eleştirilerin bir kısmı da, ihtisas mahkemelerinin bulunmamasına ilişkindir. Sadece bir iki büyük şehirde,

geniş bir bilirkişi desteğiyle kurulacak ihtisas mahkemelerinin kapatma kararlarında daha seçici davranabileceği ve kararların daha sağlıklı verileceği öngörülmektedir.

Erişim engellemelerine ilişkin eleştiriler TİB'nı, tüm kullanıcıları kapsayan zorunlu uygulamalardan ziyade kişisel tercihe dayalı seçenekli alternatif uygulamalara yöneltmiştir. Bu kapsamda; “seçmek özgürlüktür” sloganı ile Güvenli İnternet Hizmeti sunulmuş ve yapılan düzenleme ile Türkiye’de faaliyet gösteren tüm erişim sağlayıcılar bu hizmeti abonelerine ücretsiz olarak vermekle yükümlü kılınmıştır. 22.11.2011 tarihinde başlatılan bu hizmette, Çocuk ve Aile Profil Kriterleri Çalışma Kurulu tarafından tespit edilen kriterlere göre TİB’in hazırladığı beyaz, gri ve siyah listeler esas alınmaktadır. Bu listeler referans alınarak İnternet kullanıcılarına çocuk ve aile profillerini seçme özgürlüğü getirilmiştir.

Güvenli İnternet hizmeti, hazırlık aşamasında ve uygulamaya geçildikten sonra bazı kesimlerce devlet eli ile merkezi filtre uygulaması ve yeni bir sansür girişimi olarak görülerek yoğun olarak eleştirilere maruz kalsa da, ilgiyle karşılanmış ve 1 yıl içinde 1,4 milyon abone ve yaklaşık 5 milyon kullanıcı sayısına ulaşmıştır.

5651 sayılı Kanun ile TİB tarafından uygulamaya konulan ve olumlu netice alınan işlemlerden birisi de uyar-kaldır yöntemi ile içeriğin yayından kaldırılmasıdır. Yasa’nın 9. maddesi ile düzenlenen ve Basın Yasası’ndaki “Düzeltilme ve cevap” mekanizmasını İnternet ortamında yapılan yayınlara taşıyan uygulama, İnternet ortamındaki yayın içeriği dolayısıyla hakları ihlal edilen kişilere, içerik veya buna ulaşamaz ise yer sağlayıcısından içeriğin yayından çıkarılmasını talep etme ve cevap hakkını düzenlenmiştir. Düzenleme, hakkı ihlal edilen kişilere, söz konusu ilk başvurusu neticesiz kalması halinde yargı yoluna başvurma imkanı sunmaktadır.

TİB, hakları ihlal edilen kişilerin muhataplarını tespitde faydalı olabilecek bilgi kaynaklarına erişimleri konusunda yardımcı olmaktadır. İlk olarak, 5651 sayılı Yasa ve ikincil düzenlemeleri içerik, yer ve erişim sağlayıcılara iletişim bilgilerini İnternet ortamında herkesin göreceği bir şekilde yayınlama zorunluluğu getirerek sorumluların İnternetin anonimliğinden yararlanmasının önüne geçmeye çalışmakta

ve bu yolla mağdurlara yardımcı olmaktadır. İkinci olarak ise, ilgili düzenlemeler gereği TİB’ndan faaliyet belgesi almış yer sağlayıcılar ile yetkilendirilmiş olan erişim sağlayıcıların listesini ve iletişim bilgilerini resmi İnternet adresinde yayınlarak, tespit olunan ilgililerin erişim ve yer sağlayıcı olarak Başkanlık kayıtlarında yer alıp almadığını sorgulama ve kayıtlı olanların iletişim bilgilerine ulaşılabilme imkanı sunmaktadır. TİB ayrıca, yine kendi İnternet sitesinde yer alan site bilgileri sorgu sayfasından talebe konu adreslerle ilgili olarak açık kaynak bilgi sorgusu yapılabilmesine imkan sağlamaktadır.

Diğer yandan TİB, bu düzenlemeye dayanarak herhangi bir erişimin engellenmesi kararı verilmeden önce suç unsuru bulunan kısmi içeriklerin yer aldığı İnternet siteleriyle, ulaşılabilir iletişim bilgileri üzerinden irtibata geçmekte ve “uyar-kaldır” yöntemi ile yalnızca suça konu içeriğin kaldırılmasını temin etmektedir. Nitekim, TİB’nca gerçekleştirilen uyar-kaldır işlemleri ile 2012 yılı sonu itibariyle yayından kaldırılan içeriklerin sayısı 130 bini geçmiştir. TİB’nın Yasa’da yer alan bu imkanı kullanarak, yasadışı ve zararlı içerikle mücadelede erişim engellemeden ziyade tüm dünyada kabul gören bu sisteme öncelik vermesi yerinde bir tercih ve yaklaşımdır.

5651 sayılı Yasa ve ilgili yönetmelikler, İnternet kafelere TİB tarafından onaylanan içerik filtreleme programlarından birisini kullanma mecburiyeti getirirken, TİB’na da bu programların asgari ölçütleri ve yöntemlerini belirleme görevi vermiştir. Nitekim TİB onaylama kriterleri ile bu kriterlere ve teknik özelliklere uygun üretilen ve onayladığı filtre programlarını resmi web sitesinde yayınlamaktadır. Ayrıca İnternet kafeler ile ilgili olarak bir iç IP dağıtım loglama yazılımı hizmeti sunulmakta ve bu yazılım ücretsiz olarak indirilip kurulabilmektedir.

5651 sayılı Kanun ve ilgili yönetmeliklerle Katalog suçları ile mücadelede getirilen en önemli yeniliklerden birisi, İnternetin önemli aktörlerini ilk kez tanımlanması ve bu aktörlere ilişkin yükümlülöklere ve müeyyidelere ayrıntılı olarak yer vermiş bulunmasıdır. Bu kapsamda TİB, yer sağlayıcılara faaliyet belgesi verilmesi, barındırdıkları alan adlarına ilişkin dosyaların kontrolü ve alan adlarının veri tabanına aktarılması, içerik, yer ve erişim sağlayıcıların tanıtıcı bilgilerini web

sitelerinde bulundurmalarının takip edilmesi ve faaliyetini sonlandıran erişim sağlayıcıdan trafik bilgilerinin temini gibi işlemleri yürütmektedir. Nitekim TİB’in 2012 yılı sonuna kadar verdiği yer sağlayıcı belgesi sayısı 2.783’ü bulmuştur.

Diğer yandan, İnternet ortamındaki yasa dışı içerikler ile mücadelede içeriklerin yurtdışına kaçmaması ve kayıt dışılığa engel olmak için, yurtiçi yer sağlayıcılık hizmetlerinin vergi yükünün azaltılması, altyapının geliştirilerek bağlantı hızının artırılması ve kayıtlı yer sağlayıcılara, özel bir tarife üzerinden elektrik enerjisi verilmesi gibi politikalarla teşvik edilmesi gerekmektedir. Bunun yanında, ülkede izinsiz bir şekilde bu hizmeti verenlerle ilgili caydırıcı yasal düzenlemeler de yapılmalıdır. Ayrıca, kendisi ile irtibat kurulamayan ve çocuk pornografisi içerikleri barındıran sunucunun İnternet omurgasına bağlanmasını sağlayan İnternet aboneliğinin erişimi abonelik iptali yolu ile kesilebilmelidir.

TİB, İnternetin güvenli kullanımına yönelik olarak kendisine bilinçlendirme faaliyetleri kapsamında verilen birçok görev ve sorumluluklar çerçevesinde aileler, eğitimciler, çocuklar için zengin içeriklerle desteklenen, “Güvenliweb” adındaki bilinçlendirme sitesi ile, çocuklara yönelik “Güvenliçocuk” web sitesiyle hizmet vermektedir. Keza, toplumda bilişim şuurunu geliştirmek ve güvenli İnternet kullanımı konusunda farkındalık oluşturmak amacıyla çocuklara ve ebeynlere yönelik rehber kitapçık ve broşür dağıtımı gerçekleştirmekte, etkinlikler, toplantılar ve seminerler düzenlemektedir.

Yine TİB, ilgili mevzuat gereği, bilişim ve İnternet alanındaki faaliyetler ile ilgili yurt içi ve yurt dışı gelişmeleri takip etmeye, bu kapsamda ulusal ve uluslararası kurum ve kuruluşlarla işbirliği ve koordinasyonu sağlamaya yönelik çalışmalar yapmaktadır. Bu çerçevede, TİB, AB Güvenli İnternet Programını takip etmekte, programda öngörülen hedeflere uygun çalışmalar yapmakta ve AB Komisyonu Bilgi Toplumu ve Medya Genel Müdürlüğü ile irtibatlı olarak çalışmalar hakkında bilgi alışverişinde bulunmaktadır. Nitekim yapılan çalışmalar sonucunda Türkiye AB’nden “Safer Internet Programme”na katılım daveti almıştır.

Son olarak, Türkiye'nin içerik düzenlemesi uygulamalarını, bu düzenlemelerin meşruiyetini normatif olarak değerlendirmede kullanılan Bambauer'in açıklık, şeffaflık, kısıtlılık ve sorumluluk ölçütleri bağlamında değerlendirerek, Türkiye örneğine ilişkin analitik bir analiz yapılmış ve nesnel sonuçlara ulaşılmaya çalışılmıştır. Buna göre sonuçlar bir bütün olarak değerlendirildiğinde; "kısıtlılık" ölçütünün kullanılmasıyla beliren olumsuz sonuçlar dışında erişim engellemesi uygulamalarımız açısından genel olarak önemli bir sorun gözükmemektedir. Dolayısıyla, Türkiye'deki erişim engellemesi uygulamalarının "kısıtlılık" konusu dışında ciddi bir meşruiyet sorununun olmadığı söylenebilir.

Sonuç olarak, dünyada birçok ülkede İnternet için özel bir düzenlemenin eksikliği devam ederken, Türkiye'de 5651 sayılı özel yasa ve yönetmelikleri ile İnternet aktörlerinin tanımlanmış, sorumluluklarının belirlenmiş ve içerik çıkarma "uyar-kaldır", erişim engelleme usul ve esaslarının yasal düzeyde belirlenmiş olması, temel hak ve özgürlüklere ilişkin sınırlamaların yasa ile yapılması gerektiği şeklindeki uluslararası ilkeye uygunluk açısından önemlidir. Böylece, ülkemizin demokratik ülkelerin birçoğundan bir adım öne geçmiş bulunduğunu, dolayısıyla, söz konusu Yasa ve bu Yasa'nın uygulayıcısı olan TİB, süreç içerisinde bazı uygulamalarından dolayı eleştirilse de, içerik düzenlemeleri açısından Türkiye'nin attığı bu adımın genel olarak olumlu görülebileceği söylenebilir. Fakat bunun yeterli olmadığı, İnternetin tüm boyutları ile ele alınarak oluşturulacak bütüncül bir İnternet politikası çerçevesinde içerik düzenlemesi konusunun değerlendirilerek konuyla ilgili yeni bir yol haritasının çıkartılması gereği vardır.

Türkiye örneği bir bütün olarak değerlendirildiğinde, onaltıncı alt hipotezde belirtildiği gibi, Türkiye'nin İnternet içerik düzenlemesine ilişkin uygulamasının, eleştiri konusu yapılacak bazı eksiklikler barındırmakla birlikte, yasadışı ve zararlı içeriklere devlet eli ile sınırlı müdahaleyi öngören kendine özgü ve önemli bir uygulama olma karakterini ortaya koymaktadır.

Sonuç olarak, Tezin bütünü, tüm alt hipotezler üzerinden geçerliliği ve doğruluğu test edilmeye çalışılan temel hipotez bağlamında değerlendirildiğinde, içerik

düzenlemesi sorununun mahiyetine ve çözümüne ilişkin öngörülerin genel olarak isabetli olduğunu iddia etmek yanlış olmayacaktır. Zira, alt hipotezlerin tartışılmasından ve değerlendirilmesinden, içerik düzenlemesi sorununun İnternetin kendine özgü doğasından kaynaklı olarak çok boyutlu, karmaşık, dinamik ve çözümü bir çok değişkene bağlı zor bir sorun olduğu sonucu ortaya çıkmaktadır.

Bunun yanında, özellikle çocukların, gençlerin ve ailelerin İnternette yer alan yasadışı ve zararlı içeriklerden korunması için bu tür içeriklerle mücadele edilmesinin gereği de başka bir gerçeklik olarak kendisini hissettirmektedir. O halde, İnternetin daha faydalı, bilinçli, güvenli ve etkin kullanılmasını sağlamak için İnternet içeriğine yönelik düzenlemeler yapılması, İnternetin bu yönü ile denetlenmesi kaçınılmaz bir zorunluluk olarak karşımıza çıkmaktadır.

Alt hipotezlerin değerlendirilmesinden, kamu ototritelerinin bu zorunluluğun gereğini yerine getirirken; İnternetin kendine özgü yapısını ve özelliklerini dikkate alarak, İnternetin gelişimine zarar vermeden, İnternete erişim özgürlüğünü ve bu kapsamda ifade özgürlüğü ve bilgiye erişim özgürlüğünü kısıtlamadan ve fakat, farklı kullanıcı tercihlerine de cevap verecek uygulamaları geliştirme zorunlulukları da ortaya çıkmaktadır. Yine, tüm bu süreçlerin İnternetin tarafı olan kamu-özel-STK bütün kesimlerin katılımı ile birlikte düzenleme anlayışı içinde yürütülmesi de diğer bir gereklilik olarak kendisini göstermektedir.

Alt hipotezlerle ulaşılan diğer bir gereklilik de, tüm bu temel prensipler üzerine bina edilmiş bütüncül bilgi toplumu ve İnternet politikalarının oluşturulması ve uygulanmasıdır. Buna göre, İnternet içerik düzenlemeleri, bahsi geçen prensiplere göre oluşturulacak ve en uygun yöntem ve yaklaşımları ihtiva eden bütüncül İnternet strateji ve politikalarının bir parçası olmalıdır. Keza, konunun diğer boyutu da uluslararası işbirliği mekanizmalarının kurulması ve işletilmesi zorunluluğudur. Fakat, tüm bu gereklilikler yerine getirilmiş olsa dahi, alt hipotezler üzerinden yapılan tartışma ve değerlendirmeler göstermektedir ki, yasadışı ve zararlı içerikleri tamamen önlemek mümkün değildir. Ama, minimize etmek mümkündür.

SONUÇLAR

Tezde temel hipotezimiz ve alt hipotezlerimiz üzerinden “Devlet eli ile İnternet içerik düzenlemesi sorunu ve TİB örneği” konusu ele alınmış, analiz edilmiş ve değerlendirilmiştir. Bu kapsamda, tez içerisinde tartıştığımız doğruluğunu ve geçerliliğini değerlendirdiğimiz alt hipotezlerimizle ilgili olarak ulaştığımız sonuçlar aşağıda yer almaktadır. Ulaşılan sonuçlara verilen her bir numara, aynı numaralı alt hipotezin karşılığı ulaşılan sonucu göstermektedir.

1. Teknolojik yenilikler toplumların ekonomik, sosyal, siyasal ve kültürel yapılarını belirli bir süreç içerisinde değiştirmekte ve dönüştürmektedir. İnternetin muharrik gücünü oluşturduğu ve daha sonra neredeyse kendi rengini verdiği bilgi ve iletişim teknolojilerinin ortaya çıkarak hızla gelişmesiyle tarihte benzeri görülmemiş köklü değişim ve dönüşümler meydana gelmiştir. İnsanlığın teknolojik gelişim tarihi içinde “bilgi toplumu” olarak adlandırılan bu yeni dönemde, söz konusu köklü değişim ve dönüşümler yeni yönetsel ve hukuksal sorunlar ortaya çıkarmış ve çıkarmaya devam etmektedir. Bu çerçevede, tezin birinci alt hipotezinde belirtildiği gibi, İnternetin içerik düzenlemesi sorununu da, İnternetin gelişmesi ve yaygınlaşmasıyla gündeme gelen bir “bilgi toplumu” sorunu olarak ele almak ve bu arka plan ve bağlamı içinde değerlendirmek gerekmektedir.

2. Nasıl ki, sanayi devrimi, sanayi toplumunu ve ona uygun kamu yönetimi anlayışını ortaya çıkartmış ise, bilgi ve iletişim teknolojilerindeki gelişmeler de bilgi toplumunu ve ona uygun yönetim yapısını ortaya çıkartmıştır. Varacağı son nokta ve etkileri hala tam olarak kestirilemeyen bilgi toplumu sürecinden devlet/kamu yönetimi derinden etkilenmiş ve etkilenmeye devam etmektedir.

Diğer yandan ise, “devlet/kamu yönetimi”, “bilgi toplumu” ile gündeme gelen İnternetle birlikte ortaya çıkan güvenlik, içerik düzenlemesi, mahremiyet gibi yeni sorun alanlarına ilişkin belirsizlik ve dönüşümlere yanıt ve çözümler üretmeye, gelişen kavram, yapı ve yaklaşımları doğasına uyarlamaya çalışmaktadır. Nitekim, süregelen bu etkileşim sürecinin İnternet içerik düzenlemesini ilgilendiren en somut

sonucu, “yönetişim” modelinin ortaya çıkması ve bu çerçevede İnternetin düzenlenmesi konusunun “düzenleyici kurullar”a havale edilmesi olmuştur. Dolayısıyla, tezin ikinci alt hipotezinde bahsi geçen etkileşim süreci ve İnternet içerik düzenlemesi sorun alanını ilgilendiren sonuçlarına ilişkin tespitin yanlış olmadığı gözükmemektedir.

3. Objektif olarak değerlendirildiğinde, bilgi toplumu insanlık için bir çok imkan, fırsat ve fayda sağlarken, “gözetim toplumu” olma, sayısal uçurum, güvenlik ve risk kaygıları, yabancılaşma ve tüketim çılgınlığı, bilgi kirliliği ve enformatik cehalet gibi sorunlar ile, İnternetle gelen yasadışı ve zararlı içerik, siber güvenlik, mahremiyet ihlalleri ve tüm bunların sebep olduğu bir takım sosyal, kültürel, psikolojik ve fizyolojik problemlerin ortaya çıktığı görülmektedir. Keza, bilgi toplumu kuramına da, çok köklü ve ciddi eleştiriler söz konusudur.

O nedenle İnternet içerik düzenlemesi sorunun çözümüne ilişkin ipuçlarını yakalayabilmek için tamamlanmamış bir süreç olsa da “bilgi toplumu” olgusunun, hiçbir öznel değer yargısı ve peşin hüküm katmadan, olanca nesnelliği içinde ve objektif olarak, sunduğu fırsatlar ile riskler ve tehditler, güçlü yönleri ile zayıf yönleri, getirdiği faydaları ile zararları, imkanları ile sorunları bakımlarından bütüncül bir bakış açısıyla ele alınması gerekmektedir.

Bilgi teknolojilerinin toplum üzerindeki belirleyici etkisiyle şekillenen bilgi toplumunu sadece sunduğu fırsatlar, güçlü yönleri, faydaları, imkanları açısından tek yönlü olarak değerlendirmek, bilgi toplumu modelinin gündeme getirdiği sorunları ve taşıdığı potansiyel riskleri ve tehlikeleri görmemize engel olacaktır. Bu nedenle, bilgi toplumu olmanın getirdiği sorunları, başka bir ifadeyle bilgi toplumu olmanın maliyetlerinin neler olduğunun objektif olarak irdelenmesi ve tespit edilmesi gerekmektedir. Bu yaklaşım, bütüncül bilgi toplumu ve İnternet politikaları oluşturulmasına zemin hazırlarken, bu bütünün bir parçası olarak içerik düzenleme kararlarının ve uygulamalarının da daha doğru, yerinde ve etkili olmasını sağlayacaktır. Aksi takdirde, tezin üçüncü hipotezinde de belirtildiği gibi, bilgi toplumu ve İnternetin risk ve sorunları görmezden gelinerek üzerinin örtülmesine ve

dolayısıyla, bilgi toplumu ve İnternet politikalarının eksik ve yanlış temeller üzerine oturmasına neden olacaktır. Bu da, yasadışı ve zararlı İnternet içeriği ile ilgili mücadeleyi düşünce ve uygulama olarak zayıflatacaktır.

4. Yapılan araştırmalar, bilimsel çalışmalar, yayınlanan raporlar, yaşanan tecrübeler ve vuku bulan olaylar İnternetin; güvenlik ve mahremiyet ihlalleri, yasadışı ve zararlı içerikler ile İnternetin yanlış kullanımından kaynaklanan birçok risk, tehlike ve toplumsal soruna neden olduğunu ortaya koymuştur. Hızla gelişen ve yaygınlaşan İnternetin denetimden uzak yapısı, İnterneti, illegal ve zararlı pek çok iş ve oluşumun yeni buluşma alanı haline getirirken, İnternetin yanlış ve bilinçsiz kullanımı sorunları daha da artırmaktadır.

Bu kapsamda, İnternet, bilişim suçları olarak da adlandırılan bilgisayar sistemlerine ve servislerine yetkisiz erişim, bilgisayar sabotajı, bilgisayar yoluyla dolandırıcılık ve sahtecilik, izinsiz yazılım kullanımı, telekomünikasyon hizmetleri hırsızlığı, bilgisayar sistemlerinin suç ve terör örgütleri tarafından kullanılması, tehdit ve gasp, siber saldırılar, casus yazılımlar, bilgisayar virüsleri, solucanlar (spamlar), truva atları (trojenler), phishing (oltalama), botnetler gibi suç çeşitlerinin ve dijital tehlikelerin hayatımıza girmesine sebep olmuştur.

Keza, İnternet teknolojilerinin gelişmesi, hükümetlere, küresel büyük şirketlere (Microsoft, Facebook gibi), kişilere ve suç örgütlerine kişilerin telefon ve İnternet iletişimini takip etme, dinleme ve izleme, kişisel verilerin istismarı ve bireysel haberleşmeye izinsiz giriş konularında yeni imkanlar sağlamıştır. Bunun sonucunda mahremiyet ihlalleri ve riski tarihin hiçbir döneminde olmadığı kadar artmıştır.

Diğer yandan, İnternet içeriklerinin önemli bir kısmını; pornografi ve çocuk pornografisi, fuhşa aracılık, ırkçılık, ayrımcılık, kumar oynamaya ve uyuşturucu kullanmaya teşvik, şiddet, vahşet, nefret ve intihara yönlendirme içerikleri ile telif hakkı ihlallerine ait yasadışı ve zararlı içerikler oluşturmaktadır. İnternet, söz konusu içeriklere kolay ve sınırsız erişim imkanı sağladığı için birçok toplumsal riskler ve

sorunlar ortaya çıkmaktadır. Dolayısıyla, yasadışı ve zararlı İnternet içerikleri bir bütün olarak toplumu ve özellikle çocukları, gençleri ve aileleri tehdit etmektedir.

Söz konusu yasadışı ve zararlı içeriklerden özellikle pornografik içerikler her türü ile (çocuk, genç, ergen, ekstrem pornografi vb.) kolay, hızlı, ucuz ve sınırsız bir şekilde ulaşılma, çoğaltılma ve paylaşılma imkanına kavuştuğu için tarihin hiçbir devrinde olmadığı kadar yaygınlaşmış ve kullanımı artmıştır. Bu durum, pornografiyi, özellikle çocuklar, gençler ve aileler üzerinde meydana getirdiği olumsuz etkiler nedeniyle adeta küresel bir sorun haline getirmiştir. Pornografi, çocukların cinsel istismarı başta olmak üzere, cinsel şiddeti ve cinsel suçları artırma, bağımlılık oluşturma, ailede eşler arası huzursuzlukları, aldatma ve boşanmaları artırma, erkeklerin kadınlarla ilgili yanlış cinsel algı ve düşüncelere sahip olmasına neden olma gibi sonuçlar doğurması yanında, küçük yaşta çocukların pornografiyle tanışmasından dolayı yüksek toplumsal maliyetler de oluşturmaktadır.

Günümüzde, ülkelerin genel olarak pornografi ve türleri konusunda farklı yaklaşım içinde olmaları ve ortak bir anlayış ve tavır ortaya konulamaması, tüm dünyada pornografinin toplumsal maliyetlerinin gün geçtikçe daha da artırmasına neden olmakta ve sorunu büyötmektedir. Bu sonucun ortaya çıkmasında; çocuk ve yetişkin pornografisi/fahişeliği/seks turizmi ve insan kaçakçılığı gibi birbirini üreten ve büyüten sektörlerin yerel, bölgesel ve küresel ölçekteki yakın işbirlikleri ile pornografik ürünlerin üreticileri ve dağıtıcıları yanında, bankalarını, yazılım üreticilerini, kredi kartı firmalarını, İnternet sağlayıcıları, kablolu yayıncılık yapan şirketleri ve otel zincirlerini de içine alan ve silsile olarak birbirine bağlı, trilyonlarca dolarlık büyük bir pastayı paylaşan devasa bir endüstrinin, toplumsal maliyeti ne olursa olsun, daha çok kazanmak ve kar elde etmek için var gücü ile çalışmasının ve pornografinin yayılmasının önündeki toplumsal, kültürel ve yasal tüm engelleri aşmaya, dirençleri kırmaya çaba göstermesinin önemli bir etkisi vardır.

Keza, Pornografik içeriklerin İnternette serbestçe dolaşımının devam etmesini sağlamak için konuyu “İnternet özgürlüğü” ve “ifade özgürlüğü” bağlamına ve alanına çekme çalışmalarını da pornografi sektörünün bu kapsamdaki uğraşı ve

stratejilerinden birisi olarak görülmelidir. Fakat, pornografiye sınırsız dolaşım ve erişim özgürlüğünün ifade özgürlüğü ve İnternet özgürlüğü kapsamında değerlendirilmesinin mümkün olamayacağı genel olarak kabul gören bir görüştür. Bu çerçevede, tezdeki dördüncü alt hipotezimizin yerindeliliğinin tespiti ile, tüm yasadışı ve zararlı İnternet içerikleri yanında her tür pornografik içerikle, temel hipotezimizde belirtilen sınırlar içerisinde, ulusal ve uluslararası ölçekte mücadele edilmesi gerekliliği bir kez daha teyit edilmiş olacaktır.

5. Çok boyutlu/ aktörlü ve dinamik yapısı ile kendine özgü doğası olan İnternetin en önemli özelliklerinden birisi ulusal sınırları aşarak belirli bir yer veya coğrafyaya bağlı kalmamasıdır. Dolayısıyla, içerik düzenlemesiyle ilgili önemli parametrelerinden birisini İnternetin uluslararası yönetimi ve işbirliği konusu ve sorunu oluşturmaktadır. İnternetin kötüye kullanılmasını önlemek, güvenliğinin, güvenilirliğinin ve istikrarının sağlanması, telif hakları, zararlı içeriğin önlenmesi, veri gizliliği ve güvenliği, kültürel ve dilsel çeşitliliğin sağlanması için İnternetle ilgili uluslararası düzenlemeler yapılması ve işbirliği geliştirilmesi gereğine karşın, İnternet ağının tamamını kontrol eden ve yaptırım uygulamaya yetkili, meşru, tarafsız ve yasal bir uluslararası merkezi otorite bulunmaması, İnternetin küresel ve merkezi olmayan yapısının getirdiği en önemli sorunlardan birisidir.

Zira, çeşitli kuruluşların işbirliğinden ve karmaşık ilişkiler bütününden oluşan mevcut çok aktörlü yapı, başta ABD olmak üzere, İnternetin mucidi ve teknoloji geliştiricileri olan ve siber uzayın temel mimarisini şekillendiren devletlerin politikaları doğrultusunda bu mimariye uygun olarak oluşturulmuştur. Bu mimari, söz konusu devletlerin etki ve etkinliği dışında, üzerinde tamamını kontrol eden tek bir ulusal veya uluslararası yasal bir otorite veya merkezi bir kural koyucu bulunmama prensibine göre şekillendirilmiştir. Bu devletler, büyük oranda, bu alanın regüle edilmesinde de egemenliklerini sürdürmekte, özel ve kamusal güçleriyle bu alanın sınırlarını ve kurallarını belirlemeye devam etmektedir.

Nitekim, günümüzde İnternetin yönetiminde önemli iki kurum olarak ortaya çıkan ICANN ve IANA'nın, uluslararası meşruluğunun bulunmadığı, ABD etkisinde

kalmaları sebebiyle, yapılanma şekillerinin ve karar alma süreçlerinin İnternet politikalarının taraflı oluşmasına neden olduğu bilinmektedir. Keza, ABD, İnternet üzerindeki hakimiyetini ve İnternetin yönetimi ile ilgili sahip olduğu yetkilerini elinde tutmak istemektedir. ABD, askeri iletişim stratejisinin bir parçası olarak ortaya çıkardığı İnterneti, güvenlik stratejisinin bir parçası olarak kullanmaya devam etmekte ve bu nedenle İnternet üzerindeki egemen konumunu korumayı ekonomik ve ulusal güvenlik menfaatleri için gerekli görmektedir.

Buna karşılık, İnternetin tüm dünyada yaygınlaşmasıyla; bir yandan, İnternetin sosyal, siyasal ve ekonomik hayatı yönlendiren etkili bir araç olduğunun farkına varan devletlerin, İnternet üzerindeki etkilerini ve etkinliklerini hem ulusal hem de uluslararası düzeyde artırmaya çalışmaları, diğer yandan, e-ticaretin artması, telif hakları, yasadışı ve zararlı içeriğin önlenmesi, İnternetin ulusal güvenliğin bir parçası olarak görülmesi, kültürel ve dilsel çeşitliliğin sağlanması gibi nedenlerle alan adları ve IP adreslerinin yönetimi büyük bir menfaat çatışması ve mücadeleye konu olmuş ve İnternetin uluslararası yönetimi önemli bir sorun haline gelmiştir.

Bu ve benzeri nedenlerden dolayı bu sorunla ilgili olarak uluslararası toplum “İnternet Yönetişimi” kavramını ortaya atmış ve savunmuştur. Fakat, bu gün için henüz devletlerin İnternet yönetişimi konusunda gittikçe artan taleplerini tatmin edecek düzeyde bir yapılanmaya gidilebilmiş değildir.

Bu çerçevede, çok boyutlu/aktörlü İnterneti her yönü ile ve bütünlüğü içerisinde kavrayacak ve uluslararası sahipliğini yapacak gerçek anlamda yetkili ve etkili bir uluslararası merkezi kuruluşa olan ihtiyaç açıkça kendisini göstermektedir. İnternetin küresel ağ olma özelliğinin korunmasını sağlayacak şekilde, IP tahsisi, protokol parametrelerinin belirlenmesi, kök sunucu ve alan adı sisteminin yönetimi de dahil olmak üzere, İnternetin uluslararası mekanizmalarının yönetimini ve temel politikalarının belirlenmesiyle ilgili görevleri de üstlenecek bu çatı örgüt, devletlerin eşit olarak temsilini esas alan bir yapıda olmalıdır. İnternetin uluslararası yönetimine uluslararası meşruiyet getirecek bu örgütte, İnternet yönetişimi yaklaşımına göre sektör ve kullanıcıları temsil edecek STK’ları da yer almalıdır. ABD egemenliğine

dayalı mevcut sistemdeki ICANN ve IANA gibi kuruluşların görev ve yetkileri bu yeni uluslararası kuruluşa devredilmelidir.

Yeni örgüt, İnternetin uluslararası yönetimini, İnternet tarafsızlığını gözeterek, çok taraflı, şeffaf, dengeli, tutarlı ve demokratik bir biçimde gerçekleştirmeli, adil bir kaynak dağılımının sağlanmasını, herkesin kendi dilinde erişiminin kolaylaştırılmasını ve İnternetin istikrarlı ve güvenli şekilde çalıştırılmasını temin etmelidir. Bu kuruluş BM'e bağlı ITU'nün bünyesinde olabileceği gibi, ayrı bir örgütsel yapı da oluşturulabilir. İnternet yönetişimi temelinde gerçekleştirilecek olan bu yeni yapılanmanın nasıl olabileceği veya nasıl olması gerektiği konusunda bugüne kadar yapılan tartışmalar, yürütülen çalışmalar, hazırlanan raporlar ve yapılan yayınlar, yeni dönemin şekillendirilmesine ilişkin yeterli zengin fikir, teklif ve veriye sahiptir. Bu konuda eksik olanın, ABD'nin karşı direncini kırarak uluslararası güçlü bir iradenin ortaya konulması olduğu gözükmektedir.

Bu yeni örgüt ve kuracağı yeni sistemin İnternet içerik politikalarının da çerçevesini oluşturacak bir platform olması; bu sanal ortamın zararlı tesirlerinden korunmak ve işlenen suçlara karşı mücadele etmek için gerekli olan uluslararası işbirliği ve her ülke için geçerli olacak yeknasak kurallar belirlemede öncü olması beklenmektedir. Bu çerçevede, yönetim yaklaşımı içinde yasadışı ve zararlı içeriklerin tür ve kapsamı ile mücadele yöntemlerinin uluslararası toplumca uzlaşıya varılan asgari sınırlarının belirlenmesi mümkündür.

Bu durumda, bu uzlaşının, yasadışı ve zararlı içeriklerle mücadele konusunda bugün ihtiyaç duyulan işbirliği ve koordinasyon sorunlarını büyük oranda çözecek bir mekanizma veya kurumsal yapıya dönüşmesi ihtimali daha da güçlenecektir. ABD'nin mevcut uluslararası sistemdeki egemen konumu devam ettiği sürece, yakın zamanda gerçekleşmesi zor gibi gözükse de, İnternet ortamındaki yasadışı ve zararlı içeriklerin en aza indirilmesi konusunun en önemli parametrelerinden birisini oluşturan bu adımın uluslararası toplumun baskısı ile atılması zarureti kaçınılmaz olarak karşımızda durmaktadır. Bu nokta tam da tezin beşinci alt hipotezinin işaret ettiği hususlarla örtüşmekte ve hipotezi doğrulamaktadır.

6. İlk zamanlarda tamamen bir özgürlük alanı olarak kabul edilen İnternet günümüzde, dünyanın hiçbir ülkesinde sınırsız bir özgürlük alanı olarak görülmemektedir. Zaman içinde İnternetin ortaya çıkarttığı risk ve sorunlar, devletlerin İnternetin gücünü fark etmeleri devletleri İnternetle ilgili daha çok kural koymaya ve denetlemeye itmiştir. Bu nedenle, teori ve uygulamada yöntem ve kapsam farklılıkları olmakla birlikte, her ülkede İnternetin güvenli kullanımını sağlamak amacıyla İnternet içeriğiyle ilgili “önlem” ve “müdahaleleri” kapsayan düzenlemeler yapılmaktadır. Keza, söz konusu düzenlemeler zaman içinde giderek artmakta, önlem alınan konuların sınırları genişlemekte, sayısı fazlalaşmaktadır. Devletler ulusal çıkarlarını ve toplumsal değerlerini korumak için düzenleme yapılmasını kaçınılmaz görmekte, çocuk ve aileyi, genel ahlakı İnternette gelen her türlü yasadışı ve zararlı içeriğe karşı korumak için aktif rol oynamaya yönelmektedir.

Fakat, diğer yandan, devletler İnternetin düzenlenmesinde ve denetiminde bir takım zorluklar yaşamaktadırlar. Bu zorlukların en önemlisi de İnternetin, klasik ulusal egemenlik anlayışlarına meydan okuyan çok yönlü ve aktörlü, karmaşık, dinamik ve sınır tanımayan küresel yapısıdır. Devletlerin ülke sınırları içerisinde vatandaşlarına hukuk kuralı koyma ve bunu uygulama meşruiyetlerini esas alan klasik ulusal egemenlik yaklaşımlarını, vatandaşlık, ulusal sınır gibi kavramları geçersiz kılan bu teknoloji, altıncı alt hipotezde belirtildiği gibi, devletlerin kontrol altına alma kanallarını ve girişimlerini oldukça zorlamaktadır. Dolayısıyla, İnternet teknolojisi bugün, İnternetin düzenlenmesi konusu bağlamında klasik “ulusal egemenlik” ve “devletin egemenlik yetkisi” kuramlarının temelden sorgulandığı bir mecra doğru ilerlemektedir.

7. Dünya uygulamaları, ülkelerin ekonomik, teknolojik, kültürel gelişmişlik düzeylerine ve sosyolojik ve siyasal kodlarına, kültür ve inanç haritalarına göre İnternet politikalarının farklılık gösterdiğini ortaya koymaktadır. Buna göre, bazı ortak noktalar bulunmakla birlikte, ülkelerin kendilerine özgü özelliklerine göre, içerik düzenleme politikaları, kullanılan araçlar, yöntemler, teknikler ve kriterler, düzenlemelerin kapsamı ve uygulamalara ilişkin süreçler farklılık arz etmektedir.

Nitekim, bazı ülkeler içerik güvenliğine ilişkin önlem ve müdahalelerini bu konuya özel genel kapsayıcı yasal düzenlemeler yaparak gerçekleştirirken, bazıları da bunun yerine “gerçek hayatta suç olanın çevrimiçi ortamda da suç sayılması” prensibinden hareketle mevcut yasalarını İnternete uyarlayarak sonuç almaya çalışmaktadır.

Keza, devletleri bu alanda düzenleme yapmaya bazen ulusal güvenlik konularında duyulan endişeler (terörizm, ırkçılık ve ayrılıkçılık vb.), bazen ise, İnternette yer alan kimi içerikler karşısında toplumların ve devletlerin, kendi geleneksel, tarihsel, kültürel, sosyal, siyasal, dinsel ve ahlaki değerlerine ilişkin taşıdıkları kaygılar itmektedir. Kimi zaman da İnternetteki devletle ilgili değer yargılarına yönelik hakaret içeren ifadeler, rejim, resmi ideoloji aleyhtarlığı yapılması gibi kurulu siyasal sisteme ve siyasi istikrara zarar verecek içeriklerden duyulan rahatsızlıklar bu konuda etkili olmaktadır.

Ülkeler ve uluslararası kuruluşlar, bazı istisnalar dışında, genelde ortak görüş olarak çocuk pornografisi ve cinsel istismarı ile telif haklarına ait içerikler yanında çocukların pornografik içerikten korunması konularında uzlaşıya varmış gibi gözükmektedir. Bunlar dışında en çok düzenlemeye konu edilen içerik türleri ise ekstrem pornografi (ensest, ölü sevicilik, hayvan vs.), ırkçılık ve ayrımcılık, nefret ve şiddet içerikleri, online kumar, intihara ve uyuşturucu kullanmaya teşvik gibi konulardan oluşmaktadır. Genellikle de devletler ülke vatandaşlarını özellikle çocukları ve gençleri bu tür içeriklerden korumak amacıyla bu içeriklerle mücadele yoluna başvurmaktadır. Bunlar dışında ülkelerin ulusal güvenlik ve terörizm ile mücadele gerekçesiyle anti-terör yasaları çıkartarak bu kapsamda değerlendirdikleri içeriklere müdahale ettikleri veya İnternet trafiğini izlemeye aldıkları görülmektedir.

Diğer yandan, İnternet içeriğinin düzenlenmesi, kurallar konulması ve önlem alınmasına ilişkin olarak dünyada “devlet düzenlemesi”, “kendi kendine/öz düzenleme” ve “birlikte/ortak düzenleme” gibi farklı yönetsel yaklaşımlar uygulanmakta ve bu yaklaşımlar değişik boyutları ile tartışmalara konu olmaktadır. Dolayısıyla, uygulamalar tezin yedinci alt hipotezinin geçerliliğini ve doğruluğunu ortaya çıkarmaktadır.

8. Günümüzde düşüncüyü ifade etmenin en etkili ve yaygın araçlarından birisi de kuşkusuz İnternettir. Bu nedenle, içerik düzenlemelerinin ifade özgürlüğünün bir unsuru olan “İnternet özgürlüğü”nü koruması ve yaşatması gerekmektedir. Bu çerçevede, Uluslararası Sözleşmeler ile AİHM’nin ifade özgürlüğüne ilişkin hüküm ve kriterlerini gözeterek düzenlemeler ve uygulamalar gerçekleştirilmelidir. Buna göre, ifade özgürlüğünün ne zaman, nasıl ve hangi koşullarda sınırlandırılabilirliği konusundaki ölçütlere uyulmalıdır.

Dolayısıyla, özellikle erişim engelleme karar ve uygulamalarında AİHM’nin ifade özgürlüğünün sınırlanmasıyla ilgili olarak belirlediği; “sınırlama veya müdahale için mevzuat olup olmadığı”, “sınırlamanın meşru bir amacının bulunup bulunmadığı” ve “sınırlamanın demokratik bir toplum için gerekli olup olmadığı” ölçütleri önem taşımaktadır. Keza, erişim engelleme karar ve uygulamalarının AİHM içtihadında yer alan “orantılılık” ve “ölçülülük” koşullarına uygun olmasına dikkat edilmelidir.

Diğer yandan, içerik düzenlemeleri İnternetin çok yönlü/aktörlü, karmaşık ve dinamik kendine özgü yapısına uyum gösterirken gelişmesine ve büyümesine de engel olmamalıdır. Nitekim, İnternetin kendine özgü yapısına ve teknik özelliklerine uygun olmayan düzenlemelerin çoğu zaman etkisiz kaldığı veya yeni başka sorunlara sebep olduğu görülmektedir. Keza, özellikle erişim engelleme ve filtreleme uygulamalarında İnternetin kendine özgü bu doğasının dikkate alınmaması, İnternetin yavaşlaması veya kesintiye uğraması ya da sansür uygulamalarının ortaya çıkması gibi önemli sorunlara neden olabilmektedir.

Bu nedenlerle, İnternet içerik düzenlemelerinde, “sınırlı müdahale” yaklaşımının tercih edilmesi, özgürlükler ve demokratik değerler açısından ve İnternetin doğasına en uygun yaklaşım olarak görülmektedir. Bu bağlamda, düzenlemelerde uygulanabilir, adil, açık ve saydam, kamu yararına göre ölçülü ve gerekli olan en az müdahale öngörülmektedir. Nitekim, demokratik değerlere önem veren ülkelerin, genel çerçeveyi mümkün olduğunca sınırlı tutarak, sadece önemli gördükleri “çocukların cinsel istismarı”, “ırkçılık ve ayrımcılık” ve “terör” gibi belirli birkaç hususu İnternet içerik düzenlemesine konu edindikleri gözlemlenmektedir.

Dolayısıyla, tezin sekizinci alt hipotezinde söz konusu edilen içerik düzenlemelerinin “ifade ve bilgiye erişim özgürlüğü” ve İnternetin çok yönlü/aktörlü ve dinamik özgün yapısıyla uyum içinde olması ve düzenlemelerde gerekli olan “en az ve sınırlı müdahale” nin tercih edilmesi öngörülerinin haklılığı ortaya çıkmaktadır.

9. “Bilgi toplumu”nun ürünü olan “yönetişim modeli”, bir “bilgi toplumu” sorunu olan İnternet içerik düzenlemesi ve yasadışı ve zararlı içeriklerle mücadele konusunda en etkili ve elverişli yönetsel araç olarak görülmektedir. Nitekim, dünya uygulamalarında da çokça örnekleri görüldüğü gibi, İnternet ve İnternet içerik düzenlemesi konuları da dahil olmak üzere, bilgi ve iletişim teknolojilerine ilişkin yönetsel yapılar ve süreçler genellikle bilgi toplumunun popüler yönetim biçimi olan birlikte yönetim anlayışına dayalı yönetim modeli ile gerçekleştirilmektedir.

Zira, içerik düzenlemelerinde devletin otoriter gücünün gerekliliği kabul edilmekle birlikte, İnternet ile ilgili problemlerin çözümünde, İnternetin küresel ve merkezi olmayan, çok aktörlü/boyutlu ve dinamik yapısı nedeniyle devletlerin tek başlarına etkili ve tatmin edici düzenlemeler yaparak sonuç almaları mümkün gözükmemektedir. Bu nedenle, bir yandan ulusal ölçekte İnternet’in çok taraflı yönetimi/yönetişim anlayışıyla hareket ederken, diğer yandan ulusal düzeydeki politikaların geliştirilmesinde uluslararası yetki konularının dikkate alınması ve küresel İnternet aktörlerini de içine alan “birlikte düzenleme” uygulamaları geliştirmeye çalışılması gerekmektedir.

Yasadışı ve zararlı İnternet içeriğiyle mücadele konusunda Avrupa’da vitrinde daha çok sivil toplum merkezli olarak “öz düzenleme” girişimleri yer almaktadır. Genel yaklaşım ve resmi politika olarak da bu mücadelede sivil toplumun organize ettiği “öz düzenleme” girişimlerinin daha etkili olacağı yönünde hakim bir görüş bulunmasına rağmen, devletlerin arka planda “görünmez el” olarak varlıklarını hissettirdikleri ve “zorunlu gönüllülük” tesis ettikleri görülmektedir.

İnternetin güvenli kullanımını sağlamaya yönelik çalışma ve faaliyetleri İnternet sektörünün bizzat kendisinin gönüllü olarak yapmasını ifade eden öz düzenleme;

yasadışı ve zararlı İnternet içeriğinin önlenmesine yönelik tedbirlerin, kurulacak mekanizmaların, uyulacak kuralların söz konusu işletmelerin ortak iradesi ve inisiyatifi ile hayata geçirilmesini kapsamaktadır. Bu çerçevede, gönüllü olarak uyar-kaldır mekanizmasının işletilmesini sağlama, yasadışı ve zararlı içerikler için ortak filtreleme sistemleri ve sektöre özgü güvenlik politikaları geliştirmek, ihbar merkezi ve yardım hattı kurmak ve işletmek, bilinçlendirme, İnternet etiği ve İnternet okur-yazarlığı faaliyetlerinde bulunmak gibi bir dizi çalışmayı kendi belirleyecekleri uygulama prensipleri ile yerine getirmektedirler. Bu yaklaşım tüm dünyada teknolojik gelişmelere ve sosyal trendlere daha uyumlu, daha demokratik ve etkili olması yönüyle tercih edilmekte ve geliştirilmeye çalışılmaktadır. Dolayısıyla, içerik düzenlemelerinde; birlikte düzenleme ve yönetim modelini merkeze alarak, bunun yanında öz düzenleme uygulamalarının teşvik edilmesini öngören dokuzuncu alt hipotezin doğruluğu ispatlanmış olmaktadır.

10. Yasadışı ve zararlı içeriğin önlenmesi ve bu tür içeriklerle mücadeleye yönelik düzenleme ve uygulamalar belirli bir sistematik dahilinde gerçekleştirilmelidir. Öncelikle, erişim engellemeye konu suç türleri belirli ve oldukça sınırlı tutulmalıdır. Keza, erişim engelleme son çare olarak uygulanmalıdır. Öncesinde, uyar-kaldır mekanizmaları, öz düzenleme uygulamaları, büyük sektör firmaları ile özel anlaşma ve işbirliği geliştirme, bilinçlendirme ve İnternet etiği faaliyetleri, pozitif içerik oluşturma, sivil toplumun gücünü kullanma, yaş doğrulama benzeri önleyici tedbirler gibi erişim engellemesi tedbiri almayı gereksiz kılacak doğrudan veya dolaylı içerik düzenlemesi enstrümanları devreye sokulmalıdır. Bu yöntemler daha az sakıncalı, daha etkili ve her şeyden önemlisi de daha demokratiktir.

Nitekim, giderek artan eğilim daha kompleks ve rafine teknikler kullanarak daha fazla yerde ve daha fazla engelleme yapmak yönünde olmasına rağmen, erişim engellemede yüzde yüz başarılı bir teknik bulunamamıştır. Aksine, bu tür girişimler masum içeriklerin engellenmesinden İnternetle ilgili teknik sorunlara kadar birçok sakıncalar doğurmaktadır. Keza, İnternetin kendine özgü yapısı ve teknik özellikleri sebebiyle her bir erişim engelleme tekniğinin kendi içinde güçlü ve zayıf yönlerinin olduğu, bir takım açıkları, eksiklikleri ve sakıncaları barındırdığı ortaya çıkmaktadır.

Diğer yandan, İnternette erişim engellemeler yaygın hale geldikçe, bunları aşabilmeyi sağlayan araçların geliştirilmesi ve potansiyel kullanıcılara dağıtım çalışmaları da hız kazanmıştır. Yine, erişim engelleme yöntemleri kombine şekilde kullanıldıkça, engellemeleri aşma yöntemleri de kombine olarak kullanılmaya başlamıştır. Bu nedenlerle erişim engelleme uygulamalarının, erişime tamamen mani olmaktan ziyade erişimin zorlaştırılmasına hizmet ettiği görülmektedir. Dolayısıyla devletler de filtreleme ve erişim engellemede kullandıkları teknolojinin mükemmel olmasından ziyade daha etkili olmasına önem vermektedir. Dolayısıyla, tezde onuncu alt hipotezde belirtilen hususların geçerliliği açık olarak ortaya çıkmaktadır.

11. İnternet, teknik, ekonomik, sosyal, siyasal, yönetsel yönleri ve birçok aktörleri ile ve bunların girift bir şekilde birbiri içine geçmesi ve zincirleme olarak birbirini etkilemesiyle bir bütün olarak dinamik bir yapıdır. İnternetle ilgili sorunlar, İnternet gerçeğini bütün bu özellikleri ile ve bütüncüllüğü içerisinde anlamak, kavramak ve ele almakla çözüme kavuşabilir. Dolayısıyla, İnternet olgusunun bir alt başlığı ve parçası olan İnternet içerik düzenlemesi konusunu İnternetin bu çok yönlü ve aktörlü bütünlüğünden ayırıştırarak ele almak doğru olmayacaktır. Bunun yerine, konunun bizzat doğasının ortaya koyduğu özelliklerle birlikte, bütünlüğün içerisindeki yeri ve diğer yön ve aktörlerle etkileşimlerini de kapsayacak bir bakış açısıyla konuyu değerlendirmek gerekmektedir.

Bu yaklaşımla, ülkelerin İnternetle ilgili düzenlemelerinde temel olacak; İnternetin çok yönlü/aktörlü ve dinamik yapısıyla uyumlu, aynı türden özelliklere sahip çok yönlü/aktörlü ve dinamik bütüncül bilgi toplumu ve İnternet stratejileri ve politikaları oluşturmaları gerekmektedir. Keza, içerik düzenlemesine ilişkin strateji ve politikalar bu genel ve bütüncül bilgi toplumu ve İnternet strateji ve politikalarından bağımsız olarak düşünülmemelidir. Bilakis, bu üst ve bütüncül strateji ve politikalar, diğer tüm alt konulara ait strateji ve politikalarla birlikte ve onlarla uyumlu olarak, içerik düzenlemesine ilişkin strateji ve politikalara da yön vermelidir.

Dolayısıyla, İnternetin beraberinde getirdiği risk ve tehditlerin giderilmesi ve yasadışı ve zararlı içeriklerle mücadele edilmesiyle ilgili içerik düzenlemesine ilişkin

strateji ve politikalar, konunun/sorunun teknik, ekonomik, sosyal, siyasal, yönetsel tüm boyutlarını içine alan bu bütüncül strateji ve politikaların omurgası üzerine oturtulmalıdır. Bu yaklaşım içinde oluşturulacak strateji ve politikalar, bu strateji ve politikalara bağlı olarak oluşturulacak içerik düzenlemelerinin, karar ve uygulamalarının başarı şansını artıracaktır. Dolayısıyla, onbirinci alt hipotezin doğru bir öngöründe bulunarak önemli bir gerçeğe işaret ettiğı söylenebilir.

12. İnternetin küresel niteliğı, kendine özgü dinamik yapısı ve teknik özellikleri ülkelerin yasadışı ve zararlı İnternet içeriğine karşı yürüttüğü mücadeleyi etkisiz kılmaktadır. Filtreleme ve erişim engellemelerin kolaylıkla karşı yöntemlerle aşılabilmesi, ülke dışında barındırılan yasadışı ve zararlı içeriğe ilişkin ülkelerin genellikle çaresiz kalmaları, İnternetin uluslararası yönetimi sorunu, İnternetin karmaşık teknik yapısı ve anomiteyi koruması, uyar-kaldır sisteminin çoğu zaman işletilememesi, bilinçlendirme ve etik çalışmalarının zaman gerektirmesi ve somut etkisi konusundaki şüpheler, sivil toplumun konuya yeterince sahip çıkmaması, öz düzenleme kuruluşlarının ticari kaygılarla hareket etmesi, küresel firmaların çoğu zaman yerel iktidarlara işbirliğine gitmek istememesi, yasadışı ve zararlı içerik üretenlerin profesyonelleşmesi ve küresel ağın imkanlarını daha iyi kullanmaları gibi bir çok neden bu tür içeriklerin tamamen İnternet ortamından kaldırılmasına engeldir. Dolayısıyla, onikinci alt hipotezde belirtildiğı gibi, uygun strateji, politika, yöntem ve yaklaşımlar ile ancak, İnternetin daha güvenli kullanımını sağlayarak söz konusu içeriklerden oluşacak zararı en aza indirmek mümkün olacaktır.

13. Başta ABD ve AB olmak üzere, dünyadaki İnternet içerik düzenlemeleri bir bütün olarak değerlendirildiğinde, içerik düzenlemelerinde en önemli belirleyici unsurun büyük oranda sermaye, yani para ve piyasa olduğu görülmektedir. Nitekim, İnternetin, tüm eleştirilere rağmen, en hızlı ve etkin/etkili şekilde düzenleyici kurallarla kontrol altına alınan/alınmaya çalışılan içerik konularının, büyük sektörlerin menfaatlerini ilgilendiren içerik türlerine ait olduğu gözlemlenmektedir.

Müstehcenlik ve pornografi, hatta çocuk pornografisi gibi özellikle çocuk ve genç kullanıcıların güvenliği ve korunması gerekçesine dayanan içeriklerle ilgili önlem

alınmasına yönelik karar alma süreçleri yavaş ve tartışmalı bir şekilde ilerleyip, gevşek uygulamalara konu edilirken, telif hakkı ihlalleri ile online kumar ve bahis gibi ilgili sektörlerin menfaatlerine zarar veren ve sermaye ve rekabetçi piyasanın korunması gerekçesine dayanan içerik düzenlemeleri ve önlemlere ilişkin kararlar çok hızlı bir şekilde alınıp, katı bir şekilde uygulamaya geçilebilmektedir.

Zira, devasa boyutlara ulaşan dünyadaki pornografi ve çocuk pornografisi sektörünün, düzenleme süreçlerine tersinden etki ederek söz konusu içeriklerle mücadele edilmesine yönelik etkin/etkili önlemlerin alınmasına engel olmak veya alınan önlemleri etkisiz ve geçersiz kılmak konusunda büyük oranda başarılı olduğu bilinmektedir. Bu kapsamda, yüz milyar dolarlarla ifade edilen pornografi ve çocuk pornografisi sektörü karşısında, söz konusu içeriklere karşı önlem almak için geliştirilen filtreleme, erişim engelleme, bilinçlendirme, ihbar merkezi, sınıflandırma vb. tedbir ve uygulamalara ilişkin milyon dolarlık mütevazı bütçelerle etkili sonuçlar almanın mümkün olmayacağı görülmektedir. Bu nedenle, pornografinin her türü başta olmak üzere İnternetteki yasadışı ve zararlı içerikler her geçen yıl hızla artarken, sektörel hacimleri ve ciroları katlanarak büyümektedir.

Diğer yandan, başta ABD ve AB olmak üzere dünyadaki birçok ülkede ihbar ve bilinçlendirme merkezlerini ve yasadışı ve zararlı içeriklerle mücadele eden STK'larına en büyük finansal ve teknik desteği yerli ve küresel İnternet firmalarının (Microsoft, Google, Yahoo gibi) sağlıyor olması iyi niyetli girişimler olarak görülebileceği gibi, bir başka açıdan, bu firmaların bahsi geçen içeriklerle mücadeleyle ilgili çalışmaları, söz konusu finansal ve teknik destek ve işbirliği girişimleri üzerinden dolaylı olarak yönlendirme, kontrol ve denetim altında tutma çabası olarak da kabul edilebilir.

Keza, birçok ülkedeki İnternet sektörünün öz düzenleme girişimleri de sektörün yasadışı ve zararlı içeriklerle ilgili mücadelede ön alma, etkin ve belirleyici olma çabası olarak görülebilir. Böylece, sektörün, ticari menfaatleri zarar görmemesi için devletlerin daha ciddi ve etkili mücadele yöntemleri benimsemesi ve katı düzenlemeler yapması ve uygulamasının önüne geçmeye çalıştığı söylenebilir.

Bunun yanında, özellikle ABD menşeli büyük küresel İnternet şirketlerinin, İnternetin denetlenmesi ve kontrol altına alınması ve bu kapsamda özellikle merkezi filtreleme ve erişim engelleme uygulamalarına karşı mücadele veren STK'larının ya kurucuları ya da en büyük destekçileri olmaları da sektörün içerik düzenlemelerini belirleme girişimi olarak değerlendirilebilir. Bu tür girişimler, İnternette erişim özgürlüğünün sağlanması konusunda faydalı ve gerekli görmekte birlikte, söz konusu şirketler ve ABD ekonomisi açısından, İnternetin yaygınlaşması, sınırsızca kullanımının önündeki engellerin kaldırılması ve dolayısıyla, sektörün daha da büyümesi ve karlı hale gelmesini sağlamaya yönelik çabalar olarak da algılanabilir.

Dolayısıyla, sektörün genel bir yaklaşım olarak, ulusal ve uluslararası ölçekte farklı neden ve konular kapsamında yasadışı ve zararlı içeriklere karşı yürütülen mücadeleleri ve İnterneti içerik yönüyle regüle etme girişimlerini ticari çıkarlarına tehdit olarak gördüğü iddia edilebilir. Bu nedenle, İnternete sınırsız özgürlük isteyen bahsi geçen girişimlerin hepsinin amacının sadece insan hakları ihlallerinin önlenmesini sağlamak olarak görülmemesi gerekmektedir.

Diğer yandan, küresel sermayenin İnternet sansürüyle ilgili tavrında temel motivasyonu “ticari kar” saikinin oluşturduğu görülmektedir. Nitekim, CISCO, Yahoo, Google, Microsoft gibi ABD şirketlerinin Çin benzeri devlet sansürü uygulayan ülkelere teknik destek sağladığı ve sansür konusunda çeşitli düzeylerde işbirliği yaptığı bilinmektedir. Yani, İnternetin büyük küresel şirketlerinin yasadışı ve zararlı içeriklerle mücadele ve bu kapsamda devlet sansürü uygulamaları konusunda ilkesel bir tavrı söz konusu değildir. Bu konuda, ticari çıkarlarını ön planda tutan “faydacı” bir yaklaşım içindedirler.

Ayrıca, dünyada birçok ülkede bulunan İnternetle ilgili düzenleyici üst kurulların mevcut yaklaşım, görev, konum ve yapılarının, ulusal ve küresel İnternet sektörünün ülkelerin içerik politikalarında belirleyici olma girişimlerine elverişli bir vasat sağladığını da belirtmek gerekmektedir. Zira, liberal politikalar gereği, tam rekabetçi piyasa şartlarının hakim olması ve sektörün büyümesini, daha karlı hale gelmesini sağlamaya yönelik olarak faaliyet gösteren düzenleyici kurullarda, genellikle

İnternetin riskleri ve tehlikeleri, yasadışı ve zararlı içeriklere karşı önlem alınması gibi bir bakış açısı çok fazla gelişme imkanı bulamamaktadır. Çünkü, genellikle, İnternet piyasasını büyötmeye endeksli yaklaşımlar, içeriklerin risk ve tehlikelerini görmeye engel olmaktadır. Zira, bu bakış açısının İnternet sektörüne ekonomik olarak zarar vereceğı, kullanımı sınırlandıracağı, içerik düzenlemelerine kapı aralayacağı için yeni hukuki ve mali yükümlölükler getireceğinden endişe edilmektedir.

Sonuç olarak, onüçüncü alt hipotezde belirtildiğı gibi, küresel İnternet sermayesi, oldukça rafine bir biçimde, ulusal ve uluslararası ölçekte değışik finansal, siyasal ve yönetsel enstrümanlar kullanarak, doğrudan veya dolaylı olarak içerik düzenlemelerinin yönünü, politikalarını, yasadışı içeriklerle mücadelenin kapsamını ve yöntemini büyük oranda belirlemektedir. Dolayısıyla, İnternet içerik düzenlemelerine ilişkin politika oluşturma, karar verme ve uygulama süreçlerinin küresel kapitalist sistemin kurallarına göre işlediğini ve bu süreçleri büyük oranda ilgili piyasa oyuncularının belirlediğini ifade etmek mümkündür.

14. Bambuer'in örnek bir model olarak ortaya koyduğı tarzda, ölkelerin içerik düzenlemesi uygulamalarının meşruiyetini nesnel, ölçülebilir, kıyaslanabilir ve objektif olarak test etmeye yarayacak ilke ve ölçütlerin belirlenmesi ve bunlar ile uygulamaların analitik analiz yöntemleri ile değıerlendirilerek ölkeler hakkında sonuçlara ulaşılabilmesi büyük önem taşımaktadır. Böylece, normatif ve tüm ölkeler için geçerli olacak standart bir ölçüm araçlarına sahip olunabilecektir. Bunun gerçekleştirilmesi, bu alanda çalışma yapan ulusal ve uluslararası sivil ve kamu otoritelerinin ölkelerin öznel ve nesnel gerçekliklerini görmezden gelerek, çoğı zaman sübjektif ve keyfi değıerlendirmeler ile ölkeleri "İnternet düşmanı" veya "İnternet dostu" olarak ilan etmesinin önüne geçecektir.

Zira, Human Rights Watch, OpenNet Initiative, Reporters Without Borders ve Freedom House gibi her türlü devlet sansürüne karşı mücadele veren uluslararası örgütlerin İnternet özgürlüğü konusunda bazı durumlarda ABD ve AB ölkeleri lehine çifte standartlar uyguladıkları görölmektedir. Nitekim, ABD, İngiltere, Fransa ve

Almanya’da ulusal güvenlik ve terörizmle mücadele gerekçesi ile İnternetin ulusal ve uluslararası ölçekte resmi ve gayriresmi yöntemlerle ve sofistike olarak sıkı şekilde izlendiği, trafiğinin takip edildiği ve doğrudan İSS’lar üzerinden “zorunlu gönüllülük” ile filtreleme uygulamaları gerçekleştirildiği bilinmesine rağmen, bu İnsan hakları ve İnternet özgürlüğünü savunan uluslararası örgütlerin çoğu zaman bu durumu görmedikleri veya yeterince gündeme getirmediikleri gözlemlenmektedir.

Diğer yandan, İnternet sansürü tartışmalarına ilişkin konunun bir de ülkelerin ulusal güvenliklerini ilgilendiren diğer bir boyutunun daha olduğu görülmektedir. O da, tıpkı nükleer silahlara sahip olma konusunda ortaya çıkan durum gibi, söz konusu gelişmiş batılı ülkelerin, zorunluluk durumunda İnterneti tümünden veya kısmen durdurabilecek ya da izleme, kontrol ve denetim altına alabilecek teknik altyapıya sahip olmalarına rağmen, bu tartışmalar üzerinden, diğer ülkelerin bu altyapıya sahip olmalarının önüne geçmeye çalışmalarıdır.

Buna göre, İnterneti diğer ülkelere nüfuz etme ve bu ülkelerdeki sosyal ve siyasal operasyonlarda bir araç olarak kullanma eğiliminde olan İnternetin egemen güçlerinin, bu olanağı yitirmemek amacıyla, diğer ülkelerin bu tür operasyonları etkisiz kılacak İnternet altyapısına sahip olmasının önüne geçmek için “sansür” kozunu kullandığı görülmektedir. Bu çerçevede, İnternet özgürlüğünü savunan bu örgütlerin de doğrudan veya dolaylı yollarla kullanılarak, diğer ülkelerin İnterneti kontrol ve denetim altına almaya yönelik altyapı çalışmaları, içerik düzenlemesi girişimleri ve uygulamalarının bloke edilmeye çalışılması muhtemeldir. Böylece, kimi zaman haklı fakat çoğu zaman ise haksız olarak, bu ülkelerin içerik düzenlemeleri ve uygulamaları “sansür” gerekçesiyle eleştirilmekte ve uluslararası kamuoyu nezdinde “İnternet düşmanı” olarak mahkum olmaları sağlanmaktadır.

Tezde ondördüncü alt hipotezde belirtildiği gibi, tüm bu şüphe, tartışma ve sakıncaların giderilebilmesi için İnternet içerik düzenlemesi politikalarının, iddia ve uygulamaların analitik yöntemlerle normatif olarak ölçülmesine imkan tanıyacak uluslararası geçerliliği olan kıstasların ve analiz yöntemlerinin geliştirilmesi gerekmektedir. Böylece, bu alandaki subjektif ve keyfî yorumlarla ülkelerin ve

uygulamalarının değerlendirilerek mahkum edilmesinin önüne geçilebilir. Dolayısıyla, İnternetin uluslararası yönetimini üstlenecek bir kurumun bu konuyla ilgili çalışmalar yapması faydalı olacaktır.

15. Yapılan araştırmalar, yayınlanan istatistikler ve raporlar Türkiye’de İnternet kullanımının sayısal, oransal ve kullanım miktarı ve süresi bakımından hızla arttığını gösterirken, kullanıcıların daha çok gençlerden oluştuğu görülmektedir. Keza, ülkemizde, dünyadaki gelişme trendlerinin de ötesinde, neredeyse bir sosyal ağ ve özellikle Facebook çılgınlığı göze çarpmaktadır ve İnternetin Facebook, Google ve Hotmail gibi batılı platformların egemenliği altında olduğu görülmektedir.

Türkiye’deki kullanıcılar İnterneti bu batılı platformların sundukları imkanlardan yararlanarak daha çok eğlenme, vakit geçirme, haber okuma ve iletişim kurma amacıyla kullanmaktadır. Bu nedenle, İnternette en çok yapılan aktiviteler sörf yapma, sanal sohbetler, sosyal ağ faaliyetleri, video seyretme, oyun, müzik, film, görüntü, yazılım indirme, oyun oynama, çevrimiçi haber, gazete veya dergi okuma, spor ve sağlık sitelerini gezme, blogları ziyaret, e-posta gönderme/alma ve görüntülü/sesli görüşme yapmak olarak belirmektedir. Ayrıca, İnternet bağlantısının ve kullanımının giderek daha fazla cep telefonları üzerinden gerçekleştirilmeye başlandığı görülmektedir.

Türkiye’de İnternet kullanımının özelliklerini ortaya koyan araştırma verileri, çocuklar ve gençlerin artan bir şekilde genel olarak İnternette ve bilgisayar oyunlarında aşırı zaman harcadıklarını göstermektedir. Veriler, Türkiye’de İnternetin aşırı kullanımının, aile içi iletişime zarar verdiğini ortaya koymaktadır.

İnternet teknolojisi çocuklara ve gençlere cinsel istismar, pornografi, fuhuş, siber zorbalık, şiddet, nefret, intihara yönlendirme, kumar, bahis ve şans oyunları ve uyuşturucuya teşvik gibi uygun olmayan içeriklerle karşılaşma; İnternet bağımlılığı, dijital oyunlar ve sosyal ağların riskleri ve tehlikeleriyle muhatap olmalarına neden olmakta ve önemli sorunlar ortaya çıkarmaktadır. Keza, ülkemizde İnternetin

aileye ve toplumsal yapıya zararları bakımından en fazla gündeme gelen konusu ise şüphesiz müstehcenliktir.

Ayrıca, İnternet kafelerin yanlış amaçlarla ve bilinçsizce kullanılması çocukların çeşitli tehlikelerle karşılaşmasına neden olmaktadır. Bunlar, yasadışı ve zararlı içerikler olabileceği gibi, bilişim suçları mağduriyeti, yanlış kişilerle arkadaşlık kurma veya zararlı oyunlar ve bağımlılık türü olumsuzluklar da olabilmektedir. Tüm bunlar, tezin onbeşinci alt hipotezinde ortaya konulan hususları teyit etmektedir.

16. Türkiye, henüz “bilgi toplumu” ve “İnternet”i sindiren bir toplum olmasa da, İnternet içerik düzenlemesi sorununa muhatap olmuş ve bu konuda kendine özgü bir uygulama geliştirmiştir. İnternet kullanımının giderek yaygınlaşması ile çocukların, gençlerin ve ailenin yasadışı ve zararlı içeriklerden korunması konusu önemli bir sorun olarak ortaya çıkmıştır. Bu kapsamda, aynı zamanda anayasal bir zorunluluğun gereği olarak 5651 sayılı Yasa, kısa sayılabilecek bir hazırlık döneminden sonra İnternet içerik düzenlemesine özgü bir temel mevzuat olarak yürürlüğe girmiştir.

İçerik, yer, erişim ve toplu kullanım sağlayıcıların yükümlülük ve sorumlulukları ile bu aktörler üzerinden İnternet ortamında işlenen katalog suçlarıyla mücadele etmeyi amaçlayan bu Yasa, ikincil düzenlemeleriyle birlikte yeni bir hukuki düzen tesis etmiştir. Bu yeni hukuksal düzen, İnternet içerik denetiminin TİB tarafından yapılmasını ve bu kapsamda TCK ve bir özel yasada yer alan belirli suçların İnternet ortamındaki olumsuz etkilerinin önlenmesi için idari ve yargısal koruma tedbiri öngörmektedir. Bu bağlamda TİB, 5651 sayılı Yasa’nın kendisine vermiş olduğu yetki ve sorumluluklar çerçevesinde bir kısmı büyük tartışmalara neden olan önemli birçok karara ve uygulamaya imza atmıştır.

Bu kapsamda, katalog suçlarıyla ilgili ihbarları almak üzere kurulan ve INHOPE üyesi olan TİB Bilgi İhbar Merkezi, dünyadaki benzerleri arasında en fazla ihbar alan birkaç merkezden birisi haline gelmiştir. TİB, yer sağlayıcılara faaliyet belgesi verilmesi ve iptali, barındırdıkları alan adlarına ilişkin dosyaların kontrolü ve veri tabanına aktarılması, içerik, yer ve erişim sağlayıcıların tanıtıcı bilgilerini web

sitelerinde bulundurmalarının takip edilmesi gibi işlemleri de yürütmektedir. Keza, İnternet kafeler için onayladığı filtre programlarını ve hazırladığı IP Log imzalayıcı programı resmi web sitesinde yayınlamaktadır.

Fakat, Türkiye’de bulunan oldukça sınırlı sayıdaki yer sağlayıcının bu belgeyi almak için başvuruda bulunduğu ve kayıtlı olanların da iletişim bilgileri değişikliklerini düzenli bir şekilde bildirmediikleri, zorunlu olmalarına rağmen barındırdıkları sitelerin trafik bilgilerini saklamadıkları da görülmektedir. Keza, Türkiye’deki yer sağlayıcılar sunucularını özellikle barındırma maliyetinin çok düşük olduğu ülkelerde barındırmaktadır. Nitekim, yasa dışı içeriklerin çoğunun yurtdışında barındırıldığı tespit edilmektedir. Yer sağlayıcıların kayıt dışı kalmaları yasadışı içerikler ile mücadeleyi zorlaştırmaktadır. Dolayısıyla, mücadelenin bu ayağında aksamalar görülmekte, yeni tedbirlere ihtiyaç duyulmaktadır.

İlgili mevzuat gereği TİB, İnternetin güvenli kullanılmasına yönelik olarak bilinçlendirme faaliyetleri yapmaktadır. Bu kapsamda, İnternetin güvenli, etkin ve bilinçli kullanımını sağlamak amacıyla hazırlanan “Güvenliweb” ve “Güvenliçocuk” adındaki bilinçlendirme siteleri ile hizmet vermektedir. “Güvenliweb”, gelişmiş ülkelerin güvenli İnternet portalları arasında en çok ziyaret edilen web portallarından birisidir. Ayrıca, TİB, basılı, sesli ve görüntülü materyaller hazırlayarak ücretsiz olarak dağıtımını yapmakta ve eğitimler vermektedir.

Fakat, yürütülen bu faaliyetlere rağmen Türkiye’de, İnternetin bilinçli, güvenli ve etkin kullanımıyla ilgili genel kullanıcı düzeyinin yeterli olmadığı görülmektedir. Ülkemizde adeta bir dijital nesil kopukluğu yaşanmaktadır. Ebeveynlerin ve eğitimcilerin İnternetin bilinçli, güvenli ve etkin kullanımıyla ilgili ve İnternet okuryazarlığı düzeylerinin düşük olmasından ötürü çocuklara ve gençlere etkili yönlendiricilik yapamamaktadır. Keza, İnternet okur-yazarlığı ve İnternet etiğinin geliştirilmesi de ayrıca üzerinde durulması gereken bir konudur.

TİB, ulusal ve uluslararası kurum ve kuruluşlarla işbirliği ve koordinasyonu sağlamakla ilgili olarak ise, AB Güvenli İnternet Programını takip etmekte ve AB

uygulamalarını incelemekte STK'ları ve ilgili kamu kurum ve kuruluşlar ile görüşmeler yapmaktadır. Yapılan çalışmalar sonucunda Türkiye AB'nden "Safer Internet Programme"na katılım daveti almıştır.

5651 sayılı Yasa İnternet ortamındaki yayın içeriği dolayısıyla hakları ihlal edilen kişilere, içerik sağlayıcısından veya buna ulaşamaz ise yer sağlayıcısından içeriğin yayından çıkarılmasını talep etme ve cevap hakkını düzenlenmiştir. TİB, hakları ihlal edilen kişilerin muhataplarını tespit etme ve faydalı olabilecek bilgi kaynaklarına erişimleri konusunda yardımcı olmaktadır. Başkanlık, faaliyet belgesi almış yer sağlayıcılar ile yetkilendirilmiş olan erişim sağlayıcıların listesini ve iletişim bilgilerini resmi İnternet adresinde yayınlanmaktadır. Ayrıca, yine web sitesinde yer alan site bilgileri sorgu sayfasından talebe konu adreslerle ilgili olarak açık kaynak bilgi sorgusu yapılabilmesine imkan sağlamaktadır.

TİB, içeriğin yayından çıkarılmasına ilişkin düzenlemeyi bir "uyar-kaldır" sistemi olarak kurgulayıp, uygulamaktadır. Bu kapsamda, herhangi bir erişimin engellenmesi kararı verilmeden önce suç unsuru bulunan kısmi içeriklerin yer aldığı İnternet siteleriyle, ulaşılabilir iletişim bilgileri üzerinden irtibata geçmekte ve "uyar-kaldır" yöntemi ile suça konu içeriğin kaldırılmasını temin etmektedir. TİB'nin yasadışı ve zararlı içerikle mücadelede, erişim engellemeden ziyade Yasa'da yer alan ve tüm dünyada kabul gören bu sisteme öncelik vermesi yerinde bir tercih ve yaklaşımdır.

Zira, TİB'nin en çok tartışılan ve eleştirilere maruz kalan karar ve uygulamaları erişim engellemeleriyle ilgili olanlardır. Bu kapsamda, müstehcenlik kavramının belirsiz olmasından, sakıncalı içerik yanında sitenin tamamına erişimin engellenmesi nedeniyle suç ve cezada orantısızlık bulunduğu, TİB'nca re'sen kapatılan sitelerle ilgili yetki tartışmalarına, yasaklar konusunda ihtisas mahkemelerinin bulunmamasından, kapatılan sitelere ilişkin bilgi verilmemesi ve savunma hakkı tanınmamasına kadar birçok eleştiri dile getirilmektedir.

Buna karşılık TİB, erişim engelleme kararlarında yargı içtihatları yanında Türkiye'den erişim yoğunluğu ve özellikle çocukların doğrudan ulaşım ulaşamaması

gibi kriterlerin göz önünde bulundurulduğunu, bu süreçte, Anayasa’da geçen, temel hak ve özgürlüklerin kısıtlanmasının sınırı olarak ortaya konulan “ölçülülük ilkesi”ne uygunluğun gözetildiğini ve bu bağlamda, öncelikle erişimin engellenmesi tedbirlerinin uygulanması öncesi ve sonrasındaki süreçlerde “uyar-kaldır” mekanizmasının işletilmeye çalışıldığını belirtmektedir.

Diğer yandan, mahkemeler ve TİB, ilgili sayfayı URL’si üzerinden engellemek yerine alan adı veya IP adresinden erişim engelleme yöntemlerini tercih etmektedir. Bu durum ise, bazen masum içeriklerinde erişiminin engellenmesi sonucunu doğurmaktadır. Ancak, URL tabanlı filtrelemenin maliyeti yüksek ilave yatırım gerektirmesi yanında, bir takım teknik sorunlara sebep olması ve İnterneti yavaşlatması gibi nedenlerle servis sağlayıcıların direnciyle karşılaştığı görülmektedir. Bu nedenle, ülkemizde erişimi engelleme konusunda zor, masraflı ancak yararlı olan yöntemi kullanmak yerine kolay, ucuz, ancak bilgiye erişimi engelleme potansiyeli bulunan yöntemin uygulandığına tanık olunmaktadır.

Bunun yanında TİB, resmi web sitesinde idari tedbir olarak uygulamakta olduğu erişimi engelleme kararlarına karşı itirazda bulunulabileceğini hatırlatarak, bunun için önce “eekg.tib.gov.tr” adresinden ilgili siteye erişimin olup olmadığının sorgulanmasını talep etmektedir. Sitede ayrıca, web siteleriyle ilgili bilgilerin sorgulandığı ayrı bir “Site Bilgileri Sorgu Sayfası” oluşturulmuştur. Ayrıca TİB, Hukuk mahkemelerince erişimi engellenmiş İnternet site yetkililerinin, kararı uygulayan ilgili erişim sağlayıcılara ulaşarak bilgi alabilmesi için resmi web sitesinden erişim sağlayıcıların listesini de yayınlamaktadır.

Keza, TİB resmi web sitesinde açıkça, İnternetin dağınık ve düzenlenemeyen yapısı nedeniyle kesin bir engellenmenin söz konusu olamayacağı, bunun ancak içeriğin yayından çıkarılmasıyla mümkün olacağını belirtmekte ve eğitim, bilgilendirme ve bilinçlendirme ile maksada daha rahat ulaşılabilceğini vurgulamaktadır. Nitekim, uygulamalar da bunu göstermektedir. Türkiye’de yasaklı olmalarına rağmen birçok İnternet sitesinin ciddi görüntülenme rakamlarına ulaştıklarına tanık olunduğu gibi,

engellemeyi aşmaya yönelik yöntemler sunan tünel web sitelerinin ülkemizde oldukça rağbet gördükleri de bilinmektedir.

Diğer yandan, TİB, eleştirilere neden olsa da, erişim engelleme sayılarına ait bilgileri ve engellenen sitelerin listesini açıklamamakta, katalog suç türlerine göre oransal istatistikler yayınlamaktadır. Buna göre, müstehcenlik, çocuk pornografisi ve fuhuş suçları tüm engelleme tedbirlerinin neredeyse tamamını oluşturmaktadır. TİB, bu verileri yayınlamama sebebi olarak; yasadışı içerikle mücadeleyle ilişkin yöntemin ve bu sitelerin isimlerinin deşifresine yol açabilme ihtimalini ve suç işlenmesini teşvik etmek anlamına geleceği gerekçelerini dile getirmektedir. Dünya uygulamaları da, ilgili kurumların ve devletlerin genellikle engelli site sayılarını ve isim listelerini kamuoyu ile paylaşmadıklarını göstermektedir. Hatta, TİB gibi, kararı veren mahkemeyi, kararın tarih ve sayısını, engellemeyi yapan kurumu engelleme sayfasında yayınlayan çok az ülkeye rastlanılmaktadır. AB devletlerinin dahi ağ hatası tekniğini sıklıkla uyguladığı ve kullanıcıların, teknik bir sorundan dolayı siteye erişimin sağlanamadığı yanılgısına düşürüldüğü dikkat çekmektedir.

Bunun yanında, erişim engellemelerine ilişkin olarak, Youtube yanında dünyaca ünlü bazı sitelerin engellenmesi Türkiye’de ve dünyada TİB ile ilgili sansür eleştirilerine neden olmuştur. Nitekim Youtube’un kapatılması AB 2008 Türkiye İlerleme Raporu’nda ifade hürriyeti önündeki engellerden birisi olarak metne girmiştir. Halbuki, bu engellemelerin tamamına mahkemelerin karar verdiği; Youtube ve Geocities dışındakilerin ise, mahkeme kararı ile doğrudan erişim sağlayıcılar üzerinden gerçekleştirilmiş olduğu, erişim engelleme ile TİB’nin hiçbir ilgisinin bulunmadığı görülmektedir. Dolayısıyla eleştirileri TİB yerine, ilgili mevzuata ve mahkeme kararlarına yöneltmek daha doğru olacaktır.

Keza, Türkiye’de 5651 sayılı Yasa kapsamı dışında (telif hakları, özel yaşamın gizliliği, kişilik hakları ihlalleri vb.) mahkemelerin erişim engellemesi kararları vererek doğrudan ilgili erişim sağlayıcılar aracılığıyla bu kararları uygulattıkları görülmektedir. Bu tür kararlar TİB’nin bilgisi dışında verildiği ve Başkanlığın sürece herhangi bir müdahalesi olmadığı için uyar-kaldır süreci işletilememektedir.

Bunun dışında, TİB'nin re'sen uyguladığı engelleme kararları, özgürlüklerin idari karar ile değil ancak mahkeme kararıyla kısıtlanabileceği savından hareketle Anayasaya aykırılığı iddiasıyla eleştirilmektedir. Bu nedenle, ilgili yönetmeliklerin tümünün iptali için Danıştay'da dava açılmıştır. Fakat henüz Danıştay'dan herhangi bir iptal kararı çıkmadığı gibi, TİB'in bu güne kadar yaptığı onbinlerce idari işleme karşı açılmış çok az sayıdaki davaların hepsi TİB lehine sonuçlanmıştır. Keza, AİHM'nde bugüne kadar bu konuyla ilgili olumsuz bir karar çıkmamıştır. Dolayısıyla, TİB'in Yasa ile kendisine verilen re'sen erişim engelleme yetkisini özenle ve hukuka uygun bir şekilde kullandığı söylenebilir.

Bununla birlikte, AİHM'de, Atatürk'e hakaretle ilgili verilen ve TİB'nin uyguladığı bir mahkeme kararı haksız bulunmuş ve Türkiye ifade özgürlüğünü ihlal etmekten mahkum edilmiştir. Bu karar içerik düzenlemeleri açısından oldukça önemlidir. Çünkü, sadece Türkiye'de değil Avrupa'da da web 2.0 uygulamalarıyla ilgili olarak erişim engellemeleri ve ifade özgürlüğü kapsamında AİHM'in aldığı ilk örnek karardır. Bu karar, bundan sonra hem Türkiye hem de tüm Avrupa Konseyi üye ülkeleri için yol gösterici olacaktır.

Erişim engellemelerine ilişkin eleştiriler TİB'nı, tüm kullanıcıları kapsayan zorunlu uygulamalardan kişisel tercihe dayalı seçenekli alternatif uygulamalara yöneltmiştir. Bu kapsamda Güvenli İnternet Hizmeti sunulmuş; kısıtlama isteyen kullanıcılar için, diğer kullanıcıların özgürlüklerini etkilemeyecek alternatif bir hizmet ortaya konulmuştur. Buna göre, 2011'de işletmecilere, isteğe bağlı olmak üzere abonelerine ücretsiz olarak çocuk ve aile profilinden oluşan hizmet seçenekleri sunma zorunluluğu getirilmiştir. Bu profillerin kriterleri yeni oluşturulan Çocuk ve Aile Profil Kriterleri Çalışma Kurulu belirlemekte ve TİB, söz konusu profillere esas olan beyaz, gri ve siyah listeleri oluşturmaktadır.

Diğer yandan, Güvenli İnternet Hizmeti, bazı STK'ları tarafından, devlet eli ile merkezi filtre uygulaması ve yeni bir sansür girişimi olarak kabul edilerek eleştirilere maruz kalmıştır. Fakat, uygulama ilgi ile karşılanmış ve kısa sürede 5 milyon kullanıcı sayısına ulaşılmıştır. Bu hizmet, içerik düzenlemeleri konusunda,

gelecekte daha çok gündeme geleceği tahmin edilen, kullanıcı odaklı ve kullanıcıya farklı tercih ve seçeneklerde bulunma imkanı sağlayan önemli ve dikkate değer bir uygulamanın yolunu açmıştır. Nitekim, İngiltere başta olmak üzere, yakın gelecekte diğer demokratik ülkelerde de benzer uygulamaların görülebileceği beklenebilir.

Bambauer’ın açıklık, şeffaflık, kısıtlılık ve sorumluluk ölçütlerine dayalı meşruiyet analizini Türkiye örneği üzerinden değerlendirdiğimizde; “kısıtlılık” ölçütünün kullanılmasıyla beliren olumsuz sonuçlar dışında erişim engellemesi uygulamaları açısından Türkiye’de genel olarak önemli bir sorun gözükmemektedir. Dolayısıyla, Türkiye’deki erişim engellemesi uygulamalarının “kısıtlılık” konusu dışında ciddi bir meşruiyet sorununun bulunmadığı söylenebilir.

Sonuç olarak, 5651 sayılı Yasa ve TİB uygulamalarının eleştirilebilecek bazı yönleri bulunmakla birlikte, dünya uygulamaları göz önüne alındığında kendine özgü, makul ve olumlu görülebilecek birçok yönü göze çarpmaktadır. Zira, dünyada birçok ülkede ve uluslararası ölçekte İnternet için özel bir düzenlemenin eksikliği hissedilirken, kanunilik ilkesine uygun olarak Türkiye’de özel bir yasa ve ikincil düzenlemeler ile İnternet aktörleri tanımlanmış, sorumlulukları belirlenmiş ve içerik çıkarma mekanizması olarak “uyar-kaldır”, erişim engelleme usul ve esasları yasal düzeyde belirlenmiştir. Yine, ABD ve birçok Avrupa ülkesinde İnternet içerik düzenlemesine ilişkin işler “zorunlu gönüllülük” esasına göre herhangi bir düzenleme olmaksızın yapılıyor iken, Türkiye’de konu hukuki güvenceye kavuşturulmuştur.

Keza, erişim engellemelerine ilişkin suç türleri belirli ve sınırlı hale getirilirken, bazı devletlerde görüldüğü gibi kamu düzeninin ve genel ahlakın korunması, ulusal güvenlik ve kamu yararı gibi muğlak, geniş ve keyfi uygulamalara yol açacak genel engelleme sebepleri kapsam dışı tutulmuştur. Yine, başta ABD ve Avrupa ülkeleri olmak üzere çokça örneklerine rastlanıldığı gibi, müdahalenin kapsam ve yöntemi büyük oranda idari makamların yetkisine bırakmış uygulamalarla yürütülen, açık ve şeffaflıktan yoksun içerik politikalarına karşılık, 5651 sayılı Yasa ile daha demokratik, denetlenebilir ve şeffaf bir yaklaşım sergilenmiştir.

Hülasa, tezin onaltıncı alt hipotezinde belirtildiği gibi, 5651 sayılı Yasa ve bu Yasa'nın uygulayıcısı olan TİB, süreç içerisinde bazı uygulamalarından dolayı eleştirilse de, içerik düzenlemeleri açısından genel olarak Türkiye'nin olumlu bir adım attığı söylenebilir. Zaman içerisinde ilgili mevzuatın ve uygulamaların görülen aksaklıklar göz önünde bulundurularak revize edilmesi ve daha rafine bir hale getirilmesi mümkün ve gerekli olacaktır.

Genel olarak bakıldığında, Türkiye'nin, İnternet içerik düzenlemelerinde “üçüncü yol”u temsil etmekte olduğu söylenebilir. Türkiye; Çin, İran, Suriye, Kuzey Kore gibi İnternet trafik çıkışı üzerinde devlet tarafından sansür sayılabilecek katı uygulamalara gitmeyerek bu ülkelerden, düzenleme ve uygulamaların devlet tarafından yapılmasıyla Avrupa'dan farklılaşmaktadır. Dolayısıyla, sui generis (kendine özgü) bir uygulama ortaya koyarak, dünya açısından ilginç ve farklı bir mecrada yol almaktadır.

Sonuç olarak, tüm tez çalışması boyunca alt hipotezler üzerinden yürütülen tartışmalar, değerlendirmeler ve ele alınan konular temel hipotezimizin doğruluğunu ve geçerliliğini ortaya koymaktadır. Buna göre, bilgi toplumunun sembol ürünü olan İnternet, ele avuca sığmayan, kontrolü ve denetimi zor kendine özgü çok boyutlu ve aktörlü, karmaşık ve dinamik yapısı ile insanlığa birçok yeni imkanlar ve fırsatlar sunarken, beraberinde bir çok yeni riskler, tehlikeler ve sorunlar da getirmiştir. Bu sorunlardan birisi de, bir bütün olarak toplumun ve özellikle çocukların, gençlerin ve ailelerin İnternet ortamında yer alan yasadışı ve zararlı içeriklerden korunmasıdır.

Bu kapsamda, İnternetin sunduğu eşsiz imkan ve fırsatlardan mahrum kalmadan İnternetin daha faydalı, bilinçli, güvenli ve etkin kullanımını sağlamak için söz konusu yasadışı ve zararlı içeriklerle mücadele etmek ve konuda düzenlemeler yapmak günümüz devletlerinin en önemli ve müşkil kamu yönetimi sorunlarından birisi haline gelmiştir. Zira, İnternetin fiziki bir coğrafya ile sınırlı olmayan doğası ve teknik özellikleri konunun siyasi, sosyal, ekonomik, kültürel, hukuki, uluslararası ilişkiler vb. bir boyutunu gündeme getirmektedir.

Dolayısıyla, içerik düzenlemelerinde etkili, doğru ve meşru bir çözüm için, İnternetin kendine özgü yapısı ve özellikleri gözetilerek, gelişimine zarar vermeden, ifade özgürlüğü ve bilgiye erişim özgürlüğünü koruyarak ve “birlikte düzenleme” ve yönetim ilkeleri çerçevesinde hareket edilmelidir. Bu temel prensiplere göre oluşturulacak ve uygulanacak uygun yöntem ve yaklaşımlar içeren bütüncül strateji ve politikalar ile uluslararası işbirliği mekanizmaları İnternette yer alan yasadışı ve zararlı içeriklerden kaynaklanan risk ve tehlikeleri minimize edebilir.

Bu kapsamda, Türkiye örneği, eleştirilebilecek bir takım eksiklikler taşımakla birlikte, yasadışı ve zararlı içeriklerle mücadele konusunun özel bir yasa ile düzenlenerek kapsam ve yöntem olarak sınırlarının açıkça belirlenmesi ve bu yasa çerçevesinde geliştirdiği uygulamalar açısından kendine özgü ve önemlidir.

KAYNAKÇA

01net (2011). *Nicolas Sarkozy Conforte Hadopi Mais Reconnaît Des Erreurs [MAJ]*. <http://www.01net.com/editorial/532061/nicolas-sarkozy-conforte-hadopi-mais-reconnait-des-erreurs-maj/>, Erişim Tarihi: 11.03.2012.

1117 Sayılı Küçükleri Muzır Neşriyattan Koruma Kanunu (1927). T.C. Resmi Gazete, 627, 07.07.1927.

114.it (2012). http://www.114.it/jooml114/index.php?option=com_docman&Itemid=29, Erişim Tarihi: 17.10.2012.

2003/12 Sayılı Başbakanlık Genelgesi (2003). Başbakanlık, 27.02.2003.

2003/48 Sayılı Başbakanlık Genelgesi (2003). Başbakanlık, 04.12.2003.

2007/7 Sayılı Başbakanlık Genelgesi (2007). T.C. Resmi Gazete, 03.04.2007, 26482.

2012/3842 Sayılı Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar (2012). T.C. Resmi Gazete, 28447, 20.10.2012.

3348 Sayılı Ulaştırma Bakanlığı'nın Teşkilat ve Görevleri Hakkında Kanun (1987). T.C. Resmi Gazete, 219484, 17.04.1987.

4077 Sayılı Tüketicinin Korunması Hakkında Kanun (2003). T.C. Resmi Gazete, 25048, 14.03.2003, 4822 Sayılı Kanun.

5224 Sayılı Sinema Filmlerinin Değerlendirilmesi Ve Sınıflandırılması İle Desteklenmesi Hakkında Kanun (2004). T.C. Resmi Gazete, 25529, 14.07.2004.

5237 Sayılı Türk Ceza Kanunu (2004). T.C. Resmi Gazete, 25611, 12.10.2004 .

5326 Sayılı Kabahatler Kanunu (2005). T.C. Resmi Gazete, 25772, 31.03.2005.

5369 Sayılı Evrensel Hizmetin Sağlanması Hakkındaki Kanun (2005). T.C. Resmi Gazete, 25856, 25.6.2005.

5397 Sayılı Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun (2005). T.C. Resmi Gazete, 25884, 23.07.2005.

5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun (2007). T.C. Resmi Gazete, 26530, 23.05.2007.

5680 Sayılı Basın Kanunu (2002).

T.C. Resmi Gazete, 24761, 21.05.2002, 4756 Sayılı Kanun.

5728 Sayılı Temel Ceza Kanunlarına Uyum Amacıyla Çeşitli Kanunlarda ve Diğer Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun (2008).

T.C. Resmi Gazete, 26781, 08.02.2008.

5738 Sayılı Spor Müsabakalarına Dayalı Sabit İhtimalli ve Müşterek Bahis Oyunlarının Özel Hukuk Tüzel Kişilerine Yaptırılması Hakkında Kanun (2008).

T.C. Resmi Gazete, 26800, 27.02.2008.

5809 Sayılı Elektronik Haberleşme Kanunu (2008).

T.C. Resmi Gazete, Mükerrer 27050, 10.11.2008.

5816 Sayılı Atatürk Aleyhine İşlenen Suçlar Hakkında Kanun (1951).

T.C. Resmi Gazete, 7872, 31.07.1951.

6002 Sayılı Diyanet İşleri Başkanlığı Kuruluş Ve Görevleri Hakkında Kanun İle Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun (2010).

T.C. Resmi Gazete, 27640, 13.07.2010.

6112 Sayılı Radyo Ve Televizyonların Kuruluş Ve Yayın Hizmetleri Hakkında Kanun (2011). T.C. Resmi Gazete, 27863, 03.03.2011.

641 Karar Sayılı Kalkınma Bakanlığının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname (2011). T.C. Resmi Gazete, Mükerrer 27958, 08.06.2011.

655 Karar Sayılı Ulaştırma, Denizcilik ve Haberleşme Bakanlığı Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname (2011).

T.C. Resmi Gazete, Mükerrer 28102, 01.11.2011.

ACMA (2007). *Restricted Access System Declaration*.

http://www.acma.gov.au/webwr/_assets/main/lib310563/ras_declaration_2007.pdf, Erişim Tarihi: 26.05.2012

ACMA (2012a). *Online content complaints*. <http://www.acma.gov.au/Citizen/Take-action/Complaints/Internet-content-complaints/online-content-complaints-fact-sheet>, Erişim Tarihi: 26.05.2012.

ACMA (2012b). *Broadcasting content regulation*.

<http://www.acma.gov.au/theACMA/About/The-ACMA-story/Regulating/broadcasting-content-regulation-television-acma>, Erişim Tarihi: 27.05.2012.

ACMA (2012c). *Online content regulation*.

<http://www.acma.gov.au/theACMA/About/The-ACMA-story/Regulating/internet-online-regulation>, Erişim Tarihi: 27.05.2012.

ACMA (2012d). *Structure and contacts*.

<http://www.acma.gov.au/theACMA/About/Corporate/Structure-and-contacts>, Erişim Tarihi: 27.05.2012.

ACMA (2012e). *Content&advertising*.

http://www.acma.gov.au/WEB/STANDARD/pc=PUB_CONT_DIRACMA,Content&advertising, Erişim Tarihi: 27.05.2012.

ACMA (2012f). *ACMA Hotline: combating online child sexual abuse*.

<http://www.acma.gov.au/theACMA/About/Corporate/Accountability/the-acma-hotlinecombating-online-child-sexual-abuse>, Erişim Tarihi: 27.05.2012.

ACMA (2012g). *1 January 2011 to 31 December 2011*.

http://www.acma.gov.au/WEB/STANDARD/pc=PC_90105, Erişim Tarihi: 27.05.2012.

ACMA (2012h). *Citizen*. <http://www.acma.gov.au/Citizen>,

Erişim Tarihi: 27.05.2012.

AFA (2011). *Pointdecontact*. [http://www.afa-](http://www.afa-france.com/wa_files/CP_20AFA_20Bilan_20PDC_20janvier_202011.pdf)

[france.com/wa_files/CP_20AFA_20Bilan_20PDC_20janvier_202011.pdf](http://www.afa-france.com/wa_files/CP_20AFA_20Bilan_20PDC_20janvier_202011.pdf), Erişim Tarihi: 16.08.2012.

AFRINIC (2012). *African Network Information Center*. <http://www.afrinic.net/>,

Erişim Tarihi: 08.12.2012.

Ahaber (14.02.2013). *Sürpriz açıklama: İnternet pornosunu yasaklayacağız*.

<http://www.ahaber.com.tr/Teknoloji/2013/02/14/surpriz-aciklama-internet-pornosunu-yasaklayacagiz>, Erişim Tarihi: 16.02.2013)

Ahi, M. Gökhan (2004). *İnternet'e yasal darbe ayıkla pirincin taşını*. 29.04.2004,

<http://hurarsiv.hurriyet.com.tr/goster/ShowNew.aspx?id=221730>, Erişim Tarihi: 21.12.2012.

Akbulut, Berrin (1999). *Türk Ceza Hukuku'nda Bilişim Suçları*.

Doktora Tezi, Selçuk Üniversitesi Sosyal Bilimler Enstitüsü. Konya.

Akcan, Serkan (2008). *İnternet Firmaları Çin'de "Davranış Kuralları" Konusunda*

Görüş Birliği Yaptı. <http://www.leylakeser.org/2008/08/internet-firmalari-inde-davrani.html>, Erişim Tarihi: 10.11.2011.

Akdeniz, Yaman (1996). *Section 3 of The Computer Missuse Act 1990: An Antidote for Computer Viruses!*. *Web Journal of Current Legal Issues*. <http://webjcli.ncl.ac.uk/1996/issue3/akdeniz3.html>, Erişim Tarihi: 14.12.2011.

Akdeniz, Yaman (2003). *Beyaz Kitap - İnternet'in Çok Taraflı Yönetimi*. İstanbul: Papatya Yayınları.

Akdeniz, Yaman (2010). *TİB'e Erişim Engelleme İstatistiklerini Gizlemekten Dava*, 13.5.2010. <http://bianet.org/bianet/ifade-ozgurlugu/121956-tibe-erisim-engelleme-istatistiklerini-gizlemekten-dava>, Erişim Tarihi: 02.01.2012.

Akdeniz, Yaman (2010a). *Report of the OSCE Representative on Freedom of the Media on Turkey and Internet Censorship*. http://www.osce.org/documents/rfm/2010/01/42294_en.pdf, Erişim Tarihi: 13.11.2012.

Akdeniz, Yaman (2011). *İnternet Üzerinde İfade Özgürlüğü Yasal Hükümler Ve Uygulamaları AGİT Devletlerinde İnternet Medya Çoğulculuğu Ve Bilginin Serbest Akışı*, (Çev. Ahmet Çubukcu). AGİT Medya Özgürlüğü Temsilciliği Ofisi.

Akdeniz, Yaman ve Altıparmak, Kerem (2008). *İnternet: Girilmesi Tehlikeli ve Yasaktır*. Ankara: İmaj Yayınları.

Akdenizli, Banu (2011). *İnternet, Egemenlik ve Devlet: İnternet'in Ulusal ve Uluslararası Yönetime Etkileri Üzerine Bir Değerlendirme*. http://globalmediajournaltr.yeditepe.edu.tr/makaleler/GMJ_2._sayi_Bahar_2011/pdf/Akdenizli.pdf, Erişim Tarihi: 14.03.2012.

Akgül, Mustafa (2001). *Türkiye İnternetinin ve İnternet Kurulunun Kısa Tarihi*. 5 Temmuz 2001. <http://akgul.web.tr/yazilar/dok20.htm>, Erişim Tarihi: 16.01.2013.

Akgül, Mustafa (2008). İnternet yasakları için STK önerileri. *Inet-tr'08-XIII. Türkiye'de İnternet Konferansı Bildirileri*, 22-23 Aralık 2008, Ankara: OTDÜ.

Akgül, Mustafa (2010). 3. Yılında Türkiye'nin İnternetle Savaşı: Donkişot, Deveküşü, Harakiri. *Türk Kütüphaneciliği*, 24(2). 2010.

Akgül, Mustafa (2011). *İnternet Yönetişimi: Dünyadaki Tartışmalar ve Türkiye'deki Durum*. <http://akgul.web.tr/yazilar/hukuk/inet-yonetisim-wsis-tr.html>, Erişim Tarihi: 07.12.2011.

Akgün, Kemal vd. (2002). *İnternet Yayıncılığı ve İnternet Servis Sağlayıcılarının Sorumlulukları, Genel Politikalar ve Düzenleme Önerileri*. <http://www.teknoturk.org/docking/yazilar/tt000086-yazi.htm>, Erişim Tarihi: 12.07.2012.

- Akın, Bahadır H. (2006). *2000 Yılına Doğru Bilgi Toplumu Üzerine Genel Bir Değerlendirme ve Bilgi Ekonomisinin Özellikleri*.
<http://bilgitoplumu.blogspot.com/2006/10/2000-ylina-doru-bilgi-toplumu-zerine.html>,
 Erişim tarihi: 23.12.2009.
- Akıncı, Füsün S. (2001). *Avrupa Konseyi Siber Suç Sözleşmesi 'nde Yer Alan Maddi Ceza Hukukuna İlişkin Düzenlemeler ve İnternette Çocuk Pornografisi*.
 İstanbul Üniversitesi Hukuk Fakültesi Dergisi, LIX (1-2).
- Aksiyon (2009), <http://aksiyon.com.tr/detaylar.do?load=detay&link=25235>,
 Erişim Tarihi: 16.12.2012.
- Aksiyon (2011). <http://aksiyon.com.tr/detaylar.do?load=detay&link=25235>,
 Erişim Tarihi: 13.12.2011.
- Aksoy, Şinasi (1995). Yeni Sağ ve Kamu Yönetimi, *Kamu Yönetimi Disiplini Sempozyum Bildirileri*, Cilt:2. Ankara: TODAİE.
- Aktan, C. Can ve Vural, İstiklal Y. (2005). Bilgi Çağında Bilginin Yönetimi. (Ed. C.Can Aktan, İstiklal Y. Vural). *Bilgi Çağı Bilgi Yönetimi ve Bilgi Sistemleri*.
 Konya: Çizgi Kitabevi.
- Aktan, Can C. ve Tunç, Mehtap (1998). Bilgi Toplumu ve Türkiye.
Yeni Türkiye Dergisi, 4(19), s.118-133.
- Aktan, Coşkun C. (2003). *Değişim Çağında Devlet*. Konya: Çizgi Kitabevi.
- Akyay, Serdar (2004). İnternet Kafelerin Çocuklar Üzerine Etkileri.
Çağın Polisi Dergisi 3(32). Ağustos-2004.
- Akyıldız, Fulya (2004). *Bilgi Toplumu Yönetim Anlayışı 'nın Gerçekleşebilmesi İçin Zorunlu Bir Hak: Bilgi Edinme Hakkı*. 3. Ulusal Bilgi, Ekonomi ve Yönetim Kongresi. Ankara: Sözkese Matbacılık.
- Al, Hamza (2007). *Bilgi Toplumu ve Kamu Yönetiminde Paradigma Değişimi* (2. Basım). Ankara: Bilimadamı Yayınları.
- Alan, Adil M. (2012). *İnternet'in Aile İçi İlişkilere ve İletişime Etkileri*.
 İletişim Uzmanlığı Tezi, Bilgi Teknolojileri Ve İletişim Kurumu, Ankara.
- Al-bab (2001). *Saudi İnternet Rules 2001*. <http://www.al-bab.com/media/docs/saudi.htm>, Erişim Tarihi: 26.02.2013.
- Alexa (2013a). *Global Top Sites*. <http://www.alexa.com/topsites/global>,
 Erişim Tarihi: 22.06.2013.

Alexa (2013b). *Top Sites in Turkey*.<http://www.alexa.com/topsites/countries/TR>, Erişim Tarihi: 22.06.2013.

Alikaşifoğlu, Müjgan (2012). *İnternet Kullanımı ve Çocuk ve Ergen Sağlığı*. TBMM Bilişim ve İnternet Komisyonu Sunumu.

Alkan, Haluk ve Şimşek, Z. (1998). İnternet ve Yönetime Katılım: Potansiyel ve Olasılıklara İlişkin Bir Değerlendirme. *Türk İdare Dergisi*, Sayı: 418, Ankara: İçişleri Bakanlığı Yayını.

Alkan, Mustafa (2012). *Siber Güvenlik ve Siber Savaşlar*. TBMM Bilişim ve İnternet Komisyonu Sunumu. Mayıs-2012.

Alkan, Mustafa ve Canbay, Cafer (2003). İnternet Ve Alan Adlarının Uluslararası & Ulusal Yönetimi İle Çok Dilli Alan Adları. *İnet-tr'03, IX. Türkiye'de İnternet Konferansı Bildirileri*. 11-13 Aralık 2003. İstanbul.

Alternatif Bilişim Derneği (2012a). *İnternet İçin Tekno-Sosyal Politika Önerisi*. TBMM Bilişim ve İnternet Komisyonu Sunumu.

Alternatif Bilişim Derneği (2012b). *Türkiye'de İnternet'in Durumu*.
http://www.alternatifbilisim.org/wiki/T%C3%9CRK%C4%B0YE%E2%80%99DE_%C4%B0NTERNET%E2%80%99%C4%B0N_DURUMU#T.C3.BCkiye.E2.80.99de_Dijital_G.C3.B6zetim_ve_Derinlemesine_Veri_Analizi_Giderek_Geli.C5.9Ftirilmekte.21, Erişim Tarihi: 05.03.2013.

Altheide, David L. (2004). *The Control Narrative of the Internet. Symbolic Interaction* 27(2). Berkley: University of California Pres.

Altınay, Adem (2011). *İnternette Yer Alan İçerikler Açısından Müstehcenlikle Mücadelede Türk Hukuk Mevzuatı Mukayeseli Hukuk Ve Örnek Uygulamalar*. İletişim Uzmanlığı Tezi, Bilgi Teknolojileri Ve İletişim Kurumu, Ankara.

Altınok, Ramazan, A. (2008). *Elektronik Ticaretin KOBİ'ler Açısından Uygulanabilirliği: Ankara Örneği*, Doktora Tezi, Adnan Menderes Üniversitesi Sosyal Bilimler Enstitüsü, Aydın.

Altlaw (2012). *Sunshine Book Co. v. Summerfield*, Postmaster General, 355 U.S. 372. <http://altlaw.org/v1/cases/799128>, Erişim tarihi: 14.01.2012.

Al-Zoman, Abdulaziz H. (2001). *The Internet in Saudi Arabia (Technical View)*. 30.04.2001, <http://www.isu.net.sa/library/CETEM2001-Zoman.pdf>, Erişim Tarihi: 06.11.2011

Amnesty (2011).

http://www.amnesty.org.tr/yeni/index.php?view=article&catid=70&id=481&option=com_content, Erişim Tarihi: 13.02.2012.

Anayasa Mahkemesi (2011). *AIHS*.

http://www.anayasa.gov.tr/files/bireysel_basvuru/AIHS_tr.pdf, Erişim Tarihi: 14.12.2011.

Anayasa Mahkemesi Kararı (1964). K.T.: 28.01.1964, E: 1963/128, K: 1964/8.

Anayasa Mahkemesi Kararı (2009). K.T.: 29.01.2009, E: 2005/85, K: 2009/15.

Anayasa Mahkemesi Kararı (2012). K.T.: 21.06.2012, E: 2011/44, K: 2012/99.

Anderson, Carig A. (2004). An Update On The Effects Of Playing Violent Video Games, Science Direct. *Journal of Adolescence*, 27.

Andrews, Edmund L. (1999). *German Court Overturns Pornography Ruling Against Compuserve*.

<http://www.nytimes.com/library/tech/99/11/biztech/articles/18compuserve-germany.html>, Erişim Tarihi: 10.09.2011.

Ankara Ticaret Odası (2004). *Sanal Tuzak: İnternet Kumarhaneleri*.

<http://www.atonet.org.tr/turkce/index9.html>, Erişim Tarihi: 13.02.2011.

Antiloppsi2 (2012). *LOPSSI 2 : ils soldent nos libertés !*. <http://antiloppsi2.net/002-loppsi-2-ils-soldent-nos-libertes.html>, Erişim Tarihi: 19.04.2012.

APNIC (2012). *Asia Pacific Network Information Centre*. <http://www.apnic.net/>, Erişim Tarihi: 08.12.2012.

Arabnews (02.10.2005). *Raid Qusti, Most of Kingdom's Internet Users Aim for the Forbidden*. <http://www.arabnews.com/node/273918>, Erişim Tarihi: 24.09.2011.

ARCEP (2012). *Autorité De Régulation Des Communications Électroniques Et Des Postes*. <http://www.arcep.fr/>, Erişim Tarihi: 10.03.2012.

Archive (2011). *Internet Archive: Wayback Machine*.

<http://www.archive.org/web/web.php>, Erişim Tarihi: 24.10.2011.

Ardıç, Abdullah (2012). *Toplu İnternet Kullanım Sağlayıcılığı Kavramı, Toplu İnternet Kullanım Sağlayıcıların Hukuki, İdari Ve Teknik Sorunları Ve Düzenlemeye Yönelik Çözüm Önerileri*. İletişim Uzmanlığı Tezi, Bilgi Teknolojileri Ve İletişim Kurumu, Ankara.

AREM (2008). *İnternet Ve..*

<http://www.arem.gov.tr/Arem/defaultarem.aspx?icerik=124>,

Erişim Tarihi: 25.11.2011.

Arıcak, O. Tolga vd. (2008). Cyberbullying Among Turkish Adolescents.

CyberPsychology & Behavior, Vol. 11. N.3 Mary Ann Liebert Inc.

Arıcak, O.Tolga (2009). Üniversite Öğrencilerindeki Siber Zorbalık Davranışlarının Bir Yordayıcısı Olarak Psikiyatrik Belirtiler. *Eurasian Journal of Educational Research*, S:34.

Arıkan, Hadi (2011). *İnternet Teknolojisinin Toplumun Etik Anlayışına Etkisi Ve Etik Anlayışında Bilişimin Rolü*. İletişim Uzmanlığı Tezi, Bilgi Teknolojileri Ve İletişim Kurumu, Ankara.

ARIN (2012). *American Registry for Internet*. <http://www.arin.net/>,

Erişim Tarihi: 08.12.2012.

ARJEL (2012). *Role Et Missions*. <http://www.arjel.fr/-Role-et-missions-.html>,

Erişim Tarihi: 07.04.2012.

Aru, Çağdaş (2012). *Siber Güvenlik Kurulu, Devletin Güvenlik Resmi Politikasını Belirleyecek*. 22.10.2012,

<http://www.turk.internet.com/portal/yazigoster.php?yaziid=39502>,

Erişim Tarihi: 03.01.2013.

Aru, Çağdaş (2012a). *AIHM, 2009 Yılında Google Sites'ın Kapatılması Nedeniyle 5651'i Mahkum Etti*. 18.12.2012, <http://www.turk-internet.com/portal/yazigoster.php?yaziid=40313>, Erişim Tarihi: 03.01.2013.

Aru, Çağdaş (2012b). *OpenNet İnisiyatifi 2011'deki İnternet Sansürlerinin Haritasını Çıkarttı, Türkiye 'Seçici' Olarak Sınıflandırıldı*, 25.04.2012. <http://www.turk-internet.com/portal/yazigoster.php?yaziid=36864>, Erişim Tarihi: 03.02.2013.

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

ASAGEM (2008). *Dijital Oyunlar ve Çocuklar Üzerindeki Etkileri*. Ankara: ASAGEM Yayınları.

Atamer, İlker (2008). *İnternette Müstehcenlik ve Erişim Engelleme Kararı*.

<http://bilisimhukuku.wordpress.com/2008/02/16/internette-mustehcenlik-veerisim-engelleme-karari/>, Erişim Tarihi: 17.03.2013.

Atamer, İlker (2012). *5651 sayılı Yasa, 8. Md. Değişiklik Önerisi*.
http://internetkurulu.org/Images/Editor/av.ilker_atamer_8.%20madde_önerileri.doc,
 Erişim Tarihi: 26.06.2013.

ATHGM (2006). *Güvenli İnternet Programı ve We Want Safer Children Online*.
http://www.aile.gov.tr/konu/187/GUVENLI_INTERNET_PROGRAMI_WE_WANT_SAFER_CHILDREN_ONLINE_.htm, Erişim Tarihi: 25.01.2011.

ATHGM (2007). *Yurtdışı çalışma raporları*.
<http://www.athgm.gov.tr/tr/html/18541/Yurtdisi-calisma-raporlari>,
 Erişim Tarihi: 25.01.2011.

ATHGM (2008). *İnternet Kullanımı ve Aile*. Ankara: ATHGM Yayınları.

ATHGM (2008a). *Dijital Oyunlar ve Çocuklar Üzerine Etkileri*.
 Ankara: ATHGM Yayınları.

ATHGM (2012). *Aile ve İnternet*. TBMM Bilişim ve İnternet Komisyonu Sunumu.

Atıcı, Bünyamin ve Batı, Uğur (2010). New Media and Children: Internet Content Preferences of Primary School Children in Turkey. *International Journal of Emerging Technologies in Learning (iJET)*, Vol 5(4). <http://online-journals.org/i-jet/article/view/1321>, Erişim Tarihi: 12.01.2013.

Atıcı, Bünyamin ve Gümüş, Çetin (2006). *Sanal Ortamda Gerçek Tehditler: Siber Terör*.<http://www.bilgisayarpolisi.com/index.php?sayfa=makaleoku&kategori=5&id=68>, Erişim Tarihi: 25.12.2010.

Avcı, Nabi (1990). *Enformatik Cehalet*. Ankara: Rehber Yayıncılık.

Ayas, Tuncay ve Horzum, M. Barış (2010). Sanal Zorba/Kurban Ölçek Geliştirme Çalışması. *Akademik Bakış Dergisi*, Sayı 19, Ocak-Şubat-Mart 2010,
http://www.efdergi.ibu.edu.tr/arsiv/cilt7_sayi2/2007-2-190-202-14.pdf,
 Erişim Tarihi: 15.11.2010.

Ayas, Tuncay ve Horzum, M. Barış (2012). İlköğretim Öğrencilerinin Sanal Zorba ve Mağdur Olma Durumu. *İlköğretim Online*, 11(2). <http://ilkogretim-online.org.tr/vol11say2/v11s2m8.pdf>, Erişim Tarihi: 06.03.2013.

Ayaydın, Aydın (2010). *Google Türk devletinden büyük mü?*. 10.6.2010.
<http://haber.gazetevatan.com/haberdetay.asp?Newsid=310257&Categoryid=4&wid=153>, Erişim Tarihi: 24.11.2012.

Aydın, Münevver (22.10.2007). *Terörizm İnterneti Nasıl Kullanıyor?*.
http://www.stratejikboyut.com/article_detail.php?id=175, Erişim Tarihi: 25.12.2012.

Aydın, Selim (2004). Mükafat-Zevk Sisteminde Ruh Beden Münasebeti. *Sızıntı Dergisi*, Sayı:301.

Aydoğan, Didem vd. (2009). *İlköğretim Öğrencilerinde Sosyal Destek ve Siber Zorbalığın İncelenmesi*. 18. Ulusal Eğitim Bilimleri Kurultayı, 1-3 Ekim 2009, İzmir.

Azzurro (2013a). *OurHistory*. <http://www.azzurro.it/index.php/en/telefono-azzurro-ngo/our-history>, Erişim Tarihi: 02.02.2013.

Azzurro (2013b). *Centro Nazionale d'Ascolto Telefonico*. <http://www.azzurro.it/index.php/en/our-activites/the-national-counseling-centre>, Erişim Tarihi: 02.02.2013.

Azzurro (2013c). *Tetti Azzurri*. <http://www.azzurro.it/index.php/en/our-activites/tetti-azzurri>, Erişim Tarihi: 02.02.2013.

Azzurro (2013d). *International projects*. <http://www.azzurro.it/index.php/en/our-activites/international-projects>, Erişim Tarihi: 02.02.2013.

Bakırcı, Yasin (2009). *Internet Content Regulation And Freedom Of Expression: Assessment Of Turkish Case Within The Framework Of The ECHR*. University Of Essex, School Of Law, England.

Balcı, Asım (2008). E-Devlet: Kamu Yönetiminde Yeni Perspektifler, Fırsatlar ve Zorluklar. (Ed. Asım Balcı ve diğerleri). *Kamu Yönetiminde Çağdaş Yaklaşımlar*. (2. Baskı). Ankara: Seçkin Yayıncılık.

Bambauer, Derek E. (2008). *Guiding the Censor's Scissors: A Framework to Assessing Internet Filtering*. http://works.bepress.com/cgi/viewcontent.cgi?article=1024&context=derek_bambauer, Erişim Tarihi: 19.01.2012.

Barlow, J. Perry (1996). *A Declaration of the Independence of Cyberspace*. 8 Feb. 1996, Davos-Switzerland. <http://homes.eff.org/~barlow/Declaration-Final.html>, Erişim Tarihi: 19.11.2011.

Basalla, George (2004). *Teknolojinin Evrimi*. (Çev. Cem Soydemir). Ankara: TÜBİTAK.

Başaran, Funda (2005). *İnternetin Ekonomi Politikası. İnternet, Toplum, Kültür*. (Der. Mutlu Binark ve Barış Kılıçbay). Ankara: Epos Yayınları.

Başbakanlık (2002). *Bilgi Toplumuna Doğru Türkiye Bilişim Şurası Sonuç Raporu*, Ankara: Başbakanlık.

Bayındır, Mustafa vd. (2009). Anayurt Güvenliğinin Sağlanmasında Bilgi Sistemleri Güvenliğinin Önemi. *Akademik Bilişim '09 - XI. Akademik Bilişim Konferansı Bildiriler*. 11-13.02.2009. Harran Üniversitesi, Şanlıurfa.

Bayzan, Şahin (2011). *Dünyada İnternetin Güvenli Kullanımına Yönelik Uygulama Örnekleri Ve Türkiye'de Bilinçlendirme Faaliyetlerinin İncelenmesi Ve Türkiye İçin Öneriler*. İletişim Uzmanlığı Tezi, Bilgi Teknolojileri ve İletişim Kurumu, Ankara.

BBC (08.03.2010a). *Internet Access Is 'A Fundamental Right*. <http://news.bbc.co.uk/2/hi/8548190.stm>, Erişim Tarihi: 12.11.2012.

BBC (08.03.2010b). *Four In Five Regard Internet Access As A Fundamental Right: Global Poll*. http://news.bbc.co.uk/2/shared/bsp/hi/pdfs/08_03_10_BBC_internet_poll.pdf, Erişim Tarihi: 12.11.2012

BBC (09.10.2012). *Limit children's scree time, expert urges*. <http://www.bbc.co.uk/news/education-19870199>, Erişim Tarihi: 26.12.2012.

BBC (11.06.2010). *'Shady' porn site practices put visitors at risk*. <http://news.bbc.co.uk/2/hi/technology/10289009.stm>, Erişim Tarihi: 12.11.2012.

BBC (23.05.2000). *France Bans İnternet Nazi Auctions*. <http://news.bbc.co.uk/2/hi/europe/760782.stm>, erişim Tarihi: 08.12.2011.

BBC (25.03.2009). *Social network sites 'monitored'*. http://news.bbc.co.uk/2/hi/uk_news/7962631.stm, Erişim Tarihi: 15.02.2012.

BBC (29.06.2008). *Council Ban On Atheist Websites*. http://news.bbc.co.uk/2/hi/uk_news/england/west_midlands/7530519.stm, Erişim Tarihi: 21.12.2011.

BBFC (2011). *About The BBFC*. <http://www.bbfc.co.uk/>, Erişim Tarihi: 02.12.2011.

Beceni, Yasin (2004). *Siber Uzayda Mahremiyet. Türkiye Bilişim Şurası Hukuk Çalışma Grubu Raporu*. http://www.bilisimsurasi.org.tr/hukuk/docs/siber_uzayda_mahremiyet.pdf, Erişim Tarihi: 23.10.2010

Beck, Ulrich (2002). The Terrorist Threat World Risk Society Revisited. *Theory, Culture & Society*, 19(4).

Beger, Gerrit vd. (2011). *Çevrimiçi Genç Türkiye-Türkiye'deki Dijital Durumla ilgili Araştırma Çalışması*. UNİCEF Raporu, 3.11.2011, <http://panel.unicef.org.tr/vera/app/var/files/c/e/cevrimici-genc-turkiye-18.11.11.doc>, Erişim Tarihi: 25.02.2013.

- Bell, Daniel (2000). *An Introduction The Cybercultures*. Routledge, London.
- Belsey, Bill (2007). Cyberbullying: A Real And Growing Threat. *Ata Magazine* 88(1).
<http://www.teachers.ab.ca/Publications/ATA%20Magazine/Volume%2088/Number%201/Articles/Pages/Cyberbullying.aspx>, Eriřim Tarihi: 17.10.2010.
- Bennett, Colin J. (2001). Cookies, web bugs, webcams and cue cats: Patterns of Surveillance on the world wide web. *Ethics and Informaion Technology* 3(3). Kluwer Academic Publishers, Netherlands.
- Bensghir, Türksel (1996). *Bilgi Teknolojileri ve Örgütsel Deęişim*. Ankara: TODAİE.
- Bensghir, Türksel K. Ve Altınok, A.Ramazan (2005). *İnternet'in Aile İliřkilere Etkileri: Türkiye'de Devletin ve Ailelerin Konuya Bakışı*. Ankara.
- Berber, Levent ve Kaya, M. Bedii (01.12.2010). *5651 sayılı Kanun Deęişikliğine İliřkin Gerekçeler*.
http://internetkurulu.org/Images/Editor/5651_degisiklik_gerekce_avleventberber_avmbediikaya.pdf, Eriřim Tarihi: 18.112012.
- Berber, Levent ve Kaya, M. Bedii (26.07.2010). *5651 sayılı Kanunun Teknik ve Hukuki Açından Deęerlendirilmesi - 6 / Almanya*.
<http://www.turk.internet.com/portal/yazigoster.php?yaziid=28670>, Eriřim Tarihi: 14.09.2011.
- Berkmen Center (2008). *Enhancing Child Safety and Online Technologies*.
http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/ISTTF_Final_Report.pdf, Eriřim Tarihi, 14.09.2012.
- Bianet (22.07.2013). *İngiltere Pornoyu Filtreleyecek*. <http://bianet.org/bianet/ifade-ozgurlugu/148655-ingiltere-pornoyu-filtreleyecek>, Eriřim Tarihi: 22.07.2013
- Bilgi Teknolojileri ve İletişim Kurumu Teşkilat Yönetmelięi (2011). T.C. Resmi Gazete, 27958, 08.06.2011.
- Bilgiç, Veysel (2008). *Yeni Kamu Yönetimi Anlayışı*. (Ed. Asım Balcı ve dięerleri). Kamu Yönetiminde Çaędař Yaklaşımlar. (2. Baskı). Ankara: Seçkin Yayıncılık.
- Bilgitoplumu (2004). *Bilgi Toplumuna Dönüşüm Politikası*.
http://www.bilgitoplumu.gov.tr/Documents/1/Icra_Kurulu/040610_IcraKurulu6ToplantisKararNo4.pdf, Eriřim Tarihi: 12.02.2013.
- Bilgitoplumu (2013a). *Bilgi Toplumu Tarihçesi*.
<http://www.bilgitoplumu.gov.tr/Portal.aspx?value=UE9SVEFMSUQ9MSZQQUdFS>

UQ9MTM5JIBBR0VWRVJTSU9OPS0xJk1PREU9UFVCTEITSEVEX1ZFUINJT04=, Erişim Tarihi: 11.02.2013.

Bilgitoplumu (2013b). *E-Dönüşüm Türkiye Projesi*.
<http://www.bilgitoplumu.gov.tr/Portal.aspx?value=UE9SVEFMSUQ9MSZQQUdFSUQ9MTUwJIBBR0VWRVJTSU9OPS0xJk1PREU9UFVCTEITSEVEX1ZFUINJT04=>, Erişim Tarihi: 11.02.2013.

Bilgitoplumustratejisi (2013). *Bilgi Toplumu Stratejisi Proje ve Katılımcılık Portalı*.
<http://www.bilgitoplumustratejisi.org/tr/doc/8a3247663b7ba1e7013b7bb82bdf0002>,
 Erişim Tarihi: 24.04.2013.

Bilgitoplumustratejisi (2013a). *Bilgi Toplumu Stratejisinin Yenilenmesi Projesi, İhtiyaç Tespiti ve Öneriler Raporu*. 13.05.2013.
http://www.bilgitoplumustratejisi.org/tr/node/ihhtiyac_tespiti_ve_oneriler_raporu,
 Erişim Tarihi: 21.06.2013.

Bilisim Akademi (2006). *Web Hosting Nedir?*
<http://www.bilisimakademi.net/kbOku.asp?kbID=36>, Erişim Tarihi: 12.07.2011.

Binark vd. (2009). *Dijital Oyun Rehberi Oyun Tasarımı Türler ve Oyuncu*.
 Ankara: Kalkedon Yayınları.

Binark, Mutlu ve Sütçü, Günseli B. (2008a). *Kültür Endüstrisi Olarak Dijital Oyun*.
 İstanbul: Kalkedon Yayınları.

Binark, Mutlu ve Sütçü, Günseli B. (2008b). *Dijital Oyun-Oyun Türleri Ve Oyun-Oyuncu İlişkisi: Nasıl Dijital Oyun Oynamalı? Eleştirel Pedagoji ve Yeni Medya Okuryazarlığının Gerekliliği*. <http://inet-tr.org.tr/inetconf11/bildiri/89.pdf>, Erişim Tarihi: 18.10.2010.

Birtek, Fatih (2011). *İfade Özgürlüğü ve Türk Ceza Kanunu'nun 301. Maddesinin Bu Kavram Işığında Değerlendirilmesi*.
http://www.turkhukuk sitesi.com/makale_780.htm, Erişim Tarihi: 30.04.2011.

Bitdefender (2011). *Case Study, Kids&Online Threats*.
<http://www.bitdefender.com/media/materials/white-papers/en/Bitdefender-CaseStudy-Kids.pdf>, Erişim Tarihi: 19.06.2012.

Bolişik, Bahire ve K. Muslu, Gonca (2009). *Çocuk ve Gençlerde İnternet Kullanımı. TAF Preventive Medicine Bulletin*, 8.

Bora, Erhan (08.02.2008). *2007 Siber Suçluların ve DDOS Saldırıların Arttığı Yıl Oldu*. <http://turk.internet.com/haber/yazigoster.php3?yaziid=20166>,
 Erişim Tarihi: 12.7.2011.

Botfrei (2012). *DDoS*. <https://www.botfrei.de/tr/fragen.html#ddos>
Eriřim Tarihi: 27.04.2012.

Bouché, Noel J. (2009). *EXPLOITED: Sex Trafficking, Porn Culture, and the Call to a Lifestyle of Justice*. <http://www.purehope.net/images/purejustice/Exploited.pdf>,
Eriřim Tarihi: 14.12.2012.

Bozarth, Michael A. (1994). *Pleasure Systems In The Brain*.
<http://www.addictionscience.net/ASNreport01.htm>. Eriřim Tarihi: 15.10.2011.

Bozkurt, Abdullah S. (2012). *Dünyadaki İnternet İçerik Düzenleyici Kuruluşlar, Bunların Uygulamaları Ve Telekomünikasyon İletişim Başkanlığı Örneği*. İletişim Uzmanlığı Tezi, Bilgi Teknolojileri ve İletişim Kurumu, Ankara.

Bozkurt, Veysel (1996). *Enformasyon Toplumu ve Türkiye*.
İstanbul: Sistem Yayınları.

Bozkurt, Veysel (2011). *Gözetim ve İnternet: Özel Yaşamın Sonu Mu?*.
<http://www.isguc.org/vbozkurt4.htm>, Eriřim Tarihi: 13.01.2011.

BSA (2011). *2010'da Yazılım Hırsızlığının Türkiye'ye Maliyeti 516 milyon dolar*.
http://globalstudy.bsa.org/2010/downloads/press/pr_turkey_turkish.pdf,
Eriřim Tarihi: 02.08.2011.

BTK (2011a). *Ulusal Siber Güvenlik Tatbikatı 2011*.
http://www.tk.gov.tr/bilgi_teknolojileri/siber_guvenlik/usgt2011.php,
Eriřim Tarihi: 17.04.2013.

BTK (2011b). *Güvenli İnternet Hizmetine İlişkin Usul ve Esaslar*.
http://www.tk.gov.tr/mevzuat/kurul_kararlari/dosyalar/2011%20DK-14-461.pdf,
Eriřim Tarihi: 24.04.2013.

BTK (2011c). *Güvenli İnternet Hizmeti Basın Açıklaması*, 02.11.2011.
http://www.btk.gov.tr/basin_bultenleri/dosyalar/guvenliinternethizmeti22-11-2011.pdf, Eriřim Tarihi: 13.10.2012.

BTK (2011d). *24.08.2011 tarihli ve 2011/DK-14/461 sayılı Kurul Kararı*.
http://www.tk.gov.tr/mevzuat/kurul_kararlari/dosyalar/2011%20DK-10-91sss.pdf,
Eriřim Tarihi: 23.07.2013.

BTK (2012). *Türkiye'de Genişbant İnternet Pazarı ve Güvenli İnternet Kullanımı*.
TBMM Biliřim ve İnternet Komisyonu Sunumu.

BTK (2012a). *Siber Kalkan Tatbikatı 2012*.
http://www.tk.gov.tr/bilgi_teknolojileri/siber_guvenlik/uskt2012.php,
Eriřim Tarihi: 17.04.2013.

BTK (2012b). *Tüketici Ödülleri Yarışmasında BTK'ya "Güvenli İnternet" Ödülü Verildi*. <http://www.tk.gov.tr/sayfa.php?ID=90>, Erişim Tarihi: 12.01.2013.

BTK (2013). *2012 Yılı Faaliyet Raporu*. Ankara: BTK.

BTK (2013a). *Türkiye Elektronik Haberleşme Sektörü, 2012 Yılı 4. Çeyrek Raporu*. Mart-2013.
http://www.btk.gov.tr/kutuphane_ve_veribankasi/pazar_verileri/ucaylik12_4.pdf,
Erişim Tarihi: 10.04.2013.

BTK (2013b). *Çalışmalar*.
http://www.tk.gov.tr/bilgi_teknolojileri/siber_guvenlik/calismalar.php,
Erişim Tarihi: 17.04.2013.

BTK (2013c). *Ulusal Siber Güvenlik Tatbikatı 2013*.
http://www.tk.gov.tr/bilgi_teknolojileri/siber_guvenlik/usgt2013.php,
Erişim Tarihi: 17.04.2013.

BTK (2013d). *Kurumun Görevleri*. http://www.tk.gov.tr/kurum_hakkinda/gorevler/,
Erişim Tarihi: 17.04.2013.

BTK (2013e). *Kuruluş*. http://www.tk.gov.tr/kurum_hakkinda/kurulus/index.php,
Erişim Tarihi: 17.04.2013.

Bt-stk.org. (2006). *Bilişim Ağı Hizmetlerinin Düzenlenmesi ve Bilişim Suçları Kanun Tasarısı, Kişisel Verilerin Korunması Hakkında Kanun Tasarısı-Genel Gerekçe*.
<http://bt-stk.org.tr/bilisim-hizmetler-suclari.html>, Erişim Tarihi: 12.02.2013.

Bulut, Eduard A. (2009). *Türkiye'de İnternet Yasakları*.
<http://www.unak.org.tr/BilgiDunyasi/gorusler/2009/cilt10/sayi2/163-185.pdf>,
Erişim Tarihi: 12.01.2012.

Bulut, Nihat (2013). *Hak ve Özgürlüklerin Sınırlandırılma Nedeni Olarak Genel Ahlak*. <http://archiv.jura.uni-saarland.de/turkish/NBulut.html>,
Erişim Tarihi: 17.03.2013.

Bundespruefstelle (2012a). *Wegweiser Jugendmedienschutz: Computer- und Konsolenspiele*.
<http://www.bundespruefstelle.de/bpjm/Jugendmedienschutz/Wegweiser-Jugendmedienschutz/pc-und-konsolenspiele,did=33032.html>,
Erişim Tarihi: 03.04.2012.

Bundespruefstelle (2012b). *Wegweiser-jugendmedienschutz*.
<http://www.bundespruefstelle.de/bmfsfj/generator/bpjm/Jugendmedienschutz/wegweiser-jugendmedienschutz>, Erişim Tarihi: 03.04.2012.

Bundespruefstelle (2012c). *Wegweiser Jugendmedienschutz: Internet*.
<http://www.bundespruefstelle.de/bpjm/Jugendmedienschutz/Wegweiser-Jugendmedienschutz/internet.html>, Eriřim Tarihi: 03.04.2012.

Bundespruefstelle (2012d). *Medienerziehung*.
<http://www.bundespruefstelle.de/bpjm/Jugendmedienschutz-Medienerziehung/Erziehung-Medienkompetenz/medienerziehung.html>,
 Eriřim Tarihi: 03.04.2012.

Buzer (2007). *Teledienstegezet-TDG*.
<http://www.buzer.de/s1.htm?g=TDG+1997&f=1>, Eriřim Tarihi: 14.01.2012.

Caincross, Frances (1997). *The Death of Distance*. London: Orion Business Books.

Campbell, Penny and Machet, Emmanuelle (1999). European Policy on Regulation of Content on the Internet. Liberating Cyberspace: Civil Liberties, *Human Rights And The Internet*, (Edited by Liberty). London.

Canbay, Cafer (2005). *Alan Adları Yönetimi, Dünya Uygulamaları Türkiye İçin Çözümsel Yaklaşımlar*. Telekomünikasyon Kurumu Uzmanlık Tezi. Ankara.

Canbek, Gürol ve Sağıroğlu, Şeref (2007a). Kötücül ve Casus Yazılımlar: Kapsamlı Bir Arařtırma. *Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi* 22 (1).

Canbek, Gürol ve Sağıroğlu, Şeref (2007b). Çocukların ve Gençlerin Bilgisayar ve İnternet Güvenliğı. *Politeknik*. Sayı:1.

Castells, Manuel (2008). *Ağ Toplumunun Yükseliři*. (Çev. Ebru Kılıç). İstanbul: Bilgi Üniversitesi Yayınları.

Castells, Manuel ve İnce, Martin (2006). *Manuel Castells'le Söyleřiler*. (Çev. Ebru Kılıç). İstanbul: Bilgi Üniversitesi Yayınları.

Caydı, S. Salih (15.11.2010). *Endüstrisi ve Sosyal Tahribatıyla Yeni Pornografi*.
<http://bianet.org/biamag/bianet/126083-endustrisi-ve-sosyal-tahribatiyla-yeni-pornografi>. Eriřim Tarihi: 21.12.2012.

Center for the Digital Future (2008). *Digital Future Report*.
<http://www.digitalcenter.org/pdf/2008-Digital-Future-Report-Final-Release.pdf>,
 Eriřim Tarihi: 23.11.2011.

CEOP (2012). *Child Exploitation And Online Protection Centre*.
<http://www.ceop.police.uk/>, Eriřim Tarihi: 02.06.2012.

CGI.br (2013a). *Sobre o CGI.br*. <http://www.cgi.br/sobre-cg/index.htm>,
 Eriřim Tarihi: 28.02.2013.

- CGI.br (2013b). *Ortaria Interministerial N° 147, de 31 de maio de 1995*. <http://www.cgi.br/regulamentacao/port147.htm>, Eriřim Tarihi: 28.02.2013.
- CGI.br (2013c). *Decreto N° 4.829, de 3 de setembro de 2003*. <http://www.cgi.br/regulamentacao/decr4829.htm>, Eriřim Tarihi: 28.02.2013.
- CGI.br (2013d). *Decreto Presidencial n° 4.829*. <http://www.cgi.br/sobre-cg/definicao.htm>, Eriřim Tarihi: 28.02.2013.
- CGI.br (2013e). *Membros do CGI.br*. <http://www.cgi.br/sobre-cg/membros.htm>, Eriřim Tarihi: 28.02.2013.
- CGI.br (2013f). *Reunioes Extraordinarias*. http://www.cgi.br/acoes/reunioes_extraordinarias/2013/, Eriřim Tarihi: 28.02.2013.
- CGI.br (2013g). *Comissões de Trabalho*. <http://www.cgi.br/acoes/conteudos.htm#1>, Eriřim Tarihi: 28.02.2013.
- China Digital Times (2009). *Baidu's Internal Monitoring and Censorship Document Leaked*. <http://chinadigitaltimes.net/2009/04/baidus-internal-monitoring-and-cens>, Eriřim Tarihi: 11.01.2012.
- China.org (2009). *China begins crackdown on Web porn*. http://www.china.org.cn/government/central_government/2009-01/06/content_17059928.htm, Eriřim Tarihi: 11.12.2012.
- Chinainternetwatch (2012). *China Internet Illegal Information Reporting Centre*. <http://www.chinainternetwatch.com/tag/ciirc/>, Eriřim Tarihi: 14.12.2012.
- CIA (2012). *Directorate of Intelligence, Chiefs of State & Cabinet Members of Foreign Governments*. <https://www.cia.gov/library/publications/world-leaders-1/pdfversion/March2012ChiefsDirectory.pdf>, Eriřim Tarihi: 12.07.2012.
- Clayton, Richard (2012). *Failures in a Hybrid Content Blocking System*. <http://www.cl.cam.ac.uk/~rnc1/cleanfeed.pdf>, Eriřim Tarihi: 12.02.2012.
- Clayton, Richard, vd. (2006). *Ignoring the Great Firewall of China*. Computer Laboratory, William Gates Building, 15 JJ Thomson Avenue, Cambridge CB3 0FD, University of Cambridge, United Kingdom.
- Cnews (2008). *For a Virtual Offence of Putin Was Given a Prison Sentence*, 1 November 2008. <http://internet.cnews.ru/news/top/index.shtml?2008/11/01/32576>, Eriřim Tarihi: 12.05.2011.
- CNIL (2012a). *Missions*. <http://www.cnil.fr/la-cnil/missions/>, Eriřim Tarihi: 10.03.2012.

CNIL (2012b). *International*. <http://www.cnil.fr/la-cnil/international/>,
Eriřim Tarihi: 10.03.2012.

CNIL (2012c). *Plainte en ligne*. <http://www.cnil.fr/vos-libertes/plainte-en-ligne/>,
Eriřim Tarihi: 10.03.2012.

CNN (25.02.2008). *Pakistan move knocked out YouTube*.
<http://www.cnn.com/2008/WORLD/asiapcf/02/25/pakistan.youtube/>,
Eriřim Tarihi: 03.10.2012.

CNNTURK (20.11.2006). *Çocuk pornosu Türkiye'ye yayılıyor*.
http://www.cnnturk.com/TURKIYE/haber_detay.asp?PID=318&HID=1&haberID=262080, Eriřim Tarihi: 30.07.2011.

CNNTURK (2008). *Türkler, Youtube yasağını deliyor*.
http://www.cnnturk.com/haber_detay.asp?haberID=471134&PID=16,
Eriřim Tarihi: 18.09.2011.

Cnnumerique (2012). *Missions*. <http://www.cnnumerique.fr/missions/>,
Eriřim Tarihi: 11.03.2012.

COE (2001). *Convention on Cybercrime*.
<http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm>,
Eriřim Tarihi: 24.03.2012.

COE (2003a). *Additional Protocol To The Convention On Cybercrime, Concerning The Criminalisation Of Acts Of A Racist And Xenophobic Nature Comitted Through Computer Sysytems*. <http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm>,
Eriřim Tarihi: 24.03.2012.

COE (2003b). *Declaration on Freedom of Communication on the Internet*.
<https://wcd.coe.int/ViewDoc.jsp?id=37031>, Eriřim Tarihi: 12.02.2012.

COE (2005). *Declaration of the Committee of Ministers on Human Right and the Rule of Law in the Information Society*.
[https://wcd.coe.int/ViewDoc.jsp?Ref=CM\(2005\)56&Sector=secCM&Language=lanEnglish&Ver=final&BackColorInternet=9999CC&BackColorInternet=FFBB55&BackColorLogged=FFAC75](https://wcd.coe.int/ViewDoc.jsp?Ref=CM(2005)56&Sector=secCM&Language=lanEnglish&Ver=final&BackColorInternet=9999CC&BackColorInternet=FFBB55&BackColorLogged=FFAC75), Eriřim Tarihi: 12.01.011.

Comlaw (2012a). *Broadcasting Services Act*.
<http://www.comlaw.gov.au/Details/C2004C02582>, Eriřim Tarihi: 12.01.2012.

Comlaw (2012b). *Australian Communications and Media Authority Act*.
<http://www.comlaw.gov.au/Details/C2005A00044>, Eriřim Tarihi: 25.02.2012.

Comlaw (2012c). *Classification (Publications, Films and Computer Games) Act*. <http://www.comlaw.gov.au/Details/C2010C00487>, Erişim Tarihi: 25.02.2012.

Comlaw (2012d). *Guidelines for the Classification of Films And Computer Game*. <http://www.comlaw.gov.au/Details/F2008C00126>, Erişim Tarihi: 25.02.2012.

Computerweekly (2001). *Judge dismisses French case against Yahoo*. <http://www.computerweekly.com/Articles/2001/11/09/183630/judge-dismisses-french-case-against-yahoo.htm>, Erişim Tarihi: 10.12.2011.

ComScore (14.10.2011). *More than 200 Billion Online Videos Viewed Globally in October*. http://www.comscore.com/Insights/Press_Releases/2011/12/YouTube_Accounts_for_At_Least_34_Percent_of_All_Videos, Erişim Tarihi: 15.03.2013.

ComScore (18.10.2011). *Turkey Has Third Most Engaged Online Audience in Europe*. http://www.comscore.com/Insights/Press_Releases/2011/10/Turkey_Has_Third_Most_Engaged_Online_Audience_in_Europe, Erişim Tarihi: 15.03.2013.

ComScore (20.12.2012). *Argentina Ranks First in Worldwide Desktop Social Networking Engagement at Nearly 10 Hours per Visitor Each Month*. http://www.comscore.com/Insights/Press_Releases/2012/12/Argentina_Ranks_First_in_Worldwide_Desktop_Social_Networking_Engagement, Erişim Tarihi: 07.02.2013.

ComScore (21.03.2013). *2013 Europe Digital Future in Focus*. http://www.comscore.com/Insights/Presentations_and_Whitepapers/2013/2013_Europe_Digital_Future_in_Focus, Erişim Tarihi: 05.03.2013.

Constitution (2013). *The Constitution of the Russian Federation-1993*. <http://www.constitution.ru/en/10003000-01.htm>, Erişim Tarihi: 25.02.2013.

Cornwell, John (27.04.2008). *Is Technology Ruining Children?*. <http://www.thesundaytimes.co.uk/sto/style/living/article87672.ece>, Erişim Tarihi: 26.12.2012.

Coşkun, Bayram (2008). Kamu Yönetiminde Yeniden Yapılanma Üzerine Bir Değerlendirme. (Ed. Asım Balcı ve diğerleri). *Kamu Yönetiminde Çağdaş Yaklaşımlar*. (2. Baskı). Ankara: Seçkin Yayıncılık.

Coşkun, Selim (2008). Kamu Yönetiminde Yönetişim Yaklaşımı, Kamu Yönetiminde Çağdaş Yaklaşımlar. (Ed. Asım Balcı ve diğerleri). *Kamu Yönetiminde Çağdaş Yaklaşımlar*. (2. Baskı). Ankara: Seçkin Yayıncılık.

Covenanteyes (02.19.2013). *Get the Latest Pornography Statistics*.
<http://www.covenanteyes.com/2013/02/19/pornography-statistics/>,
 Eriřim Tarihi: 08.03.2013.

Creativecommons (2011). *About*. <http://www.creativecommons.org>,
 Eriřim Tarihi: 11.02.2011.

CSA (2012). *Conseil Supérieur De L'audiovisuel*. <http://www.csa.fr/>,
 Eriřim Tarihi: 10.03.2012.

Csmonitor (16.09.2005). *UN control of Internet? Try again*.
<http://www.csmonitor.com/2005/0916/p08s02-comv.html>, Eriřim Tarihi: 11.12.2012.

Culture (2012a). *What we do*. http://www.culture.gov.uk/what_we_do/default.aspx,
 Eriřim Tarihi: 15.02.2012.

Culture (2012b). *Telecommunications and online*.
http://www.culture.gov.uk/what_we_do/telecommunications_and_online/7761.aspx,
 Eriřim Tarihi: 15.02.2012.

Cybercrime (2011). *Patriot Act*. <http://www.cybercrime.gov/PatriotAct.htm>,
 Eriřim Tarihi: 12.01.2012.

Cyberhus (2013). www.cyberhus.dk, Eriřim Tarihi: 12.01.2013.

Cyberlaw (2008). *Extreme Pornography Offence Includesdisproportionate Penalties*.
<http://cyberlaw.org.uk/2008/05/01/extreme-pornography-offence-includes-disproportionate-penalties/>, Eriřim Tarihi: 05.09.2011.

Cyber-rights.org (2002). *Statement by Dr. Yaman Akdeniz in relation to the Internet related provisions of the Turkish Supreme Board of Radio and Television (RTUK) Bill (No 4676)* 15 May, 2002. http://www.cyber-rights.org/press/tr_rtuk.htm,
 Eriřim Tarihi: 11.03.2013.

Cybersmart (2012). <http://cybersmart.gov.au/>, Eriřim Tarihi: 19.06.2012.

CYBERTIP (2013). *Federal mandatory reporting*.
http://www.cybertip.ca/app/en/federal_mandatory_reporting, Eriřim Tarihi: 6.8.2012.

CYBERTİP (2009). *Child Sexual Abuse Images: An Analysis of Websites by Cybertip.ca in November 2009*.
https://www.cybertip.ca/pdfs/Cybertip_researchreport.pdf, Eriřim Tarihi: 09.04.2012.

Çağiltay vd., Kürřat (2008). *A Descriptive Study of Turkish High School Students' Game –Playing Characteristics and Their Considerations Concerning the Effects of Games*. *Computers in Human Behavior*. Sayı 24.

Çağlar, Edip (2011). *Türk Hukukunda ve Mukayeseli Hukukta İnternet Sitelerine Erişimin Engellenmesi ve İfade Hürriyeti*. İletişim Uzmanlığı Tezi, Bilgi Teknolojileri ve İletişim Kurumu, Ankara.

Çam, Şerife (2003). Çocuk Pornografisi Tartışmalarına İlişkin Sorular. *İletişim Araştırmaları*, 1(2). <http://acikarsiv.ankara.edu.tr/browse/5095/5704.pdf>, Erişim Tarihi: 12.01.2013.

Çamlı, Ceyhun (2010a). *5651 Sayılı Kanunun Teknik ve Hukuki Açısından Değerlendirilmesi - 4 / İSS'lerin Sorumlulukları*. <http://www.turk.Internet.com/portal/yazigoster.php?yaziid=28668>, Erişim Tarihi: 21.01.2012.

Çamlı, Ceyhun (2010b). *5651 Sayılı Kanunun Teknik ve Hukuki Açısından Değerlendirilmesi - 6/ Almanya*. <http://www.turk.Internet.com/portal/yazigoster.php?yaziid=28669>, Erişim Tarihi: 11.03.2012.

Çamlı, Ceyhun (2010c). *5651 Sayılı Kanunun Teknik ve Hukuki Açısından Değerlendirilmesi -7 / Fransa & İngiltere*. <http://www.turk.Internet.com/portal/yazigoster.php?yaziid=28671>, Erişim Tarihi: 11.03.2012.

Çehreli, Murat (04.10.2011). *Online Porno İzleme Gençler Arasında Yaygınlaşıyor*. <http://www.turk-internet.com/portal/yazigoster.php?yaziid=33987>, Erişim Tarihi: 12.07.2012.

Çehreli, Murat (11.06.2008). *ABD'nin 3 ISS'i Çocuk Pornosu İçeriğini Bloklama Kararı Aldı*. <http://www.turk.internet.com/portal/yazigoster.php?yaziid=21182>, Erişim Tarihi: 24.05.2012.

Çehreli, Murat (18.07.2008). *Ayşen Gürcan: Bilgisayar Oyunları Çocukları Şiddete Özendirebiliyor*. <http://www.turk.internet.com/portal/yazigoster.php?yaziid=21484>, Erişim Tarihi: 16.10.2012.

Çehreli, Murat (22.12.2009). *Facebook Boşanma Nedeni*. <http://www.turk.internet.com/portal/yaziyaz.php?yaziid=25931>, Erişim Tarihi: 14.12.2011.

Çetinkaya, Esra B. (15.09.2006). *Pedofili (Çocuk Tacizi) Vakaları Hakkında Detaylı Bir Çalışma*. <http://www.hukuki.net/archive/index.php?t-13890.html>, Erişim Tarihi: 27.04.2012.

Çoban, Hasan (1996). *Bilgi Toplumuna Planlı Geçiş*. Ankara: DPT.

Çocukhakları (2012). *The Optional Protocol to the Convention on the Rights the Child on the sale of children, child prostitution and child pornography*.

http://www.cocukhaklari.gov.tr/condocs/mevzuat/cocuk_haklari_sozlesmesi.pdf,

Erişim Tarihi: 18.02.2012.

Çubukcu, Ahmet ve Bayzan, Şahin (2013). Türkiye’de Dijital Vatandaşlık Algısı ve Bu Algıyı İnternetin Bilinçli, Güvenli ve Etkin Kullanımı ile Artırma Yöntemleri.

Middle Eastern & African Journal of Educational Research. Issue 5,

http://www.majersite.org/issue5/12_cubukcu_and_bayzan.pdf,

Erişim Tarihi: 25.06.2013.

Dailybits (2008). *Top 10 Countries Censoring the Web*.

<http://www.dailybits.com/top-10-countries-censoring-the-web/>,

Erişim tarihi: 29.12.2012.

Dal, Seniha (2010). Türk Hukukunda İnternet Alan Adları (Domain Names) ve Bu Alandaki Son Gelişmeler. *Marmara Üniversitesi İ.İ.B.F. Dergisi, Cilt XXV(1)*.

http://iibf.marmara.edu.tr/iysdosya/fakulte/iibfdergi_2010_1/24_dal.pdf,

Erişim Tarihi: 16.04.2013.

DBCDE (2012). *Cybersafety help button*.

http://www.dbcde.gov.au/online_safety_and_security/cybersafetyhelpbutton_downlo

ad, Erişim Tarihi: 19.06.2012.

DBCDE (2012). *Online safety and security*, <http://www.dbcde.gov.au/broadband>;

http://www.dbcde.gov.au/online_safety_and_security, Erişim Tarihi: 27.05.2012.

Dede, Melih B. (03.05.2010). *Sosyal Ağlar 'Dikizleme Çağı' Araçları mı?*.

<http://yenisafak.com.tr/Bilisim/?t=03.06.2010&i=260124>, Erişim Tarihi: 11.09.2012.

Dedeoğlu, Gözde (2006). *Bilişim Toplumu ve Etik Sorunlar*. Bursa: Alfa Yayınları.

Deibert, Ronald, Palfrey, John, Ronozinski, Rafal and Zittrain, Jonathan (2008).

Access Denied: The Practice and Policy of Global Internet Filtering.

Cambridge, Massachusetts: The MIT Pres.

Delegation Internet (2012a). *Mission*.

<http://www.delegation.internet.gouv.fr/mission/index.htm>,

Erişim Tarihi: 28.06.2012.

Delegation Internet (2012b). *Membres*. <http://www.cnnumerique.fr/membres/>,

Erişim Tarihi: 28.06.2012.

- Demirkan, Erkan (09.09.2010). *Ulusal Güvenlikte Antivirüs Tehdidi*. <http://www.bilgiguvenligi.gov.tr/zararli-yazilimlar/ulusal-guvenlikte-antivirus-tehdidi.html>, Erişim Tarihi: 25.11.2012.
- Dewaagnederland (2013). <http://www.dewaagnederland.nl/>, Erişim Tarihi: 23.2.2013.
- DFT (2012). *What we do*. <https://www.gov.uk/government/organisations/department-for-transport>. Erişim Tarihi: 15.02.2012.
- Diffie, W. & Landau, S. (1998). *Privacy on the Line: The Politics of Wiretapping and Encryption*. Cambridge, Massachusetts: The MIT Pres.
- Dilmaç, Bülent (2009). Cyber bullying: a Preliminary Report on College Students. *Kuram ve Uygulamada Eğitim Bilimleri*, 9(3). İstanbul: EDAM Yayınları.
- Dinç, Mehmet (2010). *İnternet Bağımlılığı*. İstanbul: Ferfir Yayınları.
- Dinç, Mevlüt (2012). *Ülkemizde ve Dünyada Dijital Oyunlar Sektörü Hakkında Genel Rapor*. TBMM Bilişim ve İnternet Komisyonu Sunumu.
- Dines, Gail (04.01.2011). *Porn: A Multibillion-Dollar Industry That Renders All Authentic Desire Plastic*. <http://www.guardian.co.uk/commentisfree/2011/jan/04/pornography-big-business-influence-culture?INTCMP=ILCNETTXT3487>, Erişim Tarihi: 23.12.2012.
- Doğu, A. Haydar (2012). Bilgi Toplumu Olabilmede İnternet Kafelerin Etkisi: Trabzon Örneği. *Karadeniz Teknik Üniversitesi Sosyal Bilimler Dergisi*, Sayı: 3.
- Dolu, Osman (2012). *İnternet, Teknoloji Ve Çocuklar: Sorunlara Proaktif Çözümler İçin Ulusal Bir Araştırma Önerisi*. TBMM İnternet Araştırma Komisyonu Sunumu.
- DPT (2003). *Kısa Dönem Eylem Planı (2003-2004)*. Ankara: DPT Yayınları.
- DPT (2005). *2005 Yılı Eylem Planı*. Ankara: DPT Yayınları.
- DPT (2006a). *Bilgi Toplumu Stratejisi (2006-2010)*. Ankara: DPT Yayınları.
- DPT (2006b). *Bilgi Toplumu Stratejisi Eylem Planı (2006-2010)*. Ankara: DPT Yayınları.
- DPT (2011). *Bilgi Toplumu İstatistikleri 2011*. http://www.bilgitoplumu.gov.tr/Documents/1/Yayinlar/Information_Society_Statistics_2010.pdf, Erişim Tarihi: 25.12.2012.
- DPT (2013a). *Bilgi Toplumu Stratejisinin Yenilenmesi Projesi, Bilgi Güvenliği, Kişisel Bilgilerin Korunması ve Güvenli İnternet Eksenli Mevcut Durum Raporu*.

30.05.2013, http://www.bilgitoplumustratejisi.org/tr/node/mevcut_durum_raporu, Erişim Tarihi: 13.06.2013.

DPT (2013b). *Bilgi Toplumu Stratejisinin Yenilenmesi Projesi, Bilgi Güvenliği, Kişisel Bilgilerin Korunması ve Güvenli İnternet Eksenli Küresel Egilimler ve Ülke İncelemeleri Raporu*. http://www.bilgitoplumustratejisi.org/tr/node/kuresel_egilimler_ve_ulke_incelemeleri_raporu, Erişim Tarihi: 22.05. 2013.

DPT (2013c). *Onuncu Kalkınma Planı (2014-2018)*. 06.07.2013. Ankara: DPT.

Dreyfus, Hubert L. (2002). Bilgi Otobanında Nihilizm: Günümüz Çağında Anonimlik Karşısında Bağlılık (Çev. E. Gamze Atıcı). *Cogito*. Sayı: 30.

Drezner, Daniel W. (2004). The Global Governance of the Internet: Bringing the State Back In. *Political Science Quarterly*, 119(3). New York.

Drissel, David (2006). Internet Governance in a Multipolar World: Challenging American Hegemony. *Cambridge Review of International Affairs*, 19(1). Cambridge.

Drucker, Peter (1994). *Kapitalist Ötesi Toplum*. (Çev. Belkıs Çorakçı). Ankara: İnkılap Kitabevi.

Drucker, Peter (1995). *Değişim Çağının Yönetimi*. (Çev. Zülfü Dicleli). İstanbul: Henkel Yayınları.

Dülger, M. Volkan (2004). *Bilişim Suçları*. Ankara: Seçkin Yayınları.

Dülger, M. Volkan (2007). İnternet Erişiminin Engellenmesinin Hukuksal Açıdan Değerlendirilmesi ve 5651 Sayılı Yasayla Getirilen Düzenleme. *İstanbul Barosu Dergisi*, 81(4).

Dülger, M. Volkan (2011). *Avrupa Konseyi ve Avrupa Birliği Düzenlemelerinde Çocuk Pornografisinin İnternet Aracılığıyla Yayılmasına Karşı Yapılan Düzenlemeler*. <http://www.dulger.av.tr/assets/pdf/akveabcocukpornografisi.pdf>, Erişim Tarihi: 15.08.2011.

Earlyinterventionteam (2010). *School's Out and Your Kids Are Online*. <http://earlyinterventionteam.org/wp-content/uploads/2010/07/Schools-Out-And-Your-Kids-Are-Online.pdf>, Erişim Tarihi: 11.03.2011.

Eberstadt, Mary (2010). *The Social Costsof Pornography*. http://www.winst.org/family_marriage_and_democracy/WI_SocialCosts.pdf, Erişim Tarihi: 23.04.2011.

ECHO (1996). *European Commission Working Party on Illegal and Harmful Content on the Internet Report*. <http://www.echo.lu/legal/en/internet/content/wpen.html>, Eriřim Tarihi: 12.07.2011.

Edri (2005). *Free Parental Control Software In France*. <http://www.edri.org/edrigram/number4.7/parentalsoft>, Eriřim Tarihi: 11.02.2012.

Edri (2006). *Loppsi 2 french law*. <http://www.edri.org/edrigram/number8.24/loppsi-2-french-law>, Eriřim Tarihi: 09.03.2012.

Edri (2009a). *France Wants To Filter Online Gambling Sites*. <http://www.edri.org/edrigramnumber8-19first-email-three-strikes-france/>, Eriřim Tarihi: 19.06.2012.

Edri (2009b). *Telecom Package In Second Reading – Dangerous Amendments*. <http://www.edri.org/book/export/html/1891>, Eriřim Tarihi: 07.10.2011.

Edri (2010). *First warning letters sent by French ISPs under the three strikes system*. <http://www.edri.org/edrigramnumber8-19first-email-three-strikes-france/>, Eriřim Tarihi: 19.06.2012.

Edri (2011a). *French Law Loppsi 2 Under Debate Again*. <http://www.edri.org/edrigram/number8.24/loppsi-2-french-law>, Eriřim Tarihi: 19.12.2011.

Edri (2011b). *French Decree Establishes What Data Must Be Retained By Hosting Providers*. <http://www.edri.org/edrigram/number9.5/data-retention-hosting-france>, Eriřim Tarihi: 25.06.2012.

Edri (2011c). *French ISPs Explain Why Blocking Is Wrong*. <http://www.edri.org/edrigram/number9.6/french-isps-blocking-wrong>, Eriřim Tarihi: 25.06.2012.

Edri (2011d). *French Digital Council With No Representative From Internet Users*. <http://www.edri.org/edrigram/number9.9/french-digital-council>, Eriřim Tarihi: 27.06.2012.

Edri (2012). *French Law Loppsi 2 Adopted By The General Assembly*. <http://www.edri.org/edrigram/number9.1/loppsi-2-adopted-assembly>, Eriřim Tarihi: 21.06.2012.

Edubilim (2011). *İlginç ölümler*. http://www.edubilim.com/forum/ilginc_olumler-t16219.0.html, Eriřim Tarihi: 05.09.2011.

Education (2012). *UK Council For Child Internet Safety*. <http://www.education.gov.uk/>, Eriřim tarihi: 14.05.2012.

EFA (2011). *Internet Censorship: Law & policy around the world*.
<http://www.efa.org.au/Issues/Censor/cens3.html>, Erişim Tarihi: 13.03.2011.

EFF (2004). *United States Court Of Appeals For The Ninth Circuit*.
http://w2.eff.org/legal/Jurisdiction_and_sovereignty/LICRA_v_Yahoo/20040823_yahoo_v_licra-9th.pdf, Erişim Tarihi: 08.12.2011.

Egger, O. and Rauterberg, M. (1996). *Internet Behavior and Addiction*. Swiss Federal Institute of Technology, Zurich.

Ekici, Armağan (2002). Bir Kötü Alışkanlık Olarak İnternet. *Cogito*, Sayı: 30.

Elektronik Haberleşme Sektöründe Tüketici Hakları Yönetmeliği (2010).
 T.C. Resmi Gazete, 27655, 28.07.2010.

Elektronik Haberleşme Sektöründe Tüketici Hakları Yönetmeliği (2010).
 T.C. Resmi Gazete, 27655, 28.07.2010.

Ellison, C. (04.04.2003). *New Offences To Clamp Down On Internetchild Pornography*. Minister for Justice and Customs, Press Release.

Engelliweb (2013). *Hakkında*. <http://engelliweb.com/kategoriler/>,
 Erişim Tarihi: 12.05.2013.

Engelliweb (2013a). *Kategoriler*. <http://engelliweb.com/kategoriler/>,
 Erişim Tarihi: 12.05.2013.

Erdoğan, Mustafa (2010). *Bilgi Toplumu": İyi Haber, Kötü Haber*.
<http://www.liberal-dt.org.tr/>, Erişim Tarihi: 23.12.2010.

Erdur-Baker, Özgür ve Kavşut, Fatma (2007). Akran Zorbalığının Yeni Yüzü: Siber Zorbalık. *Eğitim Araştırmaları Dergisi*, 27.

Ergene, Tuncay (2012). *İnternet ve Çocuklar, Gençler ve Aile Üzerindeki Etkileri*. TBMM Bilişim ve İnternet Komisyonu Sunumu.

Ergun,Turgay ve Polatoğlu, Aykut (1992). *Kamu Yönetimine Giriş*.Ankara:TODAİE.

Erkan, Boğaç ve Songür, Murat (1999). *Açıklamalı Bilgisayar ve İnternet Terimleri Sözlüğü*. Ankara: Hacettepe-TAŞ Yayınları.

Erkan, Hüsnü (1997). *Bilgi toplumu ve Ekonomik Gelişme* (3. Baskı). İstanbul: T. İş Bankası Kültür Yayınları.

Ersanel, Nedret (2001). *Sanal ve Dijital Casusluğun Anatomisi: Siber İstihbarat*. Ankara: ASAM Yayınları.

ESRB (2010). *Frequently asked Question*. <http://www.esrb.org/ratings/faq.jsp>, Erişim Tarihi: 12.01.2012.

Etika (2013). <http://www.etika.ru/>, Erişim Tarihi: 25.02.2013.

EU (1997). *Feasibility Of Censoring And Jamming Pornography And Racism in Informatics*.
http://ec.europa.eu/information_society/activities/sip/programme/evaluations/index_en.html, Erişim Tarihi: 23.10.2011.

EU (1999). *Action Plan on Promoting Safer Use of the Internet. Decision No 276/1999/EC of the European Parliament and of the Council of 25 January 1999*,
<http://ec.europa.eu/archives/ISPO/legal/fr/internet/actplan.html>, Erişim Tarihi: 25.03.2012.

EU (2005). *European Framework for Safer Mobile Use by Younger Teenagers and Children*.
http://ec.europa.eu/information_society/activities/sip/docs/mobile_2005/europeanframework.pdf, Erişim Tarihi: 30.11.2012.

EU (2006). <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2006-0324+0+DOC+XML+VO//EN&language=EN>, Erişim Tarihi: 25.10.2011

EU (2011a). *Digital Agenda: Coalition of top tech & media companies to make internet better place for our kids*. http://europa.eu/rapid/press-release_IP-11-1485_en.htm?locale=en, Erişim Tarihi: 01.12.2011.

EU (2011b). *Statement of Purpose of the Coalition, including its Work Plan*.
http://ec.europa.eu/information_society/activities/sip/docs/ceo_coalition/ceo_coalition_statement.pdf, Erişim Tarihi: 01.12.2011.

EU (2011c). *Programme history*.
http://ec.europa.eu/information_society/activities/sip/policy/programme/early_prog/index_en.htm, Erişim Tarihi: 27.12.2011.

EU (2011d). *Safer Internet Plus Programme 2005-2008*.
http://ec.europa.eu/information_society/activities/sip/policy/programme/prog05_08/index_en.htm, Erişim Tarihi: 27.12.2011.

EU (2011e). *Safer Internet Programme 2009-2013*.
http://ec.europa.eu/information_society/activities/sip/policy/programme/current_prog/index_en.htm, Erişim Tarihi: 27.12.2011.

EU (2011f). *Communication on Europe's Way to the Information Society, an Action Plan*. http://ec.europa.eu/information_society/index_en.htm,
Eriřim Tarihi: 11.10.2011.

EU (2011g). *Safer Internet Action Plan Extension*. http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!CELEXnumdoc&lg=EN&numdoc=32003D1151, Eriřim Tarihi: 28.10.2011.

EU Kids Online (2010). *Avrupa Çevrimiçi Çocuklar Arařtırma Projesi Türkiye Bulguları Özeti*.
http://eukidsonline.metu.edu.tr/sites/default/files/image/Eukids_TurkiyeBulgulari_TR.doc, Eriřim Tarihi: 12.10.2012.

Eur-lex (1996). <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31996F0443:EN:HTML>,
Eriřim Tarihi: 9.9.2011.

Eur-lex (1997). <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:41997X0306:EN:HTML>,
Eriřim Tarihi: 24.10.2011.

Eur-lex (2000). *Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market*. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:EN:NOT>,
Eriřim Tarihi: 18.10.2011.

Eur-lex (2003). *Council Framework Decision 2004/68/JHA*. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:013:0044:0048:EN:PDF>,
Eriřim Tarihi: 23.11.2012.

Eur-lex (2008). *Council Framework Decision 2008/913/JHA*. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32008F0913:EN:NOT>,
Eriřim Tarihi: 24.11.2012.

Eur-lex (2008a). *Turkey 2008 Progress Report*. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SEC:2008:2699:FIN:EN:PDF>,
Eriřim Tarihi: 13.11.2012.

European Parliament Temporary Committee on the ECHELON Interception System (18.05.2001). *Draft Report on the Existence of a global System for the Interception of Private and Commercial Communications (PR/439868en.doc-1/113 – PE 305.391)*. Brussel.

Evci, Özge (2010). *Facebook Gizlilik Politikası Çerçevesinde Olası Tehlikeler*. <http://hukukcu.com/modules/smartsection/item.php?itemid=205>, Erişim Tarihi: 23.12.2010.

Explore Live (2011). *Code Of Conduct*. <http://explore.live.com/code-of-conduct>, Erişim Tarihi: 10.11.2011.

Facabook (2010). *Veri Kullanımı İlkesi*. <http://www.facebook.com/policy.php>, Erişim Tarihi: 23.12.2010.

Facebook (2011). *Statement of Rights and Responsibilities*. <https://www.facebook.com/terms.php>, Erişim Tarihi: 16.9.2011.

Fallows, Deborah (2008). Few in China Complain About Internet Controls, *Pew Internet & American Life Project*, Mar. 27, 2008, <http://pewresearch.org/pubs/776/china-internet>, Erişim Tarihi: 23.12.2011.

Fallows, James (2008). *The Connection Has Been Reset*. <http://www.theatlantic.com/doc/200803/chinese-firewall>, Erişim Tarihi: 16.09.2011.

FCC (2001). *Children's Internet Protection Act*. <http://www.fcc.gov/guides/childrens-internet-protection-act>, Erişim Tarihi: 7.9.2011.

FCC (2011). *Our Work*. <http://www.fcc.gov/>, Erişim Tarihi: 13.03.2011.

Findlaw (2011). *Miller v. California*. <http://laws.findlaw.com/us/413/15.html>, Erişim Tarihi: 14.10.2011.

Firstamendment (2011). *On Second Thought... --What does the UIGEA really mean for internet gambling?*. <http://www.firstamendment.com/sitearticles/UIEGA/>, Erişim Tarihi: 08.11.2011.

Foley, C. (1999). 'Human rights and the Internet' Liberating Cyberspace: Civil Liberties. *Human Rights & The Internet*, (Der. Liberty). London: Pluto Pres.

Forum Internet (2012a). *Pourquoi le forum*. http://www.foruminternet.org/institution/institution/pourquoi-le-forum/#haut_page, Erişim Tarihi: 28.06.2012.

Forum Internet (2012b). *Tribune*. <http://www.foruminternet.org/institution/tribune/>, Erişim Tarihi: 28.06.2012.

Forum Internet (2012c). *Mediatio*. <http://www.foruminternet.org/particuliers/mediatio>, Erişim Tarihi: 28.06.2012.

- Forum Internet (2012d). *International*.
<http://www.foruminternet.org/specialistes/international/>, Erişim Tarihi: 28.06.2012.
- FOSI (2011a). *Welcome*. <http://www.fosi.org/>, Erişim Tarihi: 18.09.2011.
- FOSI (2011b). *About ICRA*. <http://www.fosi.org/icra/>, Erişim Tarihi: 18.09.2011.
- FRANCE24 (10.06.2009). *Top legal body strikes down anti-piracy law*.
<http://www.france24.com/en/20090610-top-legal-body-strikes-down-antipiracy-law-hadopi-constitutional-council-internet-france>, Erişim Tarihi: 18.06.2012).
- Freedom House (2011). *Internet Freedom 2011: Turkey*.
www.freedomhouse.org/images/File/FotN/Türkiye2011.pdf,
 Erişim Tarihi: 13.11.2012.
- Friendly Runet Foundation (2013a). *Legislation*.
<http://www.friendlyrunet.ru/legislation/116/index.phtml>, Erişim Tarihi: 25.02.2013.
- Friendly Runet Foundation (2013b). *Foundation*.
<http://www.friendlyrunet.ru/foundation/>, Erişim Tarihi: 25.02.2013.
- Friendly Runet Foundation (2013c). *Partnership*.
<http://www.friendlyrunet.ru/en/partnership/>, Erişim Tarihi: 25.02.2013
- Friendly Runet Foundation (2013d). *Hotline*. <http://www.friendlyrunet.ru/en/hotline/>
 Erişim Tarihi: 25.02.2013
- Friendly Runet Foundation (2013e). *Safety*. <http://www.friendlyrunet.ru/safety/>,
 Erişim Tarihi: 25.02.2013
- Friendly Runet Foundation (2013f). *Comops*.
<http://www.friendlyrunet.ru/charter/comops/index.phtml>, Erişim Tarihi: 25.02.2013
- FSM (2010). *Statistiken 2010*. http://www.fsm.de/de/Statistiken_2010,
 Erişim Tarihi: 16.08.2012.
- FSM (2012). http://www.fsm.de/de/Wir_ueber_uns, Erişim Tarihi: 05.04.2012.
- Fuller, Kathleen E. (2001). ICANN: The Debate Over Governing the Internet. *Duke Law & Technology Review*, Rev. 2, 14 February 2001.
- Ganesan, Arvind (2008). *Global Internet Freedom: Corporate Responsibility and the Rule of Law*. 20.05.2008, <http://hrw.org/english/docs/2008/05/20/usint18894.htm>,
 Erişim Tarihi: 17.01.2012.

Gayathri, Amrutha (2012). *Iran To Shut Down Internet Permanently; 'Clean' National Intranet In Pipeline*. 09.04.2012. <http://www.ibtimes.com/iran-shut-down-internet-permanently-clean-national-intranet-pipeline-434948>,

Erişim Tarihi: 27.02.2013.

Gazetavatan (21.02.2009).

http://www.gazetavatan.com/haberdetay.asp?detay=Erkek_sehvet_duskunu&tarikh=21.02.2009&Nesid=224366&categoryid=7, Erişim Tarihi: 13.12.2011.

Geçer, Aynur K. ve Dağ, Funda (2010). Üniversite Öğrencilerinin Bilgisayar Okur-Yazarlık Düzeylerinin Belirlenmesi: Kocaeli Üniversitesi Örneği. *Yüzüncü Yıl Üniversitesi Eğitim Fakültesi Dergisi*, VII(1), Haziran-2010.

Geist, Michael (2003). *Cyberlaw 2.0*.

<http://lawdigitalcommons.bc.edu/cgi/viewcontent.cgi?article=2227&context=bclr>, Erişim Tarihi: 25.11.2011.

Gendarmerie (2012). *Service Technique De Recherches Judiciaires Et De Documentation De La Gendarmerie/Division De Lutte Contre La Cyber Criminalité*.

<http://www.gendarmerie.interieur.gouv.fr/eng/Sites/Gendarmerie/Presentation/Criminal-investigation-department/Recherches-et-documentation-STRJD>, Erişim Tarihi: 12.03.2012.

Gesetze-im-internet.de (2002). *Jugendschutzgesetz*. <http://www.gesetze-im-internet.de/juschg/BJNR273000002.html>, Erişim Tarihi: 15.12.2011.

Gesetze-im-internet.de (2011). *Strafgesetzbuch*. <http://www.gesetze-im-internet.de/stgb/BJNR001270871.html>, Erişim Tarihi: 13.12.2011.

Giddens, Anthony (1998). *Risk Society: The Context of British Policies. The Politics of Risk Society* (Ed. J. Franklin). Oxford: Polity Pres.

Giddens, Anthony (2000). *Sosyoloji*. (Çev.Hüseyin Özel ve Cemal Güzel). Ankara: Ayraç Yayınları.

Goldenessays (2011). *Child Pornography On Internet*.

http://www.goldennessays.com/free_essays/1/alcohol-d/child-pornography-on-internet.shtml, Erişim Tarihi: 15.11.2011.

Goldsmith, Jack L. and Wu, Tim (2006). *Who Controls the Internet? Illusions of a Borderless World*. North Carolina: Oxford University Press.

Google (16.04.2013a). *Insights For Search, 2013*.

<http://www.google.com/trends/explore#q=porno&cmpt=q>, Erişim Tarihi: 16.04.2013.

Google (16.04.2013b). *Insights For Search, 2013*.
<http://www.google.com/trends/explore#q=seks&cmpt=q>, Erişim Tarihi: 16.04.2013.

Google (16.04.2013c). *Insights For Search, 2013*.
<http://www.google.com/trends/explore#cmpt=q>, Erişim Tarihi: 16.04.2013.

Google (16.04.2013d). *Insights For Search, 2013*.
<http://www.google.com/trends/explore#q=facebook%20holdem%20poker&cmpt=q>,
 Erişim Tarihi: 16.04.2013.

Google (16.04.2013e). *Insights For Search, 2013*.
<http://www.google.com/trends/explore#q=facebook%20holdem%20poker&date=1%2F2012%2012m&cmpt=q>, Erişim Tarihi: 16.04.2013.

Google (22.08.2013). *Insights For Search, 2013*.
<http://www.google.com/trends/explore#geo=TR&cmpt=q>, Erişim Tarihi: 22.08.2013.

Googleguide (2011). *Google Cached Pages: What Are Cached Pages?*.
http://www.googleguide.com/cached_pages.html, Erişim Tarihi: 24.10.2011.

Gönül, A. S. (2002). Patolojik İnternet Kullanımı, *Yeni Symposium*, 40 (3).

GPO (1996). *Communications Decency Act*.
http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=104_cong_public_laws&docid=f:publ104.104.pdf, Erişim Tarihi: 14.08.2011.

GPO (1998). *Child Online Protection Act*.
http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=104_cong_public_laws&docid=f:publ104.104.pdf, Erişim Tarihi: 14.08.2011.

Gpoaccess (2011). *United States Code*,
<http://www.gpoaccess.gov/uscode/browse.html>, Erişim Tarihi: 17.09.2011.

Guardian (02.07.2010). *The truth about the porn industry*.
<http://www.guardian.co.uk/lifeandstyle/2010/jul/02/gail-dines-pornography>, Erişim Tarihi: 24.12.2012.

Guardian (07.02.2006). *35,000 Blocks A Day On Internet Child Porn*.
<http://www.theguardian.com/technology/2006/feb/07/security.childrengovernment>,
 Erişim Tarihi: 13.12.2012.

Güvenli Çocuk (2013). <http://www.guvenlicocuk.org.tr/>, Erişim Tarihi: 21.4.2013.

Gültan, Seçkin (2009). *Toplumsal Açından Bilgi ve İletişim Çağı*. <http://inet-tr.org.tr/inetconf9/bildiri/61.doc>, Erişim Tarihi: 14.12.2009.

Günaydın, Barış (2010). *İnternet Yayıncılığı ve İfade Özgürlüğü*. Ankara:Adalet Yay.

Güneş, Abdulhamit (2012). *Dijital Oyunların Güvenlik Bağlamında Yasal ve Yönetmelik Düzenleme Sorunları*. Yüksek Lisans Tezi, Polis Akademisi Güvenlik Bilimleri Enstitüsü, Ankara.

Güngör, Müberra ve Evren, Gökhan (2002). *İnternet Sektörü ve Türkiye İncelemeleri*. Ankara:Telekomünikasyon Kurumu.

Günüç, Selim (2009). *İnternet Bağımlılık Ölçeğinin Geliştirilmesi Ve Bazı Demografik Değişkenler İle İnternet Bağımlılığı Arasındaki İlişkilerin İncelenmesi*. Yüksek Lisans Tezi, Yüzüncü Yıl Üniversitesi Sosyal Bilimler Enstitüsü, Van.

Gürkaynak, Gönenç vd. (2010). *Türk İnternet Hukuku Uygulamasının ve Mevzuatının Evriminin İlk Dönemini Tamamlaması İçin Öneriler ve Gözlemler*. www.elig.com.tr/docs, Erişim Tarihi: 12.01.2012.

Güvenliweb (2009). *Norton Online Family Report, 2009*. http://www.guvenliweb.org.tr/aileler/files/Norton_Report.pdf, Erişim Tarihi: 17.08.2011.

Güvenliweb (2012). *İnternet pornografisinin zararları*. http://www.guvenliweb.org.tr/aileler/files/internet_pornografisinin_zararlari.pdf, Erişim Tarihi: 29.05.2012.

Güvenliweb (2013). *İnternet İstatistikleri*. <http://www.guvenliweb.org.tr/istatistikler/files/erisimengellemeistatistik.pdf>, Erişim Tarihi: 27.04.2013.

GWU (2011). *Information Operations Roadmap*. http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB177/info_ops_roadmap.pdf, Erişim Tarihi: 14.12.2011.

Haber7 (01.12.2010). *Facebook üzerinden mahremiyet kavgası*. <http://www.haber7.com/haber/20100112/Facebook-uzerinden-mahremiyet-kavgasi.php>, Erişim Tarihi: 23.10.2012.

Haber7 (09.07.2009). <http://www.haber7.com/haber/20090907/Internet-hastalari-restart-edilecek.php>, Erişim Tarihi: 16.12.2012.

Haber7 (13.08.2009). *Facebook Kıskançlık Yapıyor*. <http://www.haber7.com/haber/20090813/facebook-kiskanclik-yapiyor.php>, Erişim Tarihi: 13.12.2011.

Haberrus (03.11.2012). *Google Ve Youtube'dan Rus Sansür Kurumuna Destek.* <http://haberrus.com/headline/2012/11/03/google-ve-youtubedan-rus-sansur-kurumuna-destek.html>, Erişim Tarihi: 14.02.2013.

Haberturk (19.01.2010). *Pornografik rakamlar.* <http://www.haberturk.com/ekonomi/haber/201551-Pornografik-rakamlar.aspx>. Erişim Tarihi: 12.11.2012.

Haberturk (24.06.2010). *Bakan Yıldırım YouTube'u topa tuttu.* <http://ekonomi.haberturk.com/teknoloji/haber/526278-bakan-yildirim-youtubeu-topa-tuttu>, Erişim Tarihi: 24.11.2012.

HADOPI (2012). *Haute Autorité Pour La Diffusion Des Oeuvres Et La Protection Des Droits Sur Internet.* <http://www.hadopi.fr/>, Erişim Tarihi: 01.03.2012.

Hamelink, Cees J. (1991). *Enformasyon Devriminden Sonra Yaşam Sürececek mi?. Enformasyon Devrimi Efsanesi* (Der. Yusuf Kaplan). İstanbul: Rey Yayınları.

Heise (2007). *GEMA obtains injunctions against data exchange services.* <http://www.heise.de/english/newsticker/news/83948>. Erişim Tarihi: 19.12.2011.

Helvacıoğlu, Aslı D. (2004). *Avrupa Konseyi Siber Suç Sözleşmesi-Temel Hükümlerin İncelenmesi. İnternet ve Hukuk*, Der. Yeşim M. Atamer, İstanbul: Bilgi Ünversitesi Yayınları.

Henes, Rachel (02.01.2011). *Internet porn is ruining your relationship: XXX marks the rot.* http://www.nydailynews.com/opinions/2011/01/02/2011-01-02_internet_porn_is_ruining_your_relationship_xxx_marks_the_rot.html, Erişim Tarihi: 23.04.2011.

Hernandez, Javier C. (2010). *Google Calls for Action on Web Limits.* <http://www.nytimes.com/2010/03/25/technology/25google.html?hp>, Erişim Tarihi: 23.12.2012.

Horkheimer, Max (1990). *Akıl Tutulması* (Çev. O. Koçak). İstanbul: Metis Yayınları.

Hostbul (2012). *Web hosting nedir?.* <http://www.hostbul.net/yeni-baslayanlar/36/web-hosting-nedir.aspx>, Erişim tarihi: 27.03.2012.

Howstuffworks (2011). *How Web 3.0 Will Work.* <http://computer.howstuffworks.com/web-30.htm>, Erişim Tarihi: 03.10.2011.

Huffingtonpost (18.05.2009). http://www.huffingtonpost.com/2009/05/18/google-ceo-eric-schmidt-u_n_204797.html, Erişim Tarihi: 12.12.2011.

Human Rights Watch (2005). *Country Profiles: Egypt. Nov. 2005.*
<http://www.hrw.org/reports/2005/mena1105/4.htm>, Eriřim Tarihi: 14.12.2012.

Human Rights Watch (2006). *Vietnam: Montagnards Face Religious, Political Persecution*, 14.06.2006, <http://hrw.org/english/docs/2006/06/14/vietna13542.htm>,
 Eriřim Tarihi: 14.01.2012.

Hürriyet (01.11.2012). *Rusya'da İnternette Kara Liste Uygulaması Başladı.*
<http://www.hurriyet.com.tr/teknoloji/21827352.asp>, Eriřim Tarihi: 14.02.2013.

Hürriyet (07.12.2009). *Porno sitesi bul, ödül al.*
<http://www.hurriyet.com.tr/dunya/13128121.asp?gid=200>, Eriřim Tarihi: 13.08.2012.

Hürriyet (09.02.2008). *Türkiye, 'access denied' için arada kaldı.*
<http://www.hurriyet.com.tr/ekonomi/8196257.asp>, Eriřim Tarihi: 19.07.2011.

Hürriyet (17.07. 2006). *Pedofili partisine izin.*
<http://www.hurriyet.com.tr/dunya/4768478.asp>, Eriřim Tarihi: 08.03.2013.

Hürriyet (25.12.2009).
<http://www.hurriyet.com.tr/yasasinhayat/13299492.asp?gid=245>,
 Eriřim Tarihi: 13.12.2011.

IANA (2012a). *About the Internet Assigned Numbers Authority.*
<http://www.iana.org/about/>, Eriřim Tarihi: 08.12.2012.

IANA (2012b). *Number Resources.* <http://www.iana.org/ipaddress/ip-addresses.htm>,
 Eriřim Tarihi: 09.12.2012.

IBM (2008). *Internet Security Systems X-Force® 2007 Trend Statistics.* http://www-935.ibm.com/services/us/iss/pdf/etr_xforce-2007-annual-report.pdf,
 Eriřim Tarihi: 07.04.2013.

ICANN (2007). *Publishes Revision to Proposed ICM (.XXX) Registry Agreement.*
<http://www.icann.org/en/announcements/announcement-05jan07.htm>,
 Eriřim Tarihi: 10.12.2012.

ICANN (2011a). *Top-Level Domains (gTLDs).* <http://www.icann.org/tlds/>,
 Eriřim Tarihi: 24.09.2011.

ICANN (2011b). *Factsheet.* <http://www.icann.org/en/factsheets/fact-sheet.html>,
 Eriřim Tarihi: 05.10.2011.

ICANN (2012b). *Accredited Registrars.* <http://www.icann.org/registrars/accredited-list.html>, Eriřim Tarihi: 07.12.2012.

ICANN (2012c). *Governmental Advisory Committee*. <http://gac.icann.org/>, Erişim Tarihi: 08.12.2012.

ICANN (2012d). *Bylaws For Internet Corporation For Assigned Names And Numbers*. <http://www.icann.org/general/bylaws.htm>, Erişim Tarihi: 09.12.2012.

ICEC (2013a). *Commissioners*. <http://www.icec.or.kr/eng/Commissioners.php>, Erişim Tarihi: 23.02.2013.

ICEC (2013b). *Committees*. http://www.icec.or.kr/eng/02_Operation/Committees.php, Erişim Tarihi: 23.02.2013.

Ichay&Mullenex (2004). *Practical Guide The Liability Of The Internet Hosting Server*. <http://www.ichay-mullenex.com/download/practical-guide-the-liability-of-the-internet-hosting-server.pdf>, Erişim Tarihi: 11.02.2012.

ICMEC (2012a). *Financial Coalition Against Child Pornography*. http://www.icmec.org/en_X1/pdf/FCACPBackgrounder1-13.pdf, Erişim Tarihi: 13.03.2012.

ICMEC (2012b). *About the ICMEC*. http://www.icmec.org/missingkids/servlet/PageServlet?LanguageCountry=en_X1&PageId=1222, Erişim Tarihi: 13.03.2012.

ICMEC (2012c). *Global Efforts to Expand the Financial Coalition*. http://www.icmec.org/missingkids/servlet/PageServlet?LanguageCountry=en_X1&PageId=4355, Erişim Tarihi: 14.03.2012

Ifex (16.03.2012). *The Communist Cyber-Block*. <http://www.ifex.org/en/content/view/full/68881/>, Erişim Tarihi: 30.11.2012.

Ifex (2011). *The Communist Cyber-Block*. <http://www.ifex.org/en/content/view/full/68881/>, Erişim Tarihi: 28.01.2011.

INACH (2012). *About*. <http://www.inach.net/about.html>, Erişim Tarihi: 01.04.2012.

INACH (2012). *Network*. <http://www.inach.net/network.html>, Erişim Tarihi: 04.07.2012.

INCB (2009). *Guidelines for Governments on Preventing the Illegal Sale of Internationally Controlled Substances through the Internet*. http://www.incb.org/documents/Narcotic-Drugs/Guidelines/internet/NAR_guide_Internet_guidelines_English.pdf, Erişim Tarihi: 16.03.2013.

INCP (2011). *Annual Report 2011*. http://www.incb.org/pdf/annual-report/2011/English/AR_2011_English.pdf, Erişin Tarihi: 30.02.2012.

Information Office of the State Council (2010). *The Internet in China*. http://www.china.org.cn/government/whitepaper/node_7093508.htm, Erişim Tarihi: 26.12.2012.

INHOPE (2010). *Annual Reports 2010*. http://www.inhope.org/Libraries/Annual_reports/2010_Annual_report.sflb.ashx?download=true, Erişim Tarihi: 4.7.2012.

INHOPE (2012a). *Hate Speech*. <http://www.inhope.org/gns/internet-concerns/overview-of-the-problem/hate-speech.aspx>, Erişim Tarihi: 03.07.2012.

INHOPE (2012b). *Child sexual abuse material (Child Pornography)*. <http://www.inhope.org/gns/internet-concerns/overview-of-the-problem/child-pornography.aspx>, Erişim Tarihi: 04.07.2012.

INHOPE (2012c). *Annual Reports 2012*. http://www.inhope.org/Libraries/Annual_reports/INHOPE_Annual_Report_2012.sflb.ashx, Erişim Tarihi: 23.04.2013.

INHOPE (2012d). *Internet trends*. <http://www.inhope.org/gns/internet-concerns/internet-trends.aspx>, Erişim Tarihi: 04.07.2012.

INHOPE (2013). *About INHOPE*. <https://www.inhope.org/gns/about-us/about-inhope.aspx>, Erişim Tarihi: 25.04.2013.

INSAFE (2011). *Home*. <http://www.saferinternet.org/web/guest/home>, Erişim Tarihi: 23.05.2011.

Interneshka (2013). www.interneshka.ru, Erişim Tarihi: 25.02.2013.

Internet Filter Software Review (2006). *Internet Pornography Statistics*. <http://internet-filter-review.toptenreviews.com/internet-pornography-statistics.html>, Erişim tarihi: 27.04.2012.

Internet Hotline Centre Japan (2013). *What is Harmful Information*. http://www.internethotline.jp/guideline/yugai_en.html, Erişim Tarihi: 28.02.2013.

Internet Society of China (2002). *Public Pledge of Self-Regulation and Professional Ethics for China Internet Industry*. <http://www.isc.org.cn/20020417/ca102762.htm>, Erişim Tarihi: 29.12.2011.

- Internet.sa (2013a). *Content filtering in Saudi Arabia*.
<http://www.internet.gov.sa/learn-the-web-ar/guides-ar/content-filtering-in-saudi-arabia-ar>, Erişim Tarihi: 26.02.2013.
- Internet.sa (2013b). *Resources*. <http://www.internet.gov.sa/resources-ar>,
 Erişim Tarihi: 26.02.2013.
- Internet.sa (2013c). *Learn the web*. <http://www.internet.gov.sa/learn-the-web-ar>,
 Erişim Tarihi: 26.02.2013.
- Internet.sa (2013d). *Unblock request*. <http://www.internet.gov.sa/resources-ar/block-unblock-request-ar/unblock-ar>, Erişim Tarihi: 26.02.2013.
- Internet.sa (2013e). *FAQ about filtering services*.
<http://www.internet.gov.sa/resources-ar/block-unblock-request-ar/FAQ-about-filter-service-ar/>, Erişim Tarihi: 26.02.2013.
- Internet-beschwerdestelle (2012). *Ueberuns*. <http://www.internet-beschwerdestelle.de/ueberuns/>, Erişim Tarihi: 06.04.2012.
- Internet-signalement (2012a). <https://www.internet-signalement.gouv.fr/PortailWeb/planets/Accueil!input.action>,
 Erişim Tarihi: 11.03.2012.
- Internet-signalement (2012b). *Einreichen*. <http://www.internet-beschwerdestelle.de/beschwerde/einreichen/index.htm>, Erişim Tarihi: 11.03.2012.
- Internet-signalement (2012c). *Ratgeber*. <http://www.internet-beschwerdestelle.de/ratgeber/>, Erişim Tarihi: 11.03.2012.
- Internet-signalement (2012d). *Partner*. <http://www.internet-beschwerdestelle.de/partner/>, Erişim Tarihi: 11.03.2012.
- ISC (2002). *Public Pledge of Self-Regulation and Professional Ethics for China Internet Industry*. <http://www.isc.org.cn/20020417/ca102762.htm>,
 Erişim Tarihi: 29.12.2011.
- ISFE (2011). *About*. <http://www.isafe.org/about>, Erişim Tarihi: 26.12.2011.
- ISFE (2011). *Things You Should Know*.
<http://www.isfe.eu/index.php?PHPSESSID=v32ekpdss9ubsihlq8dhm3cj86&oidit=T001:13a6822a85ec66ddd301a010aa3bca57>, Erişim Tarihi: 13.08.2011.
- ISOC (2012). *Are you an ISP? - Ambiguity in the Internet Censorship Legislation*.
<http://www.isoc-au.org.au/Regulation/PFoxBSA.html>, Erişim Tarihi: 28.05.2012.

ISPO (1996a). *Communication On Illegal And Harmful Content On The Internet*. <http://www.ispo.cec.be/legal/en/Internet/communic.html>, Eriřim Tarihi: 18.10.2011.

ISPO (1996b). *Green Paper On Protection Of Minors And Human Dignity*. <http://www.ispo.cec.be/legal/en/Internet/gpen-toc.html>, Eriřim Tarihi: 22.10.2011.

ISU (1999). *The Old User Survey Results, July – Sept. 1999*. <http://www.isu.net.sa/surveys-&-statistics/user-survey.htm>, Eriřim Tarihi: 7.11.2011.

Iřıklı, Hasibe (2001). *İnternet Alan İsimleri Sistemi*. Ankara: DPT Yayınları.

ITU (2003a). *ccTLD Doc 25 Rev.1*. <http://www.itu.int/itudoc/itu-t/workshop/cctld/025r1.pdf>, Eriřim Tarihi 10.12.2012.

ITU (2003b). *Geneva Declaration of Principles. First Phase of the WSIS, 10-12 December 2003, Geneva*, http://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0004!!MSW-E.doc, md. no. 6/48-50, Eriřim Tarihi: 23.10.2011.

ITU (2005). *Tunis Agenda for the Information Society, Second Phase of the WSIS, 16-18 November 2005, Tunis*. <http://www.itu.int/wsis/docs2/tunis/off/6rev1.doc>, Eriřim Tarihi: 27.10.2011.

ITU (2012). *The World Summit on the Information Society*. <http://www.itu.int/wsis/tunis/index.html>, Eriřim Tarihi: 11.12.2012.

ITU Cop-brochure (2009). *Child Online Protection*. <http://www.impact-alliance.org/download/pdf/resource-centre/cop/cop-brochure.pdf>, Eriřim Tarihi: 28.11.2011.

IWF (2010). *Annual Report 2010*. <http://www.iwf.org.uk/accountability/annual-reports/2010-annual-report>, Eriřim Tarihi: 07.03.2012).

IWF (2011a). *The Obscene Publications Act, Laws relating to the work of IWF*. <http://www.iwf.org.uk/police/page.22.htm>, Eriřim Tarihi: 13.10.2011.

IWF (2011b). *The Hotline and the law*. <http://www.iwf.org.uk/public/page.31.htm>, Eriřim Tarihi: 06.12.2011.

IWF (2011c). *Iwf Statement Regarding Wikipedia Webpage*. <http://www.iwf.org.uk/media/news.archive-2008.251.htm>, Eriřim Tarihi: 18.12.2011.

IWF (2012). *History*. <http://www.iwf.org.uk/about-iwf/iwf-history>, Eriřim Tarihi: 07.02.2012.

i-cozum (2011). <http://i-cozum.com/kurumsal-web-sitesi/haberler.php?op=Haber&hid=393&kid=1>, Eriřim Tarihi: 28.07.2011.

İçel, Kayıhan vd. (2000). *AB'ne Uyum Sürecinde Türk Ceza Hukuku*. İstanbul: Beta Yayınları.

İHA (09.04.2009). *Almanya'dan çocuk pornosuna önlem*. <http://www.iha.com.tr/almanya-dan-cocuk-pornosuna-onlem-65349-haber>, Erişim Tarihi: 14.05.2012.

İhbarweb (2013). *Hakkımızda*. <http://www.ihbarweb.org.tr/hakkimizda.html>, Erişim Tarihi: 25.04.2013.

İhbarweb (2013a). *Sıkça Sorulan Sorular*. <http://www.ihbarweb.org.tr/ss.html>, Erişim Tarihi: 25.04.2013.

İhbarweb (2013b). *Gizlilik Bildirimi*. <http://www.ihbarweb.org.tr/ss.html>, Erişim Tarihi: 25.04.2013.

İİKO (2012). *İstanbul İnternet Kafeciler Esnaf Odası (İİKO) Tespit ve Önerileri*. TBMM Bilişim ve İnternet Komisyonu Sunumu.

İlkiz, Fikret (2006). *Bilişimde Bilgiye Erişim*. 26.10.2006, <http://eski.bianet.org/2006/10/26/86952.htm>, Erişim Tarihi: 13.02.2013.

İnan, Aslan (1998). *İnternet El Kitabı*. İstanbul: Sistem Yayınları.

İnternet Alan Adları Yönetmeliği (2010). T.C. Resmi Gazete, 27752, 7.11.2010.

İnternet Daire Başkanlığı (2008). *2008 Yılı Faaliyet Raporu*. http://akgul.bilkent.edu.tr/Yasak/tib-08-faaliyet_raporu.pdf, Erişim Tarihi: 4.12.2012.

İnternet Geliştirme Kurulu (2013). *Üyeler*. <http://kurul.ubak.gov.tr/>, Erişim Tarihi: 24.04.2013.

İnternet Kurulu (2001a). *RTÜK Yasası Hakkında Bilişim Sivil Toplum Kuruluşları Ortak Deklarasyonu*. <http://kurul.ubak.gov.tr/m06.php>, Erişim Tarihi: 17.12.2012.

İnternet Kurulu (2001b). *RTÜK Yasası Hakkında İnternet Kurulu Üyelerinin Ortak Deklarasyonu*. <http://kurul.ubak.gov.tr/m06.php>, Erişim Tarihi: 17.12.2012.

İnternet Kurulu (2010). *29 Aralık 2010 tarihli İnternet Kurulu'nun değişiklik taslağı metni ve gerekçesi*. http://internetkurulu.org/Images/Editor/5651_mevzuat_calismasi_gerekceli_29aralik_2010.doc, Erişim Tarihi: 12.10.2012.

İnternet Kurulu (2011). *AB Bakanlığı, 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun” Hakkında İnternet Kurulu Tarafından Yapılan*

Çalışmaya İlişkin Görüş. http://Internetkurulu.org/Images/Editor/5651_sayili_Internet_kanunu_degisikligi_Internet_kurulu_hakkinda_gorus.doc, Erişim Tarihi: 07.01.2012.

İnternet Kurulu (2013). *İnternet Geliştirme Kurulu, Görüşler.* <http://www.internetkurulu.org/tr/Gorusler.aspx>, Erişim Tarihi: 24.6.2013.

İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik (2007). T.C. Resmi Gazete, 27241, 28.05.2009.

İnternet Toplu Kullanım Sağlayıcıları Hakkında Yönetmelik (2007). T.C. Resmi Gazete, 26687, 01.11.2007.

internetworldstats (2012a). *Facebook Users In The World, June 30, 2012.* <http://www.internetworldstats.com/facebook.htm>, Erişim Tarihi: 22.06.2013.

internetworldstats (2012b). *Internet Users In The World, June 30, 2012.* <http://www.internetworldstats.com/stats.htm>, Erişim Tarihi: 22.06.2013.

internetworldstats (2012c). *European Union Internet Users, June 30, 2012.* <http://www.internetworldstats.com/stats9.htm>, Erişim Tarihi: 22.06.2013.

internetworldstats (2012d). *Internet Users in the Americas, June 30, 2012.* <http://www.internetworldstats.com/stats2.htm>, Erişim Tarihi: 22.06.2013.

internetworldstats (2012e). *Internet Users in Europe, June 30, 2012.* <http://www.internetworldstats.com/stats4.htm>, Erişim Tarihi: 22.06.2013.

internetworldstats (2012f). *Internet Users in Asia 2012.* <http://www.internetworldstats.com/stats3.htm>, Erişim Tarihi: 22.06.2013.

internetworldstats (2012g). *Top 20 Internet Countries By Users-2012.* <http://www.internetworldstats.com/top20.htm>, Erişim Tarihi: 22.06.2013.

internetworldstats (2012h). *Top 20 Countries With The Highest Number Of Internet Users, 2012.* <http://www.internetworldstats.com/top20.htm>, Erişim Tarihi: 04.03.2013.

internetworldstats (2012i). *Top 50 Countries With The Highest Internet Penetration Rate, 2012.* <http://www.internetworldstats.com/top25.htm>, Erişim Tarihi: 04.03.2013.

internetworldstats (2012j). *Internet Users Europe, 2012.* <http://www.internetworldstats.com/facebook.htm>. Erişim Tarihi: 04.03.2013.

İstanbul İnternet Kafeciler Esnaf Odası (2012). *Güvenli Web Filtre Pro V3.0 TIB Projesi.* TBMM Bilişim ve İnternet Komisyonu Sunumu.

Jameson, Frederic (1997). *Marksizm ve Biçim* (Çev. M. H. Doğan). İstanbul: Yapı Kredi Yayınları.

Java (2011). *Proxy sunucu nedir? Proxy sunucusuyla ilgili bilgileri nasıl elde edebilirim?*. http://www.java.com/tr/download/help/proxy_server.xml, Erişim Tarihi: 14.11.2011.

Jugendschutz (2007). *Effectively Combating Hate on the Internet*. http://www.jugendschutz.net/pdf/report_cyberhate_2007.pdf, Erişim Tarihi: 28.02.2013.

Jugendschutz (2012a). *Beschwerdeverfahren*. <http://www.jugendschutz.net/hotline/beschwerdeverfahren/index.html>, Erişim Tarihi: 25.03.2012.

Jugendschutz (2012b). *Rechtsextremismus*. <http://www.jugendschutz.net/rechtsextremismus/index.html>, Erişim Tarihi: 2.4.2012.

Jugendschutzlandesstellen (2012). *Gesetze*. http://www.jugendschutzlandesstellen.de/jugendschutz_sucht_medien_gewalt.html#gesetze, Erişim Tarihi: 01.04.2012.

Jugendschutzlandesstellen.de (2012). http://www.jugendschutzlandesstellen.de/jugendschutz_sucht_medien_gewalt.html#gesetze, Erişim Tarihi: 01.04.2012.

Kangal, Zeynel T. (2001). *Fransa'da İnternet Yoluyla İşlenen Suçlardan Doğan Ceza Sorumluluğu*. <http://www.iudergi.com/tr/index.php/hukukmecnua/article/view/4181/3775>, Erişim Tarihi: 26.07.2012.

Karaca, Nihal B. (27.06.2010). *Porno ile Özgürlük Savunusu Yapmak*. <http://www.haberturk.com/yazarlar/527072-porno-ile-ozgurluk-savunusu-yapmak>, Erişim Tarihi: 21.04.2011.

Kaya, M. Bedii (2009). *Türk Hukukunda ve Mukayeseli Hukukta İnternet Erişiminin Engellenmesi*. Yüksek Lisans Tezi, İstanbul Bilgi Ün. Sosyal Bilimler Enstitüsü.

Kaya, M. Bedii (2010). *Teknik ve Hukuki Boyurlarıyla İnternet Erişiminin Engellenmesi*. İstanbul: On İki Levha Yayınları.

Kayri, Murat ve Günüş, Selim (2009). İnternet Bağımlılık Ölçeğinin Türkçeye Uyarlanması: Geçerlik Ve Güvenirlik Çalışması. *Ankara University, Journal of Faculty of Educational Sciences*, Sayı 42.

KCSC (2013). *Overview*. <http://www.safenet.ne.kr/rsys.do>, Erişim Tarihi: 25.2.2013.

Kelleci, Meral (2008). İnternet, Cep Telefonu, Bilgisayar Oyunlarının Çocuk Ve Gençlerin Ruh Sağlığına Etkileri. *TAF Preventive Medicine Bulletin*, 7(3).
http://www.scopemed.org/mnstemps/1/khb_007_03-253.pdf, Erişim Tarihi:2.9.2011.

Kff (30.11.2002). *2002 National Survey of Latinos*.<http://kff.org/disparities-policy/poll-finding/2002-national-survey-of-latinos/>, Erişim Tarihi: 11.03.2011.

Kiremitci, Ümmügül (2012). *İnternetin Gelişimi İle Birlikte Ortaya Çıkan Sorunlar Ve İnternetin Düzenlenmesine Yönelik 5651 Sayılı Yasanın Getirdiği Önlemler, Uygulama Sorunları Ve Çözüm Önerileri*. İletişim Uzmanlığı Tezi. Bilgi Teknolojileri Ve İletişim Kurumu. Ankara.

Kjm-online (2002). *Jugendmedienschutz-Staatsvertrag-JMStV*. http://www.kjm-online.de/files/pdf1/_JMStV_Stand_13_RStV_mit_Titel_deutsch3.pdf, Erişim Tarihi: 12.05.2012.

Kjm-online (2012a). *Kommission Für Jugendmedienschutz Landesmedienanstalten*, http://www.kjm-online.de/de/pub/recht/gesetze_und_staatsvertraege/jugendmedienschutz-staatsvertr.cfm, Erişim Tarihi: 23.02.2012.

Kjm-online (2012b). *İnternet*. http://www.kjm-online.de/de/pub/die_kjm/institutionen-wegweiser/internet.cfm, Erişim Tarihi: 23.02.2012.

Kjm-online (2012c). *Auftrag*. http://www.kjm-online.de/de/pub/die_kjm/auftrag.cfm, Erişim Tarihi: 23.02.2012.

Kjm-online (2012d). *Stabsstelle*. http://www.kjm-online.de/de/pub/die_kjm/organisation/stabsstelle.cfm, Erişim Tarihi: 23.02.2012.

Kjm-online (2012e). *Jugendschutzprogramme*. http://www.kjm-online.de/de/pub/jugendschutz_in_telemedien/jugendschutzprogramme.cfm, Erişim Tarihi: 23.02.2012.

Kjm-online (2012f). *Jugendschutznet*. http://www.kjm-online.de/de/pub/die_kjm/organisation/jugendschutznet.cfm, Erişim Tarihi: 23.02.2012.

Kjm-online (2012g). *Aufgaben*. http://www.kjm-online.de/de/pub/die_kjm/aufgaben.cfm, Erişim Tarihi: 24.02.2012.

Kocacık, Faruk (2003). Bilgi Toplumu ve Türkiye. *Cumhuriyet Üniversitesi Sosyal Bilimler Dergisi*, Cilt : 27. No:1

Koç, Serhat (2013). *Hukuksal Bağlamda Sosyal Medya Analizi Ve Kıyaslamalı Mevzuat Önerileri*. Yüksek Lisans Tezi. İstanbul Üniv. Sosyal Bilimler Enstitüsü.

Kongar, Emre (2001). *Küresel Terör ve Türkiye*. İstanbul: Remzi Kitabevi.

Korkmaz, Fahrettin (2010). *Birçok AB Ülkesi İnternet İçeriğine Türkiye'den Daha Fazla Müdahale Ediyor*. www.sentezhaber.com/bircok-ab-ulkesi-internet-icerigine-turkiyeden-daha-fazla-mudahale-ediyor.htm, Erişim Tarihi: 25.11.2011.

Kozanoğlu, Can (1997). *İnternet Dolunay Cemaat*. İstanbul: İletişim Yayınları.

Köksal, Ahmet T. vd. (1999). *Kim Korkar Bilgisayardan? İnternet*, İstanbul: Pusula Yayınları.

Köse, Güven ve Özen, Kerem (2010). *İnternet'te Sansür Üzerine Bir Değerlendirme*. http://www.bby.hacettepe.edu.tr/e-bulten/dosyalar/file/kose_ozen_by2010.pdf, Erişim Tarihi: 16.09.2011.

Kraut, R. vd. (1998). Internet Paradox, A Social Technology That Reduces Social Involvement and Psychological Well-being? *Am. Psychol.* 53(9).

KTCF (2013). *KT Cultural Foundation*. <http://www.ktcf.or.kr>, Erişim Tarihi: 25.02.2013.

Kumar, Krishan (1999). *Sanayi Sonrası Toplumdan Postmodern Topluma Çağdaş Dünyanın Yeni Kuramları*. (Çev. Mehmet Küçük). Ankara: Dost Yayınları.

LACNIC (2012). *Latin American and Caribbean Internet Adresses Registry*. <http://lacnic.net/>, Erişim Tarihi: 08.12.2012.

Laquadrature (2012). *Rapprochement Arcep - CSA : le gouvernement sur le chemin de la censure du Net ?*. <http://www.laquadrature.net/fr/rapprochement-arcep-csa-le-gouvernement-sur-le-chemin-de-la-censure-du-net>, Erişim Tarihi: 11.03.2012.

Laudon C., Kenneth & Laudon, P. Jane (1996). *Management Information Systems: Organization and Technology – 4th Edition*. Prentice Hall.

Legifrance (1994). *Nouveau Code Penal*. http://www.legifrance.gouv.fr/affichCode.do;jsessionid=D138FDF0921ED45CE9D4CDFD8FD84711.tpdjo11v_1?idSectionTA=LEGISCTA000006165321&cidTexte=LEGITEXT000006070719&dateTexte=19980617, Erişim Tarihi: 14.06.2012.

Legifrance (2003). *Décret n° 2003-1168 du 8 décembre 2003 portant création d'une délégation aux usages de l'internet*. <http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000431423>, Erişim Tarihi: 14.06.2012.

Legifrance (2004a). *Pour La Confiance Dans L'économie Numérique*.
http://www.legifrance.gouv.fr/affichTexte.do;jsessionid=BC2216B27CC06FF301B6F6174C4A30B5.tpdjo09v_2?cidTexte=JORFTEXT000000801164&dateTexte=20120527, Erişim Tarihi: 12.04.2012.

Legifrance (2004b).
http://www.legifrance.gouv.fr/affichTexte.do;jsessionid=035001C634A6EC1391D68FA4420BCB37.tpdjo13v_1?cidTexte=JORFTEXT000000441676&dateTexte=20040807, Erişim Tarihi: 29.06.2012.

Legifrance (2006). *Loi Sur Le Droit D'auteur Et Les Droits Voisins Dans La Société De L'information*.
<http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000266350>, Erişim Tarihi: 14.06.2012.

Legifrance (2009a). *Favorisant La Diffusion Et La Protection De La Création Sur Internet*.
<http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000020735432&fastPos=3&fastReqId=1896908772&categorieLien=id&oldAction=rechTexte>, Erişim Tarihi: 14.06.2012.

Legifrance (2009b).
http://legifrance.gouv.fr/affichTexte.do;jsessionid=D46B4A842F8F25C2AD05814838C41B48.tpdjo02v_3?cidTexte=JORFTEXT000021573619&dateTexte=20100104, Erişim Tarihi: 14.06.2012.

Legifrance (2010). *La Régulation du Secteur des Jeux D'argent et de Hasard en Ligne*.
http://legifrance.gouv.fr/affichTexte.do;jsessionid=FD2B6B56BCE38CDDD41AC9DBD36F1249.tpdjo11v_3?cidTexte=JORFTEXT000022204510&categorieLien=id, Erişim Tarihi: 14.06.2012.

Legifrance (2011a). *Programmation Pour La Performance De La Sécurité Intérieure*.
<http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000023707312&fastPos=1&fastReqId=1447818568&categorieLien=id&oldAction=rechTexte>, Erişim Tarihi: 14.06.2012.

Legifrance (2011b). *Décision no 2011-625 DC du 10 Mars 2011*.
http://www.legifrance.gouv.fr/affichTexte.do;jsessionid=702CE410441A2747B4363F7890374650.tpdjo15v_1&dateTexte=?cidTexte=JORFTEXT000023708024&categorieLien=cid, Erişim Tarihi: 21.06.2012.

Legifrance (2011c).
<http://www.legifrance.gouv.fr/affichTexte.do;jsessionid=?cidTexte=JORFTEXT000023646013&dateTexte=?&oldAction=rechJO&categorieLien=id>, Erişim Tarihi: 25.06.2012.

- Legislation (2010). *Digital Economy Act*.
<http://www.legislation.gov.uk/ukpga/2010/24>, Eriřim Tarihi: 15.02.2012.
- Lemos, Robert (2007). *Tor Hack Proposed To Catch Criminals*. *Securityfocus*. 8 Mar. 2007, <http://www.securityfocus.com/news/11447>, Eriřim Tarihi: 12.11.2011.
- Lessig, Lawrence (1998). *The Architecture of Privacy*. *Taiwan Net '98 Conference, Taipei, March, 1998*. http://cyber.law.harvard.edu/works/lessig/architecture_priv.pdf, Eriřim Tarihi: 11.12.2012.
- Lessig, Lawrence (2003). *Internet and Censorship in Germany*.
<http://odem.org/material/internet-censorship-germany.pdf>, Eriřim Tarihi: 18.09.2011.
- LINX Public Affairs (2006). *Government sets deadline for universal network-level content blocking*. <https://publicaffairs.linx.net/news/?p=497>, Eriřim Tarihi: 14.05.2012.
- LOC (1997). *Internet Gambling Prohibition Act*.
<ftp://ftp.loc.gov/pub/thomas/c105/s474.is.txt>, Eriřim Tarihi: 17.09.2011.
- LSE (2009). *EU Kids Online II*.[http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/EUKidsII%20\(2009-11\)/home.aspx](http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/EUKidsII%20(2009-11)/home.aspx), Eriřim Tarihi: 05.12.2010.
- Lyon, David and Höller, Christian (22.05.1997). *Surveillance Systems-Towards an Electronic Panoptical Society?*. <http://www.heise.de/tp/artikel/8/8026/1.html>, Eriřim Tarihi: 12.11.2010.
- Marin, Mehmet C. (2010). *Elektronik Küresel Mekanlar, Tele-Koloniler Ve Türkiye'deki Kentler*. http://www.bilgiyonetimi.org/cm/pages/mkl_gos.php?nt=516, Eriřim Tarihi: 24.12.2010.
- Marketing Türkiye (2012). *Gençler Medyayı Nasıl Tüketiyor*. 15.05.2012.
- Marzouki, Meryem (2006). *Combating Racism on the Internet while Upholding International Human Rights Standards*.
<http://www.polytic.lip6.fr/spip.php?article127>, Eriřim Tarihi: 16.01.2012.
- Mashable (2007). *Censored: List of Countries that Banned YouTube*.
<http://mashable.com/2007/05/30/youtube-bans/>, Eriřim Tarihi: 11.12.2011.
- Mason, Richard (1986). Four Ethical Issues of Information Age. *Management Information Systems Quarterly*, 10.
- Masuda, Yoneji (1990). *Managing In The Information Society*.
 Oxford: Basil Blackwell

Mattelart, Armand (2004). *Bilgi Toplumunun Tarihi* (Çev. H.Y. Altınel). İstanbul: İletişim Yayınları.

McAfee (2010). *The Secret Online Lives of Teens, 2010*.
http://promos.mcafee.com/en-US/PDF/lives_of_teen.pdf, Erişim Tarihi: 06.04.2012.

McGinnis, E. (2011). *The Horrifying Reality of Sex Trafficking*.
www.beverlylahayeinstitute.org, Erişim Tarihi: 12.08.2011.

MDA (1997). *Internet Code of Practice*.
http://www.mda.gov.sg/Documents/PDF/licences/mobj.981.Internet_Code_of_Practice.pdf, Erişim Tarihi: 21.02.2013.

MDA (2004). *Class Licence Notification*.
http://www.mda.gov.sg/Documents/PDF/licences/mobj.487.ClassLicence.pdf, Erişim Tarihi: 21.02.2013.

MDA (2013a). *Board of Directors*.
http://www.mda.gov.sg/AboutUs/Pages/BoardofDirectors.aspx, Erişim Tarihi: 22.02.2013.

MDA (2013b). *Consultation with Committees*.
http://www.mda.gov.sg/AboutUs/Overview/Pages/ConsultationwithCommittees.aspx Erişim Tarihi: 22.02.2013.

MEB (2008). *İnternet Kafelerin Öğrenciler Üzerindeki Etkisi*. Ankara: Eğitimi Araştırma ve Geliştirme Dairesi Başkanlığı Yayınları.

MEB ve RTÜK (2006). *İlköğretim Medya Okuryazarlığı Dersi Öğretim Programı ve Klavuzu*. http://www.medyakuryazarligi.org.tr/documents/program.pdf, Erişim Tarihi: 03.07.2012.

MEB-EĞİTEK (2008). *Eğitim Sisteminde İnternet ve Bilgisayar Oyunlarına Yönelik Çalışmalar, Konuyla İlgili Görüş ve Öneriler*. http://egitek.meb.gov.tr/, Erişim Tarihi: 09.12.2010.

Medyahayat, http://www.medyahayat.com/haber.php?haber_id=7216.
Erişim Tarihi: 13.11.2010)

Medyatava (09.02.2010). http://medyatava.com/haber.asp?id=62091.
Erişim Tarihi: 11.09.2012

Megatrends, J. Naisbitt (1984). *Ten New Directions Transforming Our Lives*. N.York.

Meldkindersekstoerisme (2013). http://www.meldkindersekstoerisme.nl/, Erişim Tarihi: 12.01.2013.

Meldknop.nl (2013). *Ets vervelends gebeurd op Internet?*. <http://www.meldknop.nl/>, Eriřim Tarihi: 22.02.2013.

Meldpunt-kinderporno (2013a). *Criteria*. http://www.meldpunt-kinderporno.nl/dropdownmenu__criteria.htm, Eriřim Tarihi: 22.02.2013.

Meldpunt-kinderporno (2013b). *Vraag en antwoord*. http://www.meldpunt-kinderporno.nl/dropdownmenu__criteria.htm, Eriřim Tarihi: 22.02.2013.

Milliyet (08.04.2012). *Muzır Kurulu artıřtan řikayetçi*. <http://siyaset.milliyet.com.tr/muzir-kurulu-artistan-sikayetci/siyaset/siyasetdetay/08.04.2012/1525508/default.htm>, Eriřim Tarihi: 06.11.2012.

Milliyet (10.09.2012). *Çocuk Pornosu Yasallařsın*. <http://www.milliyet.com.tr/Yazdir.aspx?aType=HaberDetayPrint&ArticleID=1594359>, Eriřim Tarihi: 08.03.2013.

Minkomsvjaz (2003). *The Law on Communications*. <http://minkomsvjaz.ru/5878/7687.shtml>, Eriřim Tarihi: 25.02.2013.

Missing Children Europe (2012). *European Financial Coalition*. http://www.missingchildreneurope.eu/index.php?option=com_content&view=article&id=70&Itemid=57, Eriřim Tarihi: 14.03.2012

Missingkids (2012a). *Our History*. <http://www.missingkids.com/History>, Eriřim Tarihi: 18.07.2012.

Missingkids (2012b). *Cybertipline*. <http://www.missingkids.com/cybertipline/>, Eriřim Tarihi: 14.03.2012.

Missingkids (2012c). *About us*. <http://www.missingkids.com/cybertipline/>, Eriřim Tarihi: 14.03.2012.

Missingkids (2012d). *Child Victim Program*. <http://www.missingkids.com/CVIP>, Eriřim Tarihi: 14.03.2012.

Missingkids (2012e). *Exploitation*. <http://www.missingkids.com/Exploitation>, Eriřim Tarihi: 14.03.2012.

Missingkids (2012f). *Voluntary Industry Initiatives*. <http://www.missingkids.com/Industry>, Eriřim Tarihi: 14.03.2012.

Mutlu Çocuklar Derneęi (2011). *Çocuklarda İletişim Araçları Baęımlılıęı Anket Çalışması Teknik Raporu*. Ankara.

Narkomanam (2013). <http://www.narkomanam.net/>, Erişim Tarihi: 25.02.2013.

Nebil, Füsün S. (2008). *TİD; 5651 ile İlk Defa Anayasal Bir Özgürlük olan 'Haberleşme Özgürlüğü' Bir İdari Birimin Kararına Bırakılıyor -2*. 29.08.2008, <http://turk.internet.com/haber/yazigoster.php3?yaziid=21811>, Erişim Tarihi: 13.10.2012.

Nebil, Füsün S. (2008a). *Müyap Kapatmalarındaki Kötü Alışkanlık, 5651 Dışı Site Erişim Kapatmalarında Kural Haline Dönüşmüş-1*. 06.05.2008, <http://turk.internet.com/haber/yazigoster.php3?yaziid=20882>, Erişim Tarihi: 14.02.2013.

Nebil, Füsün S. (2009). *TİB İnternet Dairesi Başkanı Osman N. Şen İnternet Alanında Türkiye ve Dünya'da Yaşanan Gelişmeleri Değerlendirdi*. <http://www.turk.internet.com/portal/yazigoster.php?yaziid=23114>, Erişim Tarihi: 17.02.2012.

Nebil, Füsün S. (2013). *ICANN Yönetim Merkezlerini 3'e Çıkartıyor, Birisi İstanbul Olacak*. 25.06.2013. <http://www.turk-internet.com/portal/yazigoster.php?yaziid=41991>, Erişim Tarihi: 25.06.2013.

Nedopusti (2013). <http://www.nedopusti.ru/>, Erişim Tarihi: 25.02.2013.

Netcraft (2013). *August 2013 Web Server Survey*. <http://news.netcraft.com/archives/category/web-server-survey/>, Erişim Tarihi: 01.05.2013.

Netica (2013). <http://new.netica.org.br/>, Erişim Tarihi: 28.02.2013.

Netsmartz (2012). About us. www.netsmartz.org, Erişim Tarihi: 18.07.2012.

News.xinhuanet (2005). http://news.xinhuanet.com/politics/2005-09/25/content_3538899.htm, Erişim Tarihi: 23.05.2012.

Nohutçu, Ahmet ve Balcı, Asım (2008). Kamu Yönetiminin Yeni Perspektif ve Dinamizmi: 'Kamu'nun Yönetilmesinden 'Kamu'nun Yönetmesi Anlayışına Doğru'. (Ed. Asım Balcı ve diğerleri). *Kamu Yönetiminde Çağdaş Yaklaşımlar*. (2. Baskı). Ankara: Seçkin Yayıncılık.

NTİA (2011). *About*. <http://www.ntia.doc.gov/>, Erişim Tarihi: 13.03.2011.

NTVMSNBC (28.03.2011). *Yüz Kızartan Tablo*. <http://www.ntvmsnbc.com/id/25196929/#storyContinued>, Erişim Tarihi: 11.09.2012.

NTVMSNBC (4.12.2009). *ABD'de 10 Gençten 8'i Oyun Oynuyor*. <http://www.ntvmsnbc.com/id/25028091/>, Erişim Tarihi: 23.12.2011.

Numerama (2010). *Les Fai Condamnés À Bloquer Un Site De Pari En Ligne, Par Dpi Si Besoin*. <http://www.numerama.com/magazine/16434-les-fai-condamnes-a-bloquer-un-site-de-pari-en-ligne-par-dpi-si-besoin.html>, Erişim Tarihi: 08.06.2012.

Numerama (2012). *C'est Officiel: Matignon Associe Hadopi, Csa Et Arcep Pour Réguler Le Net !*. <http://www.numerama.com/magazine/23465-c-est-officiel-matignon-associe-hadopi-csa-et-arcep-pour-reguler-le-net.html>, Erişim Tarihi: 11.03.2012.

O'Connell, Rachel (1999). *Untangling the Complexities of Combating Paedophile Activities in Cyberspace. COPINE Project*, Department of Applied Psychology, University College Cork, Ireland. <http://copine.ucc.ie/>, Erişim Tarihi: 27.04.2012.

O'Toole, Kathleen (2000). *Study offers early look at how Internet is changing daily life, Stanford News*. <http://news.stanford.edu/news/2000/february16/internetsurvey-216.html>, Erişim Tarihi: 24.11.2011.

Ocak, M. Akif (2012). Bağımlılığın Yeni Adı: İnternet Kumarı Ve Çocuk Pornografisi. *Yeşilay Dergisi*, Sayı: 942.

Odabaşı, H. Ferhan (2002). *İnternet ve Çocuk*. İstanbul: Kapital Medya Yayınları.

Odabaşı, H. Ferhan ve vd. (2007). *İnternet, Çocuk ve Aile*. Ankara: Nobel.

ODTÜ (2013). *Yurdum İnternet'i 10 Yaşında*. <http://www.internetarsivi.metu.edu.tr/10yil.php>, Erişim Tarihi: 04.03.2013.

OECD (02.05.2011). *The Protection of Children Online*. <http://www.oecd-ilibrary.org/docserver/download/5kgcjf71pl28.pdf?expires=1376920077&id=id&accname=guest&checksum=21FA30216EFD35829D786D5EAE8069B2>, Erişim Tarihi: 03.10.2012.

Ofcom (2012). *About*. <http://www.ofcom.org.uk/about/>, Erişim Tarihi: 23.03.2012.

Office For Internetsafety (10.02.2009). *European Commission Announces Agreement With Major Social Networking/Web Companies*. <http://www.internetsafety.ie/website/ois/oisweb.nsf/page/DPCY-7P5N4N178910-en>, Erişim Tarihi: 30.11.2012.

Oğuz, Sefer (2008). Telif Hakkı İhlallerinden İnternet Servis Sağlayıcıların Sorumlulukları. *Gazi Üniversitesi Hukuk Fakültesi Dergisi*, XII(1-2). Ankara. http://www.hukuk.gazi.edu.tr/editor/dergi/12_7.pdf, Erişim Tarihi: 18.07.2012.

Oktay, Batur and Wrenn, Greg (1999). *A Look Back at the Notice-Takedown Provision of the US Digital Millenium Copyright Act One Year After Enactment*.

www.wipo.int/edocs/mdocs/mdocs/en/osp_lia/osp_lia_2.doc,
Eriřim Tarihi: 15.12.2011.

Okday, Tuncer (2012). *İnternet Bağımlılığı*. TBMM Biliřim ve İnternet Komisyonu Sunumu.

Onecl (2011). *Crimes and Criminal Procedure - 18 USC Section 2256*.
<http://law.onecl.com/uscode/18/2256.html>, Eriřim Tarihi: 23.11.2011.

OpenNet (06.08.2009). *Saudi Arabia*. <http://opennet.net/research/profiles/saudi-arabia>, Eriřim Tarihi: 24.09.2012.

OpenNet (06.08.2012). *South Korea*. <http://opennet.net/research/profiles/south-korea>, Eriřim Tarihi: 23.02.2013.

OpenNet (07.08.2009a). *United Arab Emirates*.
<http://opennet.net/research/profiles/uae>, Eriřim Tarihi: 04.10.2012.

OpenNet (07.08.2009b). *Tunisia*. <http://opennet.net/research/profiles/tunisia>,
Eriřim Tarihi: 23.11.2011.

OpenNet (07.08.2012). *Vietnam*. <http://opennet.net/research/profiles/vietnam>,
Eriřim Tarihi: 14.12.2012.

OpenNet (09.08.2012a). *China*. <http://opennet.net/research/profiles/china>,
Eriřim Tarihi: 24.09.2012.

OpenNet (09.08.2012b) *India*. <http://opennet.net/research/profiles/india>,
Eriřim Tarihi: 07.02.2013.

OpenNet (10.05.2007). *Pakistan*. <http://opennet.net/research/profiles/pakistan>,
Eriřim Tarihi: 18.01.2012.

OpenNet (13.11.2012). *Turkey*. <http://opennet.net/countries/turkey>,
Eriřim Tarihi: 13.11.2012.

OpenNet (16.06.2009). *Iran*. <http://opennet.net/research/profiles/iran>,
Eriřim Tarihi: 24.09.2012.

OpenNet (2004). *Internet Filtering In Saudi Arabia In 2004*.
<http://opennet.net/studies/saudi#toc4b>, Eriřim Tarihi: 16.01.2012.

OpenNet (2006-2007a). *United State and Canada*.
<http://opennet.net/research/regions/namerica>, Eriřim Tarihi: 13.09.2011.

OpenNet (2006-2007b). *Internet Filtering in Europe 2006-2007*.
<http://opennet.net/studies/europe2007>, Erişim Tarihi: 12.03.2012.

OpenNet (2010). *Europe*.
http://opennet.net/sites/opennet.net/files/ONI_Europe_2010.pdf,
 Erişim Tarihi: 07.02.2013.

OpenNet (24. 03.2009). *Google Confirms YouTube Blocked in China*.
<http://opennet.net/blog/2009/03/google-confirms-youtube-blocked-china>,
 Erişim Tarihi: 09.01.2012.

OpenNet (30.08.2004). *Google Search & Cache Filtering Behind China's Great Firewall*. <http://opennet.net/bulletins/006>. Erişim Tarihi: 30.11.2011.

OPSI (2003). *Sex Offences Act 2003*.
http://www.opsi.gov.uk/Acts/acts2003/plain/ukpga_20030042_en,
 Erişim Tarihi: 13.10.2011.

OPSI (2008). *Criminal Justice And Immigration Act 2008*.
http://www.opsi.gov.uk/acts/acts2008/plain/ukpga_20080004_en,
 Erişim Tarihi: 13.10.2011.

Optenet (2010). *Press Releases*. <http://www.optenet.com/en-us/new.asp?id=270>,
 Erişim Tarihi: 27.04.2012.

Orwell, George (1985). *Bindokuzyüzseksendört* (Çev. H. Derin).
 Ankara: Kültür Bakanlığı Yayınları.

Öktem, Ferhunde vd. (2006). *Çocuklar ve Gençlerin Televizyonun Zararlı İçeriklerinden Korunması: "Akıllı İşaretler Sınıflandırma Sistemi" Akademik Çalışma Altyapısı*.
http://www.rtuk.org.tr/sayfalar/IcerikGoster.aspx?icerik_id=c1837d83-9ec8-43c3-9cce-2e23e933f151, Erişim Tarihi: 25.04.2013.

Öngören, Gürsel (2006). *İnternet Hukuku*. İstanbul: Öngören Hukuk Yayınları.

Öngören, Habibe (2005). *Küresel Kültürün Kimlik Dönüşümüne Etkileri: Üniversiteli Gençler Araştırması*. Doktora Tezi, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü.

Özbek, Veli Ö. (2009). *Müstehcenlik Suçu*. Ankara: Seçkin Yayınları.

Özbey, G. Gülay (2011). *Yer Sağlayıcılığı Kavramı; Dünya'daki ve Türkiye'deki Durumu, Türkiye'deki Yer Sağlayıcıların Hukuki, Teknik ve İdari Sorunları ve İyileştirmeye Yönelik Çözüm Önerileri*. İletişim Uzmanlığı Tezi, Bilgi Teknolojileri Ve İletişim Kurumu. Ankara.

Özcan, Mehmet (05.10.2006). *Siber Terörizm ve Ulusal Güvenliğe Tehdit Boyutu*. <http://www.turkishweekly.net/turkce/makale.php?id=87>, Erişim Tarihi: 25.11.2011.

Özdemir, Cüneyt (16.01.2011). *Porno İzlememe Özgürlüğü*. <http://www.radikal.com.tr/Radikal.aspx?aType=RadikalHaberDetayV3&ArticleID=1036681&Date=15.04.2011&CategoryID=97>, Erişim Tarihi: 15.07.2012.

Özdilek, Ali Osman (2002). *İnternet ve Hukuk*. İstanbul: Papatya Yayınları.

Özel, Cevat (2006). *Müstehcenlik Kavramı*. <http://www.hukukcu.com/bilimsel/kitaplar/mustehcenlik.htm>, Erişim Tarihi: 08.03.2013.

Özel, Cevat (2007). *5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlarlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun Hakkında Düşünceler*. http://www.turkhukuksitesi.com/makale_626.htm, Erişim Tarihi: 17.03.2013.

Özkanlı, Ahmet ve Özkanlı, Çağlar (2006). Çocuğa Yönelik İstismarda Farklı Bir Boyut: Çocuk Pornografisi. *Polis Bilimleri Dergisi*, 8(1).

Özmen, Özkan (2009). *Uyuşturucu Veya Uyarıcı Madde Suçları*. Yüksek Lisans Tezi, Bahçeşehir Üniversitesi, İstanbul.

Özsoy, Osman (2010). *İnternetin Kararttığı Hayatlar*. İstanbul: Pozitif Yayınları.

Paçacı, K.Kaya vd. (2011). *Düzenleyici Kurumların Sayısal Yayıncılıkta Rolü*. BTK, Ankara. http://www.tk.gov.tr/kutuphane_ve_veribankasi/raporlar/arastirma_raporlari/dosyalar/Duzenleyici_Kurumlarin_Sayisal_Yayincilikta_Rolu.pdf, Erişim Tarihi: 11.04.2013.

Par, Kübra (16.9.2013). *İşte Türkiye'nin en çok porno arayan 3 ili!*, O. Nihat Şen ile Röportaj, <http://ekonomi.haberturk.com/teknoloji/haber/877995-iste-turkiyenin-en-cok-porno-arayan-3-ili>, Erişim Tarihi: 16.9.2013.

Passe ton permis (2012). <http://www.passe-ton-permis-web.com/>, Erişim Tarihi: 11.02.2012.

Paul, P. (19.01.2004). The Porn Factor. *TIME Magazine*.

Peake, Adam (2004). *Internet Governance and the World Summit on the Information Society (WSIS)*. <http://www.apc.org/fr/system/files/governance.pdf>, Erişim Tarihi: 10.12.2012.

PEGI (2012). *About PEGI*. <http://www.pegi.info/en/index/id/23>, Erişim Tarihi: 23.01.2012.

Pekşirin, Hülya (2001). *İnternetin Yasal Düzenlemesi. İnternet Kurulu.*
<http://kurul.ubak.gov.tr/m06.php>, Erişim Tarihi: 17.12.2012.

Pekşirin, Hülya vd. (2012). *İnternet Yayıncılığı ve İnternet Servis Sağlayıcılarının Sorumlulukları, Genel Politikalar ve Düzenleme Önerileri.*
<http://www.teknoturk.org/docking/yazilar/tt000086-yazi.htm>,
 Erişim Tarihi: 24.01.2012.

Pingvinov (2007). *Lawlessness in Ru.net, Kiberpolitseyskie Closes Sports Web Sites.*
<http://pingvinov.net/2007/09/25/Bespredel-v-Runete-Kiberpoliceiskie-zakryvajut-sportivnye-saity.html>, Erişim Tarihi: 12.4.2011.

Planalto (2013a). *Estatuto da Criança e do Adolescente.*
http://www.planalto.gov.br/ccivil_03/leis/18069.htm, Erişim Tarihi: 28.02.2013.

Planalto (2013b). *Constituição Da República Federativa Do Brasil De 1988.*
http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm, Erişim Tarihi: 28.02.2013.

Planalto (2013c). *Crimes Resultantes De Preconceitos De Raça Ou De Cor.*
http://www.planalto.gov.br/ccivil_03/leis/17716.htm, Erişim Tarihi: 28.02.2013.

Pointdecontact (2012a). <http://www.pointdecontact.net/contact.aspx>,
 Erişim Tarihi: 18.02.2012.

Pointdecontact (2012b). *Questions courantes.*
http://www.pointdecontact.net/questions_courantes.aspx, Erişim Tarihi: 18.02.2012.

Polat, Oğuz (2006). *Çocukların Cinsel Sömürüsü.*
http://www.stgm.org.tr/docs/1164619661cocuk_cinsel_somuru_rapor_01.doc,
 Erişim Tarihi: 12.10.2011.

Police-Nationale (2012). *Office Central De Lutte Contre La Criminalité Liée Aux Technologies De L'information Et De La Communication.* <http://www.police-nationale.interieur.gouv.fr/Organisation/Direction-Centrale-de-la-Police-Judiciaire/Lutte-contre-la-criminalite-organisee/Office-central-de-lutte-contre-la-criminalite-liee-aux-technologies-de-l-information-et-de-la-communication>.
 Erişim Tarihi: 11.03.2012.

Postman, Neil (2006). *Teknopoli: Yeni Dünya Düzeni* (Çev. M. Emre Yılmaz).
 İstanbul: Paradigma Yayınları.

Preston, Cheryl B. (2008). *Internet Porn, ICANN and Families: A Call To Action.*
Journal of Internet Law, October 2008. https://futureoftheinternet.org/redmine-prod/files/100711153816_Preston_2008_Internet_PORN_ICANN_and_Families_A_Call_to_Action.pdf, Erişim Tarihi: 09.12.2012

- Protegeles (2013). *Funcionamiento*. http://www.protegeles.com/es_que_es2.asp, Eriřim Tarihi: 24.02.2013.
- Protegeles (2013). *Nuestras l neas de ayuda*. <http://www.protegeles.com/index.asp>, Eriřim Tarihi: 22.02.2013.
- Puolam ki, Kai (2008). *Finnish Internet Censorship*. <http://www.effi.org/blog/kai-2008-02-18.html#is-the-censorship-legal>, Eriřim Tarihi: 26.08.2012.
- Radikal (11.03.2013). *Pornonun b y k  ıkmazı...*, <http://www.radikal.com.tr/radikal.aspx?atype=radikaldetayv3&articleid=1124550&categoryid=41>, Eriřim Tarihi: 13.10.2012)
- Rahm, Dianne (1997). The Role of Information Tecnology in Building Public Administration Teory, *Knowledge & Policy*. 10 (3).
- Redbarnet (2013). *Mobning og overgreb*. <http://www.redbarnet.dk/Mobning-og-overgreb.aspx?ID=136>, Eriřim Tarihi: 12.01.2013.
- RG (2013). *Federal Law on Counteracting Extremist Activity*. http://www.rg.ru/oficial/doc/federal_zak/114-fz.shtm, Eriřim Tarihi: 24.02.2013.
- Rheingold, Howard (1994). *The Virtual Community: Homesteading the Electronic Frontier*. New York: Harper Perennial.
- RIPE (2012a). *Ripe Network Coordination Center*. <http://www.ripe.net/>, Eriřim Tarihi: 08.12.2012.
- RIPE (2012b). *Devolopment of the Regional Internet Registry System*. <http://www.ripe.net/ripenc/about/regional/rir-system.html>, Eriřim Tarihi: 10.12.2012)
- RoadtoGrace (13.08.2013). *Current Porn Statistics*. <http://www.roadtoGrace.net/current-porn-statistics/>, Eriřim Tarihi: 20.08.2013
- Roberts, Hal , Zuckerman, Ethan and Palfrey, John (2009). *2007 Circumvention Landscape Report: Methods, Uses, and Tools*. The Berkman Center for Internet & Society at Harvard Unv.
- Robins, Kevin (1999). * maj: G rmenin K lt r ve Politikası* ( ev. Nur ay T rko lu). İstanbul: Ayrıntı Yayınları.
- Ropelato, Jerry (2012). *Internet Pornography Statistics*. <http://internet-filter-review.toptenreviews.com/Internet-pornography-statistics.html>, Eriřim Tarihi: 07.01.2012.

RSF (2012). *Turkey*. http://en.rsf.org/IMG/pdf/turkiye_2012-2.pdf,
Eriřim Tarihi: 13.11.2012.

RSOC (2013a). *Roskomnadzor*. <http://www.rsoc.ru/about/p179/>,
Eriřim Tarihi: 25.02.2013.

RSOC (2013b). *Credentials*. <http://www.rsoc.ru/about/credentials>,
Eriřim Tarihi: 25.02.2013.

RTÜK (2013). *Medya Okuryazarlıđı Nedir?*.
<http://www.medyaokuryazarligi.org.tr/nedir.html>, Eriřim Tarihi: 16.4.2013.

Russian Criminal Code (2013). *The Criminal Code Of The Russian Federation*.
<http://www.russian-criminal-code.com>, Eriřim Tarihi: 25.02.2013.

Sabah (10.01.2013). *Siber Güvenlik Tatbikatı Başladı*.
<http://www.sabah.com.tr/Teknoloji/Haber/2013/01/10/siber-guvenlik-tatbikati-basladi>, Eriřim Tarihi: 17.04.2013.

Safeline.gr (2013). *Other Internet Crimes*.
<http://www.safeline.gr/en/legislation/other-internet-crimes>,
Eriřim Tarihi: 01.03.2013.

Safenet.ne (2013a). *What is the rating system?*. <http://www.safenet.ne.kr/rsys.do>,
Eriřim Tarihi: 25.02.2013.

Safenet.ne (2013b). *Detailed rating standards*.
<http://www.safenet.ne.kr/drstan.do#part02>, Eriřim Tarihi: 25.02.2013.

Safer Children in a Digital World (2008). *The Report of the Byron Review*.
<http://dera.ioe.ac.uk/7332/1/Final%20Report%20Bookmarked.pdf>,
Eriřim Tarihi: 14.01.2012.

Safer Internet Day (2013). *Brazil Safer Internet Day Committee*.
<http://www.saferinternetday.org/web/brazil/home>, Eriřim Tarihi: 28.02.2013.

Safer İnternet (2012). *About us*. <http://www.saferinternet.org/web/guest/about-us>,
Eriřim Tarihi: 05.07.2012.

Saferinternet.gr (2013). *Helpline*. <http://www.saferinternet.gr/helpline>,
Eriřim Tarihi: 02.02.2013.

SaferNet Brasil (2013a). *Parceria com a Google Brasil*.
<http://www.safernet.org.br/site/sites/default/files/Google.pdf>,
Eriřim Tarihi: 28.02.2013.

SaferNet Brasil (2013b). *Content type*. <http://www.safernet.org.br/site/denunciar>,
Eriřim Tarihi: 28.02.2013.

SaferNet Brasil (2013c). *Dados Institucionais*.
<http://www.safernet.org.br/site/institucional/quem-somos/dados-institucionais>,
Eriřim Tarihi: 28.02.2013.

SaferNet Brasil (2013d). *Quem Somos*. <http://www.safernet.org.br/site/institucional>,
Eriřim Tarihi: 28.02.2013.

SaferNet Brasil (2013e). *Parcerias com o MPF*.
<http://www.safernet.org.br/site/institucional/parcerias/mpf>,
Eriřim Tarihi: 28.02.2013.

SaferNet Brasil (2013f). *Central Nacional de Denúncias de Crimes Cibernéticos*.
<http://www.safernet.org.br/site/institucional/projetos/cnd>, Eriřim Tarihi: 28.02.2013.

SaferNet Brasil (2013g). *O Que Denunciar*.
<http://www.safernet.org.br/site/institucional/projetos/cnd/o-que-denunciar>,
Eriřim Tarihi: 28.02.2013.

SaferNet Brasil (2013h). *Como Funciona*.
<http://www.safernet.org.br/site/institucional/projetos/cnd/como-funciona>,
Eriřim Tarihi: 28.02.2013.

SaferNet Brasil (2013i). *Parceria com a Google Brasil*.
<http://www.safernet.org.br/site/institucional/parcerias/google>,
Eriřim Tarihi: 28.02.2013.

SaferNet Brasil (2013i). *Termo de Cooperacao*.
<http://www.safernet.org.br/site/sites/default/files/Google.pdf>,
Eriřim Tarihi: 28.02.2013.

SaferNet Brasil (2013j). *Perceria com SEDH e DPF*.
<http://www.safernet.org.br/site/institucional/parcerias/sedh>,
Eriřim Tarihi: 28.02.2013.

SaferNet Brasil (2013k). *Termo de Cooperacao Técnica, Científica e Operacional*.
<http://www.safernet.org.br/site/sites/default/files/SEDHDPF.pdf>,
Eriřim Tarihi: 28.02.2013.

SaferNet Brasil (2013l). *Parceria com as Teles*.
<http://www.safernet.org.br/site/institucional/parcerias/teles>, Eriřim Tarihi: 28.2.2013.

SaferNet Brasil (2013m). *Termo de Mutua Cooperacao*.
<http://www.safernet.org.br/site/sites/default/files/Teles.pdf>, Eriřim Tarihi: 28.2.2013.

- SaferNet Brasil (2013n). *Helpline.br*. <http://www.safernet.org.br/site/webline>, Eriřim Tarihi: 28.02.2013.
- SaferNet Brasil (2013o). *Observatorio do Legislativo*. <http://www.safernet.org.br/site/institucional/projetos/obsleg>, Eriřim Tarihi: 8.2.2013.
- SaferNet Brasil (2013ö). *Parceria com o MySpace*. <http://www.safernet.org.br/site/institucional/parcerias/myspace>, Eriřim: 28.02.2013.
- SaferNet Brasil (2013p). *Termo de Mutua Cooperaao Tcnica, Cientifica e Operacional*. http://www.safernet.org.br/site/sites/default/files/COOPERACAO%20SAFERNET_MY%20SPACE.pdf, Eriřim Tarihi: 28.02.2013.
- SaferNet Brasil (2013r). *Prevencao*. <http://www.safernet.org.br/site/institucional/projetos/prevencao>, Eriřim: 28.02.2013.
- Saferunet (2013a). *Welcome*. <http://www.saferunet.ru/en/>, Eriřim Tarihi: 25.02.2013.
- Saferunet (2013b). *Internet-threats against public safety*. http://www.saferunet.ru/en/internet_threats_against_public_safety/, Eriřim: 25.2.2013.
- Saferunet (2013c). *Helpline*. <http://www.saferunet.ru/en/helpline/>, Eriřim: 25.2.2013.
- Saferunet (2013d). *General information on Internet-threats*. http://www.saferunet.ru/en/general_information_on_internet_threats, Eriřim Tarihi: 25.02.2013.
- Saferunet (2013e). *Huliganam.net*. http://www.saferunet.ru/huliganam_net/, Eriřim Tarihi: 25.02.2013.
- Salıcı, Berfu ve Güneř, İsmail (2010). *İnternette Güvenlik ve Denetim: Masumiyet Yitiriliyor mu?*. http://www.bilgiyonetimi.org/cm/pages/mkl_gos.php?nt=243, Eriřim Tarihi: 13.11.2010.
- Sanal Ortamda Oynatılan Talih Oyunları Hakkında Yönetmelik (2006). T.C. Resmi Gazete, 26108, 14.03.2006.
- Saran, Ulvi (2004). *Kamu Yönetiminde Yeniden Yapılanma*. Ankara: Atlas Yayları.
- Sarı, Ekrem (2011). *5651 Sayılı Kanun Kapsamında Eriřim Sağlayıcılığı Kavramı: Getirilen Hak, Yükümlülük Ve Sorumluluklar, Dünya'daki Uygulama Örnekleri*. İletişim Uzmanlığı Tezi, Bilgi Teknolojileri Ve İletişim Kurumu. Ankara.
- Sarıbay, Yařar A. (1996). *Siyasal Sosyoloji*. Bursa: Uludağ Üniversitesi Yayınları.
- Sarıhan, Tan D. (1998). *Herkes İçin İnternet 98*. İstanbul: Desnet Yayınları.

Sartori, Giovanni (2004). *Görmenin İktidarı* (Çev. G. Batuş-B. Ulukan). İstanbul: Karakutu Yayınları.

Savethechildren (2013). *Child Protection*. <http://www.savethechildren.net/what-we-do/child-protection>, Erişim Tarihi: 12.01.2013.

Selçuk, Ebru (2011). *Çocukları Zararlı İçeriklerden Koruma Tedbirleri Kapsamında Dünyada Ve Türkiye’de Güvenli İnternet Kavramı: Tarihsel Süreç Ve Geleceğe Bakış*. İletişim Uzmanlığı Tezi, Bilgi Teknolojileri Ve İletişim Kurumu, Ankara.

Shein, Esther (2010). *Massachusetts Internet Obscenity Law Challenged*. 14.07.2010. http://www.informationweek.com/news/government/state-local/showArticle.jhtml?articleID=225800159&cid=RSSfeed_IWK_All, Erişim Tarihi: 13.03.2011.

Sınar, Hasan (2001). *İnternet ve Ceza Hukuku*. İstanbul: Beta Yayınları.

Sırabaşı, Volkan (2007). *İnternet ve Radyo-Televizyon Aracılığıyla Kişilik Haklarına Tecavüz*, 2. Baskı. Ankara: Adalet Yayınevi.

Silicon (2009). *La loppsi 2 renoue avec lespionnage electronique*. http://www.silicon.fr/fr/news/2009/05/26/la_loppsi_2_renoue_avec_1_espionnage_electronique, Erişim Tarihi: 15.12.2011.

Sinema Filmlerinin Değerlendirilmesi Ve Sınıflandırılmasına İlişkin Usul Ve Esaslar Hakkında Yönetmelik (2005). T.C. Resmi Gazete, 25731, 18.02.2005.

Singo (2013a). *Objectives*. http://www.singo.or.kr/eng/03_cyber/Objectives.php, Erişim tarihi: 23.02.2013.

Singo (2013b). *Activities*. http://www.singo.or.kr/eng/03_cyber/Activities.php, Erişim tarihi: 23.02.2013.

SMH (2012). *Iran's leader sets up internet control group*. 08.03.2012. <http://www.smh.com.au/it-pro/government-it/irans-leader-sets-up-internet-control-group-20120308-1uljq.html>, Erişim Tarihi: 27.02.2013.

Socialbakers (2011). *Facebook Statistics*. <http://www.socialbakers.com/facebook-statistics/turkey>, Erişim Tarihi: 25.12.2011.

Softpedia (2008). *TeliaSonera Blocks Child Sexual Abuse Material Over the Web*, 4 Sept. 2008, <http://news.softpedia.com/news/TeliaSonera-Blocks-Child-Sexual-Abuse-Material-Over-the-Web-92979.shtml>, Erişim Tarihi: 16.05.2012.

Soysal, Tamer (2005). İnternet Servis Sağlayıcılarının Hukuki Sorumlulukları. *Türkiye Barolar Birliği Dergisi*, Kasım-Aralık 2005 Sayısı. <http://www.diyarbakir.adalet.gov.tr/makaleler/iss.pdf>, Erişim Tarihi: 17.12.2011.

Spletno (2012). *Child web porn law updated by EU to erase images*". http://www.spletno-oko.si/en/r/9/74/News/Child_web_porn_law_updated_by_EU_to_erase_images/?&p1=723&p2=727, Erişim Tarihi: 04.07.2012.

Stanley, J. and Steinhardt, B. (2003). *Bigger Monster, Weaker Chains: Growth of an American Surveillance Society*. New York: ACLU.

Staples, William G. (1997). *The Culture of Surveillance Discipline and Social Control in the United States*. New York: St. Martin's Pres.

Stargazete (2011). *Oyun bağımlısı kadın çocuklarını boğdu*. <http://stargazete.com/dünya/dunya/oyun-bagimlisi-kadin-cocuklarini-bogdu-haber-183588.htm>, Erişim Tarihi: 05.09.2011.

Stargazete (31.01.2010). *Facebook fotoğraf sayısıyla şaşırtıyor*. <http://stargazete.com/dünya/facebook-fotograf-sayisiyla-sasirtiyor-haber-241507.htm>, Erişim Tarihi: 12.04.2012.

Stargazete.com (14.02.2009). *Ekonomik kriz cinsel hayatı değiştirdi*. <http://www.stargazete.com/yasam/ekonomik-kriz-cinsel-hayati-degistirdi-169124.htm>, Erişim Tarihi: 05.10.2012.

Staysafeonline (2010). *Online Security and Privacy Study*. <http://www.whitehouse.gov/files/documents/cyber/National%20Cyber%20Security%20Alliance%20-%20Harris+Online+Security+and+Privacy+Study.pdf>, Erişim Tarihi: 21.11.2011.

Stoner, James R. (2010). *The Social Costs of Pornography*, The Witherspoon Institute. Washington.

Stopchildporno (2013a). *Awareness raising campaign*. <http://www.stopchildporno.be/en/child-focus-2/awareness-raising-campaign/>, Erişim Tarihi: 05.02.2013.

Stopchildporno (2013b). *Network*. <http://www.stopchildporno.be/en/child-focus-2/network/>, Erişim Tarihi: 05.02.2013.

Stop-it (2012). <http://www.stop-it.org/spip.php?article15>, Erişim Tarihi: 17.10.2012.

Subaşı, Necdet (2005). İnternet ve Sanal Cemaat Tartışmaları. (Der: Mutlu Binark ve Barış Kılıçbay). *İnternet, Toplum, Kültür*. Ankara: Epos Yayınları.

Superonline Workshop (2000). *İnternet ve Hukuk*. S.20.

Süer, Cem (2010). *Çin Google'ı Kendi Silahıyla Vuracak*. 29.06.2010.
<http://shiftdelete.net/cin-googlei-kendi-silahıyla-vuracak-21770.html>,
 Erişim Tarihi: 24.12.2012.

Şahin, Ali ve Örselli, Erhan (2010). *E-devlet Anlayışı Sürecinde Türkiye*.
<http://www.sosyalbil.selcuk.edu.tr:8080/319/1/alisahin.pdf>,
 Erişim Tarihi: 02.01.2010.

Şan, M. Kemal ve Hira, İsmail (2009). *Bilgi Toplumu: Bir Risk Olarak Özel Alanın Kayboluşu*. http://www.ceterisparibus.net/yeniekonomi/bilgi_toplumu.htm,
 Erişim Tarihi: 23.11.2009.

Şaylan, Gencay (1995). *Değişim Küreselleşme ve Devletin Yeni İşlevi*.
 Ankara: İmge Kitabevi.

Şen, Bilal (2012). *Bilişim Suçlarıyla Mücadele*.
 TBMM Bilişim ve İnternet Komisyonu Sunumu.

Şen, Osman N. (2003). *Polisin Bilişim Suçlarıyla Mücadelede Yapması Gerekenler. 1. Polis Bilişim Sempozyumu-Bildiriler*. 21-22.10.2003

Şen, Osman N. (2008). *Türkiye’de İnternet Trendleri*. İstanbul: Rota Yayınları.

Şen, Osman N. (2009). *TİB İnternet Dairesi Başkanı Osman N. Şen İnternet Alanında Türkiye ve Dünya’da Yaşanan Gelişmeleri Değerlendirdi*.
<http://www.turk.İnternet.com/portal/yazigoster.php?yaziid=23114>,
 Erişim Tarihi: 17.02.2012.

Şenel, Alaeddin (1995). *İlkel Topluluktan Uygar Topluma*.
 Ankara: Bilim ve Sanat Yayınları.

Şener, Gülüm (2009). *Türkiye’de Facebook Kullanımı Araştırması. İnet-tr’09, XIV. Türkiye’de İnternet Konferansı Bildirileri. 12-13 Aralık 2009*. İstanbul.

Şenormancı, Ömer (2012). *İnternet Bağımlılığı*. TBMM Bilişim ve İnternet Komisyonu Sunumu.

Takvim (02.06.2010). *Kayıp çocuklar porno kiskacında*.
http://takvim.com.tr/Yasam/2010/02/06/kayıp_cocuklar_porno_kiskacında,
 ErişimTarihi: 21.04.2011.

Talbot, David (2010). *China: Our Internet is Free Enough. 16 June 2010*,
<http://www.technologyreview.com/web/25592/?a=f>, Erişim Tarihi: 29.12.1012.

Tarcan, Ahmet (2005). Dünden Bugüne İnternet Üzerine Felsefî Yaklaşımlar. *İnternet ve Toplum* (Ed. Ahmet Tarcan). Ankara: Anı Yayınları.

Tarhan, Nevzat (2002). *Psikolojik Savaş (Gri Propaganda)*. İstanbul: Timaş Yayınları.

Taşçı, Kamil (2007). *Teorik Çerçevesi ve Uygulama Örnekleriyle Dünya’da ve Türkiye’de Yazılım Endüstrisi, Planlama Uzmanlığı Tezi*, Ankara: DPT.

Taşpınar, Mehmet ve Gümüş, Çetin (2003). *İnternet Kafelerin (Dijital Kütüphaneler) Eğitim Amaçlı Kullanımının Teşviki*.
<http://ab.org.tr/ab03/tammetin/139.doc>, Erişim Tarihi: 02.09.2012.

TBD (2006). *Bilişim Ağı Hizmetlerinin Düzenlenmesi ve Bilişim Suçları Hakkında Kanun Tasarısı Görüşleri*
http://www.tbd.org.tr/genel/bizden_detay.php?kod=188&tipi=5&sube= , Erişim Tarihi: 21.02.2012.

TBMM (2002). *TBMM Genel Kurul Tutanağı, 21. Dönem 4. Yasama Yılı, 99. Birleşim*, 14.5.2002,
http://www.tbmm.gov.tr/develop/owa/tutanak_sd.birlesim_baslangic?P4=7778&P5=B&page1=123&page2=123&web_user_id=11235813, Erişim Tarihi: 11.3.2013.

TBMM (2004). *5237 Sayılı Türk Ceza Kanununun Gerekçesi ve Komisyon Raporu*.
<http://www.sayilikanun.com/5237-sayili-turk-ceza-kanununun-gerekcesi-ve-komisyon-raporu/>, Erişim Tarihi: 25.03.2013.

TBMM (2006). *Bilişim Sistemi Üzerinden Suç Teşkil Eden Zararlı Yayınlarla Mücadele Hakkında Kanun Teklifi*. <http://www2.tbmm.gov.tr/d22/2/2-0958.pdf>, Erişim Tarihi: 24.02.2013.

TBMM (2007a). *Elektronik Ortamda İşlenen Suçların Önlenmesi ile 2559 ve 2937 Sayılı Kanunlarda Değişiklik Yapılmasına Dair Kanun Tasarısı ve İstanbul Milletvekili Gülseren Topuz’un; Bilişim Sistemi Üzerinden Suç Teşkil Eden Zararlı Yayınlarla Mücadele Hakkında Kanun Teklifi ile Adalet Komisyonu Raporu*.
<http://www.tbmm.gov.tr/sirasayi/donem22/yil01/ss1397m.htm>, Erişim Tarihi: 24.02.2013.

TBMM (2007b). *Elektronik Ortamda İşlenen Suçların Önlenmesi ile 2559 ve 2937 sayılı Kanunlarda Değişiklik Yapılmasına Dair Kanun Tasarısı*.
<http://www2.tbmm.gov.tr/d22/1/1-1305.pdf>, Erişim Tarihi: 25.02.2013.

TBMM (2007c). *TBMM Genel Kurul Tutanağı, 22. Dönem 5.Yasama Yılı 99. Birleşim*, 04.05.2007,
http://www.tbmm.gov.tr/develop/owa/tutanak_g_sd.birlesim_baslangic?PAGE1=1&PAGE2=1&p4=19906&p5=B, Erişim Tarihi: 12.04.2013.

TBMM (2011). *Evrensel İnsan Hakları Bildirgesi*.

<http://www.tbmm.gov.tr/komisyon/insanhaklari/pdf01/203-208.pdf>,

Erişim Tarihi: 14.12.2011.

TBMM (2012). *Bilgi Toplumu Olma Yolunda Bilişim Sektöründeki Gelişmeler ile İnternet Kullanımının Başta Çocuklar, Gençler ve Aile Yapısı Üzerinde Olmak Üzere Sosyal Etkilerinin Araştırılması Amacıyla Kurulan Meclis Araştırması Komisyonu Raporu*. <http://www.tbmm.gov.tr/sirasayi/donem24/yil01/ss381.pdf>, Erişim Tarihi: 04.03.2013.

Techcrunch (2008). German Politician Blocks Local Wikipedia.

<http://www.techcrunch.com/2008/11/16/german-politician-blocks-local-wikipedia/>,

Erişim Tarihi: 19.12.2011.

Tekeli, Hasan (1994). *Bilgi Çağı Bilgi Çağının Sosyal, Kültürel ve Ekonomik Etkileri*. İstanbul: Simavi Yayınları.

Tekeli, İlhan (1999). *Modernite Aşılırken Siyaset*. Ankara: İmge Yayınları.

Teknoloji Bilinçlendirme Platformu (2010). *Bir İhmal Hayatınızı Nasıl Değiştirir?*. Ankara.

Telefonoarcobaleno (2009). *Online Child Abuse in 2009*.

<http://www.diocesidicagliari.it/public/attach/1202/Report%202009%20Telefono%20Arcobaleno.pdf>, Erişim Tarihi: 04.07.2011.

Telefonoarcobaleno (2011a). *Report Annuale 2011*.

http://www.telefonoarcobaleno.org/wordpress/wp-content/uploads/2012/03/ReportAnnuale2011_new.pdf, Erişim Tarihi: 13.04.2012.

Telefonoarcobaleno (2011b). *Against Child Abuse and Sexual Exploitation*.

http://www.telefonoarcobaleno.org/wordpress/wp-content/uploads/2011/07/ShortReport-giugno2011_new.pdf,

Erişim Tarihi: 04.07.2011.

Telegraph (2011). *Norway: Anders Behring Breivik used online war games as 'training'*. <http://www.telegraph.co.uk/news/worldnews/europe/norway/8663329/Norway-Anders-Behring-Breivik-used-online-war-games-as-training.html>,

Erişim Tarihi: 02.10.2011.

Telegraph (21.11.2008). *Teenager commits suicide live on internet as 1,500 watch*.

<http://www.telegraph.co.uk/news/worldnews/northamerica/usa/3497263/Teenager-commits-suicide-live-on-internet-as-1500-watch.html>, Erişim Tarihi: 26.11.2011.

Telekomünikasyon Hizmet ve Altyapılarına İlişkin Yetkilendirme Yönetmeliği (2004). T.C. Resmi Gazete, 25565, 26.08.2004.

Telekomünikasyon Kurumu Tarafından Erişim Sağlayıcılara ve Yer Sağlayıcılara Faaliyet Belgesi Verilmesine İlişkin Usul ve Esaslar Hakkında Yönetmelik (2007). T.C. Resmi Gazete, 26680, 24.10.2007.

Telekomünikasyon Kurumu Tarafından İşletmecilere Uygulanacak İdari Para Cezaları İle Diğer Müeyyide ve Tedbirler Hakkında Yönetmeliği (2004). T.C. Resmi Gazete, 25574, 05.09.2004.

Telekomünikasyon Kurumunun Teşkilat ve Görevleri ile Çalışma Esas ve Usulleri Hakkında Yönetmelik (2000). T.C. Resmi Gazete, 24171, 15.09.2000.

Telekomünikasyon Yoluyla Yapılan İletişimin Tespiti, Dinlenmesi, Sinyal Bilgilerinin Değerlendirilmesi ve Kayda Alınmasına Dair Usul ve Esaslar ile Telekomünikasyon İletişim Başkanlığının Kuruluş, Görev ve Yetkileri Hakkında Yönetmelik (2005). T.C. Resmi Gazete, 25989, 10.11.2005.

Telekomünikasyon Yoluyla Yapılan İletişimin Tespiti, Dinlenmesi, Sinyal Bilgilerinin Değerlendirilmesi ve Kayda Alınmasına Dair Usul ve Esaslar ile Telekomünikasyon İletişim Başkanlığının Kuruluş, Görev ve Yetkileri Hakkında Yönetmelikte Değişiklik Yapılmasına Dair Yönetmelik (2009). T.C. Resmi Gazete, 27312, 07.08.2009.

Telekomünikasyon Yoluyla Yapılan İletişimin Tespiti, Dinlenmesi, Sinyal Bilgilerinin Değerlendirilmesi ve Kayda Alınmasına Dair Usul ve Esaslar ile Telekomünikasyon İletişim Başkanlığının Kuruluş, Görev ve Yetkileri Hakkında Yönetmelikte Değişiklik Yapılmasına Dair Yönetmelik (2011). T.C. Resmi Gazete, 28049, 09.09.2011.

Tezcan, Mahmut (1994). *Boş Zamanların Değerlendirilmesi Sosyolojisi*. Ankara: Atilla Kitapevi.

The Citizen Lab (2007). *Everyone's Guide To By-Passing Internet Censorship*. Sept. 2007, <http://citizenlab.org/CL-circGuide-online.pdf>, Erişim Tarihi: 15.01.2012.

Theregister (18.05.2006). *Govt Sets Target For Blocking Child Porn Sites*. http://www.theregister.co.uk/2006/05/18/uk_site_blocking/, Erişim Tarihi: 13.12.2011.

TheWordTracker Report (2012). *The Top 200 Long-Term Keyword Report*. www.word-tracker.blogspot.com, Erişim Tarihi: 27.04.2012.

TİB (2008). *İngiltere Çalışma ziyareti*. http://www.tib.gov.tr/dokuman/Sunu_Ingiltere_Duzenlenmis_3Aralik2008_v2, Erişim Tarihi: 15.01.2012.

TİB (2008a). “<http://dilekce.kampanya.org.tr>” adresinde yayınlanan dilekçeye cevap. http://www.tib.com.tr/dokuman/bb-13_06_08_tib.pdf, Erişim Tarihi: 13.07.2011.

TİB (2009). *Fransa Çalışma Ziyareti*. http://www.tib.gov.tr/dokuman/TIB_Fransa_Calisma_Ziyareti.pdf, Erişim Tarihi: 26.10.2011.

TİB (2009a). *2008 Yılı İnternet Dairesi Faaliyet Raporu*. Ankara.

TİB (2010). *2010 Yılı İnternet Dairesi Faaliyet Raporu*. Aralık-2010.

TİB (2012). *İnternet Bilgi İhbar Merkezi*. Haziran-2012.

TİB (2012b). *Güvenli İnternet Hizmeti’nin 1. Yılı Dolayısıyla Ankara ve İstanbul’da Etkinlikler Düzenlendi*. <http://www.tib.gov.tr/tr-uyuru-9999-hepsi.html#>, Erişim Tarihi: 24.06.2012.

TİB (2013). *Kronolojik Tarihçe*. http://www.tib.gov.tr/tr/tr-menu-8-kronolojik_tarihce.html, Erişim Tarihi: 23.4.2013.

TİB (2013a). *İnternet İçerik Düzenlemesi Hakkında Sorular*. http://www.tib.gov.tr/tr/tr-menu-47-internet_icerik_duzenlenmesi_hakkindaki_sorular.html, Erişim Tarihi: 26.04.2013.

TİB (2013b). *Site Bilgileri Sorgu Sayfası*. http://internet.tib.gov.tr/index.php?menu=menu_hakkimizda, Erişim Tarihi: 26.04.2013.

TİB (2013c). *Erişim ve yer sağlayıcılar listesi*. http://www.tib.gov.tr/tr/tr-menu-54-erisim_ve_yer_saglayicilar_listesi.html, Erişim Tarihi: 21.4.2013.

TİB (2013d). *Onaylı içerik filtreleme yazılımları*. http://www.tib.gov.tr/tr/tr-menu-53-onayli_icerik_filtreleme_yazilimlari.html, Erişim Tarihi: 21.4.2013.

TİB (2013e). *IP log imzalayıcı programı*. http://www.tib.gov.tr/tr/tr-menu-55-ip_log_imzalayici_programi.html, Erişim Tarihi: 21.4.2013.

TİB (2013f). *Görev ve sorumluluklar*. http://www.tib.gov.tr/tr/tr-menu-67-gorev_ve_sorumluluklar.html, Erişim Tarihi: 21.4.2013.

TİB (2013g). *Bilinçlendirme amaçlı yayınlar*. http://www.tib.gov.tr/tr/tr-menu-70-bilinclendirme_amacli_yayinlar.html, Erişim Tarihi: 21.4.2013.

TİB (2013h). *Koordinasyon faaliyetleri*. http://www.tib.gov.tr/tr/tr-menu-35-koordinasyon_faaliyetleri.html, Erişim Tarihi: 21.4.2013.

TİB ve ODTÜ (2011). *İnternet Kurulu-Sosyal Paylaşım Sitelerini Kullanma Alışkanlıklarını Araştırma Raporu*

TK (2008). *Youtube denetimi istemedi*. 02.08.2008, http://www.tk.gov.tr/Basin_Duyurular/basintk/2008/02.08.2008/1d17f8.pdf, Erişim Tarihi: 25.10.2012.

TMMOB Elektrik Mühendisleri Odası (2009). *Elektronik Gözaltı Dünyası E-Göz@ltı. İletişim Özgürlüğüne Müdahale Raporu*. Ankara.

Toffler, Alvin (1992). *Yeni Güçler, Yeni Şoklar*. İstanbul: Altın Kitaplar Yayınları.

Toffler, Alvin (1981). *Üçüncü Dalga*. (Çev. Ali Seden). İstanbul: Altın Kitaplar Yay.

Tolan, Barlas (1980). *Çağdaş Toplumun Bunalımı*. Ankara: Ankara İktisadi Ve Ticari İlimler Akademisi Yayınları.

Toluner, Sevin (1996). *Milletlerarası Hukuk Dersleri: Devletin Yetkisi*. 5. Bası. İstanbul: Beta Yayınları.

Topnews (2009). *Pornographic results not to be served by Google in China, 06.21.2009*. <http://www.topnews.in/pornographic-results-not-be-served-google-china-2180643>, Erişim Tarihi: 30.01.2013.

Toprak, Ali (2009). Facebook'ta Mahremin Dönüşümü, Teşhircilik ve Görme/Gösterme Hazzı. *İnet-tr'09, XIV. Türkiye'de İnternet Konferansı Bildirileri*. 12-13 Aralık 2009. İstanbul.

Torproject (2011). *Tor: anonymity online*. <http://www.torproject.org/>, Erişim Tarihi: 24.10.2011.

Törenli, Nurcan (2004). *Enformasyon Toplumu ve Küreselleşme Sürecinde Türkiye*. Ankara: Bilim ve Sanat Yayınları.

Törenli, Nurcan (2009). *E-Gözaltı: Yasadışı Dinleme ve Yeni İletişim Teknolojileri*. http://www.sendika.org/yazi.php?yazi_no=27868, Erişim Tarihi: 07.12.2009.

TPRT (2012). Section. <http://www.yprrt.eu/yprrt/content/sections>, Erişim Tarihi: 01.04.2012.

TRABİS (2013). <http://www.trabis.gov.tr/tr/index.html>, Erişim Tarihi: 16.04.2013.

TTNET blog (2011). *Türkiye'nin İnternet ve Bilgisayar Fotoğrafını Çeken Araştırma*, 23.06.2011. <http://blog.ttnet.com.tr/turkiye%E2%80%99nin-internet-ve-bilgisayar-fotografini-ceken-arastirma/>, Erişim Tarihi: 18.01.2013.

Turan, Oğuz (2006). *Bilgisayar Ağları İle İlgili Suçlar*. Planlama Uzmanlığı Tezi, DPT, Ankara.

Turan, Saliha (2008). *İnternet Ağında Çocuğum*. İstanbul: Gül Yurdu Yayınları.

Turkish Daily News (2007). *Minding the gap in child porn laws*. 16.01.2007, <http://www.hurriyetaailynews.com/minding-the-gap-in-child-porn-laws.aspx?pageID=438&n=minding-the-gap-in-child-porn-laws-2007-01-16>, Erişim Tarihi: 13.02.2013.

TÜBİTAK (2002). *Bilgi Toplumu Politikaları Üzerine Bir Değerlendirme*. Ankara: TÜBİTAK.

TÜİK (2012). *Hanehalkı Bilişim Teknolojileri Kullanımı Araştırması, 2012*. <http://www.tuik.gov.tr/PreHaberBultenleri.do?id=10880>, Erişim Tarihi: 04.03.2013.

Türk Ceza Kanunu (1991). T.C. Resmi Gazete, 20901, 14.06.1991, 3756 Sayılı Kanun.

Türk İnternet (2008). *5 Mayıs 2008 İtibariyle Son YouTube Erişime Kapatılma Olayı ve 5651 ile İlgili Gelişmeler*. <http://turk.internet.com/dosya/0809/yazilar/>, Erişim Tarihi: 27.04.2013.

Türk İnternet (2010). *Web 2.0 Nedir?*. <http://turk.internet.com/haber/yazigoster.php3?yaziid=14394>, Erişim Tarihi: 09.12.2010

Türk İnternet (2012). *Alternatif Bilişim Derneği, AİHM'in Sites.Google.Com Kararı için Bir Açıklama Yaptı*. 19.12.2012, <http://www.turk-internet.com/portal/yazigoster.php?yaziid=40323>, Erişim Tarihi: 30.01.2012.

Türkiye Bilişim Vakfı (2011). *5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunda Değişiklik Yapılması Hakkında Kanun Tasarısı*. İstanbul.

Tüzün, Hakan (2006). *Bilgisayar Oyunlarının Yararları ve Zararları*. <http://inet-tr.org.tr/inetconf11/bildiri/101.pdf>,

U.S. Copyright Office (1998). *The Digital Millennium Copyright Act Of 1998*. <http://www.copyright.gov/legislation/dmca.pdf>, Erişim Tarihi: 15.06.2012.

U.S. Copyright Office(2012). *eCO Online System*. <http://www.copyright.gov>, Erişim Tarihi: (17.12.2011).

UCL (11.06.2008). *Information Behaviour of The Researcher of The Future*. <http://www.theatlantic.com/doc/200807/google>, Erişim Tarihi: 25.11.2010.

Uçkan, Özgür (01.04.2013). *Nefreti Filtrelemek*. <http://www.bthaber.com/nefreti-filtrelemek/#>, Erişim Tarihi: 14.04.2013.

Uçkan, Özgür (2003). *E-Devlet, E-Demokrasi ve E-Yönetişim Modeli: Bir İlkesel Öncelik Olarak Bilgiye Erişim Özgürlüğü*.
http://www.stradigma.com/turkce/haziran2003/print_09.html,
Erişim tarihi 16.10.2009.

Uçkan, Özgür (2009). *Fransa Telifli İçerik İndirene Ceza Getiren HADOPI2 Yasası'nı Kabul Etti. Türkiye Bu Akımdan Etkilenir mi?*.
<http://www.bilisimhukuk.com/2009/09/fransa-telifli-icerik-indirene-ceza-getiren-hadopi2-yasasini-kabul-etti-turkiye-bu-akimdan-etkilenir-mi/>,
Erişim Tarihi: 18.06.2012.

Uçkan, Seher vd. (2005). Bilgi Toplumu ve Bilgi Yönetimi. (Ed. C.Can Aktan, İstiklal Y. Vural). *Bilgi Çağı Bilgi Yönetimi ve Bilgi Sistemleri*.
Konya: Çizgi Kitabevi.

Uğur, Aydın ve Bilici, Mücahit (1998). Dijital Alemin Genleşen Kamusal Alanı. *Yeni Türkiye Dergisi* 21. Yüzyıl Özel Sayısı, 1(19).

UIKE (2011). *The Association For UK Interactive Entertainment*. <http://ukie.info//>,
Erişim Tarihi: 22.12.2011.

UKSIC (2012). *About*. <http://www.saferinternet.org.uk/about>,
Erişim Tarihi: 14.05.2012.

UMKC (2011). *Regulation of Obscenity*.
<http://www.law.umkc.edu/faculty/projects/ftrials/conlaw/obscenity.htm>,
Erişim Tarihi: 23.10.2011.

US Department of State Diplomacy in Action (2005). *Report on Global Anti-Semitism*. <http://www.state.gov/g/drl/rls/40258.htm>, Erişim Tarihi: 11.10.2011.

USA Today (14.11.2005). *U.N. control of Internet? An idea for the "delete" file*.
http://www.usatoday.com/news/opinion/editorials/2005-11-14-our-view_x.htm,
Erişim Tarihi: 08.12.2012.

USA Today (16.11.2005). *Be Wary of Internet 'Governance'*.
http://usatoday30.usatoday.com/news/opinion/editorials/2005-11-29-letters-tunisia_x.htm, Erişim Tarihi: 12.12.2012.

USDOJ (2011). *Child Pornography Prevention Act*. <http://www.ojp.usdoj.gov>,
Erişim Tarihi: 21.09.2011.

- USK (2012). *Wie Alterskennzeichen bei der USK entstehen*.
<http://www.usk.de/pruefverfahren/pruefverfahren/>, Eriřim Tarihi: 03.04.2012.
- Uzunay, Yusuf ve Koak, Mustafa (2005). İnternet Üzerinden ocuk Pornografisi ve Mcadelede Yařanan Sıkıntılar. *Polis Bilimleri Dergisi*, 7 (1).
- Verisign (2013). *Domain Name Industry Brief*.
<http://www.verisigninc.com/assets/domain-name-brief-april2013.pdf>,
 Eriřim Tarihi: 06.09.2013.
- Verisigninc (2013). *Domain Name Industry Brief. Volume 10-Issue 1*, April 2013.
<http://www.verisigninc.com/assets/domain-name-brief-april2013.pdf>,
 Eriřim Tarihi: 01.05.2013.
- Verkovsky, Alexander (2011). *Inappropriate Enforcement of Anti-extremist Legislation in Russia in 2011*, 27 April 2011. <http://www.sova-center.ru/en/misuse/reports-analyses/2012/04/d24302/>, Eriřim Tarihi: 25.02.2013.
- Vidinli, İ. Bahattin (2013). *Ulusal Siber Gvenlik alıřmaları ve USOM. Siber Gvenlik Konferansı-2013*, 14.05.2013, İstanbl,
<http://www.siberguvenlik.org.tr/wp-content/uploads/2013/05/bahattin-vidinli.pdf>,
 Eriřim Tarihi: 24.04.2013.
- Vill (2000). *US Court of Appeals for the 3rd Circuit, No. 99-1234*.
<http://vls.law.vill.edu/locator/3d/Jun2000/991324.txt>, Eriřim Tarihi: 12.11.2011.
- Villeneuve, Nart (2005). *Tunisia: Internet Filtering*.
<http://www.nartv.org/2005/06/07/tunisia-internet-filtering/> Eriřim Tarihi: 15.12.2011.
- Vodafone (2012). *5651 İnternet Ortamında Yapılan Yayınların Dzenlenmesi Ve Bu Yayınlar Yoluyla İřlenen Sularla Mcadele Edilmesi Hakkında Kanun İle İlgili Deęiřiklik Taslaęı*.
http://internetkurulu.org/Images/Editor/vodafone_5651_gerekceli_yasa_taslagi_v2.doc, Eriřim Tarihi: 21.09.2012.
- w3.org (2011). *PICS*. <http://www.w3.org/PICS/>, Eriřim Tarihi: 18.09.2011.
- Washington (2011). *URL Forwarding and URL Masking Services*.
<http://www.washington.edu/computing/web/publishing/url-forwarding.html>,
 Eriřim Tarihi: 22.08.2011).
- Web112.net (2010). *What is illegal content?*.
www.web112.net/en/IllegalContentEn.aspx, Eriřim Tarihi: 05.02.2010.
- Web3event (2011). *Web 3.0 Conference*. <http://www.web3event.com>,
 Eriřim Tarihi: 03.10.2011.

Weber, Max (1996). *Sosyoloji Yazıları*. (Çev.Taha Parla). İstanbul: İletişim Yay.

Webrazzi (12.12.2012). *Spor Sitelerini Ziyarette Avrupa Birincisiyiz*.
<http://www.webrazzi.com/2012/04/12/comscore-turkiye-spor-site/>,
 Erişim Tarihi: 18.04.2013.

Webrazzi (23.07.2013). *İngiltere online pornografiye tarihinin en büyük savaşını açıyor*. <http://www.webrazzi.com/2013/07/23/ingiltere-online-pornografi/>,
 Erişim Tarihi: 23.07.2013.

Webrazzi (26.08.2011). *ComScore: Türk İnternetinin Kullanıcılarının Yaklaşık Yüzde 82'si Blog Ziyaretçisi*. <http://www.webrazzi.com/2011/08/26/comscore-turk-blog-ziyaretçisi/>, Erişim Tarihi: 18.04.2013.

Weeks, Naomi (2010). *Effects of Pornography on Relationships*.
http://extension.usu.edu/files/publications/publication/FC_Marriage_2010-01pr.pdf,
 Erişim Tarihi: 28.04.2011.

WGIG (2005). *Report of the Working Group on Internet Governance. June 2005*.
<http://www.wgig.org/docs/WGIGREPORT.pdf>, Erişim Tarihi: 24.10.2011.

Whittle, D.B. (1997). *Cyberspace: The Human Dimension*. New York: W. H. Freeman and Company.

Wikipedia (2010a). *İnternet*.
http://tr.wikipedia.org/wiki/İnternet_%28%C3%B6zel_isim%29,
 Erişim Tarihi: 12.11.2010.

Wikipedia (2010b). *Milnet*. <http://en.wikipedia.org/wiki/Milnet>,
 Erişim Tarihi: 23.09.2010.

Wikipedia (2010c). *World Wide Web*.
http://en.wikipedia.org/wiki/World_Wide_Web, Erişim Tarihi: 23.09.2010.

Wikipedia (2010d). *Web 2.0*. http://en.wikipedia.org/wiki/Web_2.0,
 Erişim Tarihi: 09.12.2010.

Wikipedia (2011a). *Altın Kalkan Projesi*.http://tr.wikipedia.org/wiki/Alt%C4%B1n_Kalkan_Projesi,
 Erişim Tarihi: 12.07.2011.

Wikipedia (2011b). *CIPA*.
http://en.wikipedia.org/wiki/Children's_Internet_Protection_Act,
 Erişim Tarihi: 21.12.2011.

Wikipedia (2011c). *Nüdzizm*. <http://tr.wikipedia.org/wiki/Nudzizm>,
Erişim Tarihi: 30.12.2011.

Wikipedia (2011d). *Internet Watch Foundation And Wikipedia*.
http://en.wikipedia.org/wiki/Internet_Watch_Foundation_and_Wikipedia,
Erişim Tarihi: 18.12.2011.

Wikipedia (2012a). *Pirate Party*. http://en.wikipedia.org/wiki/Pirate_Party,
Erişim Tarihi: 12.03.2012.

Wikipedia (2012b). *Proxy server*. http://en.wikipedia.org/wiki/Proxy_server,
Erişim Tarihi: 24.04.2012.

Wikipedia (2012c). *Tags*. <http://en.wikipedia.org/wiki/Tags>, Erişim Tarihi: 24.1.2012.

Wikipedia (2012d). *Digital Economy Act 2010*.
http://en.wikipedia.org/wiki/Digital_Economy_Act_2010, Erişim Tarihi: 13.02.2012.

Wikipedia (2012e). *CNN*.
http://fr.wikipedia.org/wiki/Conseil_national_du_num%C3%A9rique,
Erişim Tarihi: 11.03.2012.

Wikipedia (2012f). *Délégation Aux Usages De l'Internet*.
http://fr.wikipedia.org/wiki/D%C3%A9l%C3%A9gation_aux_Usages_de_l'Internet,
Erişim Tarihi: 18.02.2012.

Wikipedia (2013). *Party for Neighbourly Love, Freedom, and Diversity*.
http://en.wikipedia.org/wiki/Party_for_Neighbourly_Love,_Freedom,_and_Diversity
Erişim Tarihi: 08.03.2013.

Willmaster (2011). *URL Masking*.
<http://www.willmaster.com/library/webdevelopment/URL-masking.php>,
Erişim Tarihi: 24.08.2011.

Wingate, Philippa (2001). *İnternet* (Çev. Selma İkiz). Ankara: TÜBİTAK.

Winston, S. (1996). *Herkes İçin Bilgisayar Rehber* (Çev. Serdar Yıldız).
Ankara: Sistem Yayıncılık.

Wise, Richard (2000). *The Computer Counter-Culture, Multimedia A Critical Introduction* (Ed. Richard Wise), Routledge, London.

Wolfgarten, Sebastian (2005/2006). *Investigating Large-Scale Internet Content Filtering*. M.Sc. In Security & Forensic Computing 2005/2006. Dublin City University, Ireland.

Xbox (2010). <http://www.xbox.com/en-GB/xbox360/consoles?xr=shellnav>, Erişim Tarihi: 15.10.2011.

Yamaç, Fatih (2003). Siber Terörizm Denemeleri-1. *Hatay Polis Dergisi*, Sayı: 6.

Yargıtay Kararı (1993). Yargıtay 7. Ceza Dairesi, 21.10.1993 tarihli E: 1993/5454, K: 1993/5691.

Yargıtay Kararı (1999). Yargıtay 5. Ceza Dairesi'nin, 06.05.1999 tarihli E:1999/523, K:1999/1991.

Yargıtay Kararı (2001). 02.11.2001 tarihli E:2001/6820 K:2001/6484.

Yargıtay Kararı (2010). Yargıtay Ceza Genel Kurulu'nun 07.12.2010 tarihli E:2010/5-243 K:2010/250.

Yavanoğlu, Uraz ve Sağiroğlu, Şeref (2010). Sosyal Ağlar ve Bilgi Güvenliği. 4. *Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı Bildiriler Kitabı*. 6-8 Mayıs 2010. Ankara.

Yayın Hizmeti Usul Ve Esasları Hakkında Yönetmelik (2011). T.C. Resmi Gazete, 28103, 02.11.2011.

Yeniaktüel (2006). *20 milyar dolarlık kara ticaret*. Sayı:68 <http://www.yeniaktuel.com.tr/turl12,68@2100.html>, Erişim Tarihi: 28.07.2011.

Yeşil, Sezen ve Alkan, Mustafa (2007). İnternet Yönetişimi ve İçerik Düzenlemeleri. XII. "Türkiye'de İnternet" Konferansı Bildirileri. 8-10 Kasım 2007, Ankara. <http://inet-tr.org.tr/inetconf12/bildiri/26.doc>, Erişim Tarihi: 15.08.2011.

Yeşilyurt, Nuri (2007). *ICANN Tartışmaları Ve Uluslararası Politika*. <http://ab.org.tr/ab07/bildiri/55.doc>, Erişim Tarihi: 24.10.2012.

Yıldız, M. Cengiz (2003). İnternet Kafeler, Gençlik ve Sosyal Sapma. 1. *Polis Bilişim Sempozyumu-Bildiriler*, 21-22.10.2003.

Yıldız, M. Cengiz ve Bölükbaş, Kenan (2005). *İnternet Kafeler, Gençlik ve Sosyal Sapma*. <http://www.felsefe.gen.tr/sosyalsapma.asp>, Erişim tarihi: 05.09.2011.

Yıldız, Sevil (2007). *Suçta Araç Olarak İnternetin Teknik ve Hukuki Yönden İncelenmesi*. Ankara: Nobel Yayın Dağıtım.

Yılmaz, Bülent (2006). Bilgi Toplumu: Eleştirel Bir Yaklaşım. *Hacettepe Üniversitesi Edebiyat Fakültesi Dergisi*, 15(1).

Young, K.S. (2004). Internet addiction. *Am Behav Sci*, Vol 48.

Yücel, İsmail H. (2010). *Bilim-Teknoloji Politikaları ve 21. Yüzyılın Toplumu*. <http://ekutup.dpt.gov.tr/bilim/yucelih/biltek03.pdf>, Erişim Tarihi: 02.01.2010.

Yücesan-Özdemir, Gamze (2008). *İletişim, Emek ve Kalkınma Ekonomi Politik Yaklaşım*. Ankara: Gazi Üniversitesi İletişim Fakültesi Yayınları.

Yürüşen, Melih (2001). Pornografiyi İfade Özgürlüğü Bağlamında Düşünmek. *Liberal Düşünce Dergisi*, Yıl 6, Sayı 24.

Zaman (06.11.2012). *Türk Telekom, Türkiye'nin İnternet Kullanım Haritasını Çıkardı*. http://www.zaman.com.tr/teknoloji_turk-telekomturkiyenin-internet-kullanim-haritasini-cikardi_2010501.html, Erişim Tarihi: 18.01.2013.

Zaman (2008). *İşte İnternet yasakçılık ligi*. <http://www.zaman.com.tr/haber.do?haberno=728737>, Erişim Tarihi: 18.09.2011.

Zaman (23.12.2009). <http://www.zaman.com.tr/haber.do?haberno=930927>, Erişim Tarihi: 14.12.2011.

Zaman (25.02.2009). *Facebook ve Myspace çocukların beyinlerine zararlı*. <http://www.zaman.com.tr/haber.do?haberno=819162&title=facebook-ve-myspace-cocukların-beyinlerine-zararlı>, Erişim Tarihi: 25.11.2012.

ZDNet (2006). *Image: Jingjing and Chacha, China's cartoon censorship cops*. http://content.zdnet.com/2346-9595_22-12766.html, Erişim Tarihi: 29.12.2011.

Zeller, Jr. Tom (2006). *How to Outwit the World's Internet Censors*. N.Y.Times, 29 Jan 2006.

Zeropaid (2009). *French Cybercrime Expert Discusses Loppsi 2 Legislation*. <http://www.zeropaid.com/news/86373/french-cybercrime-expert-discusses-loppsi-2-legislation/>, Erişim Tarihi: 19.04.2012.

Zuckerman, Ethan (2008). *Access Controled: Intermediary Censorship*. <http://www.access-controlled.net/>, Erişim Tarihi: 28.01.2012.

MÜLAKAT YAPILAN KİŞİLER

Dr. Osman Nihat Şen, TİB Başkan Vekili, İnternet Dairesi Başkanı, 06.08.2013

Emin Sadık Aydın, Bilgi Toplumu Dairesi Başkanı, 25.07.2013

Dr. Yasin Söyler, Başbakanlık E-Devlet Çalışma Grubu (Hukuk), 01.08.2013

Dr. Şahin Bayzan, TİB İletişim Uzmanı (Teknik), 24.07.2013

Ömer Boz, TİB İletişim Uzmanı (Hukuk), 30.07.2013

Mehmet Sarı, TİB İletişim Uzmanı (İdari), 24.07.2013

Lütfi Güvener, TİB İletişim Uzmanı (Teknik), 24.07.2013

EK-1: ÖNERİLER

Bu kısımda, İnternet içerik düzenlemesi sorunu bağlamında ele alınan tüm bu konulardan ve Türkiye örneğinin değerlendirilmesinden sonra, Türkiye’de içerik düzenlemelerinin geleceğiyle ilgili faydalı olacağı ümit edilen öneriler paylaşılacaktır. Önerilerin bir kısmı içerik politikalarıyla ilgiliyken, bir kısmı da örgütsel teklifleri içermektedir.

A. Politikalar

Bu bölümde İnternet içerik düzenlemesi açısından Türkiye’nin gelecek perspektifi içinde bulunmasını faydalı gördüğümüz politika teklifleri yer almaktadır.

1. Bütüncül Bilgi Toplumu ve İnternet Strateji ve Politikaları Oluşturulması

Türkiye’de, tüm gerçekliği ile birlikte bilgi toplumu olgusunu ele alarak ülkemiz açısından bütüncül bir bilgi toplumu stratejisi ve politikası oluşturmak gerekmektedir. Nitekim, bu çerçevede söz konusu ihtiyacı karşılamak için, 2003 yılında başlatılan e-Dönüşüm Türkiye Projesi kapsamında, günümüze kadar farklı dönemlere ait bir çok bilgi toplumu strateji ve eylem planı belgeleri hazırlanmış ve uygulanmıştır. Bütüncül bir bilgi toplumu strateji ve politikası oluşturmaya yönelik bu girişimleri takdir etmekle birlikte, söz konusu belgelerde, bilgi toplumunun beraberinde getirdiği risk, tehdit ve sorunlara ilişkin tarafın ön plana çıkartılmadığı ve eksik yansıtıldığı görülmektedir.

Keza, Türkiye’nin bilgi toplumuna ve İnternete bakışını ve İnternet politikalarının ana eksenini oluşturan söz konusu belgelerde temel yaklaşımın ekonomi ve teknoloji merkezli olduğu görülmektedir. Onun için söz konusu belgelerde daha ziyade ekonomik kalkınma, refah devleti olma, teknolojinin yaygınlaştırılması, üretimde ve kullanımda teknolojik gelişmişliği yakalama, e-devlet uygulamaları ile devleti dönüştürme ve hatta demokratikleştirme konularının ön plana çıktığı gözlemlenmektedir. Birazda yaşanan dönemin özelliklerine uygun olarak, bilgi toplumuna dönüşme ve bilgi ekonomisine geçme hedefi büyük bir ideal olarak

benimsenerek belgelere yansımıştır. Konunun, bilgi toplumuna yöneltileen eleştiriler, bilgi ve iletişim teknolojilerinin ve özellikle İnternetin taşıdığı potansiyel riskler, bizzat kendisinin veya yanlış kullanımının neden olduğu sorunlar, yasadışı ve zararlı içeriklerin durumu, sosyal maliyetler gibi olumsuz yönleri özellikle başlangıçta çok fazla ön plana çıkartılmamıştır.

Bu iyimser yaklaşımın benimsenmesinde, Türkiye’de başlangıçta İnternet kullanımının düşük olmasının ve dolayısıyla İnternetin beraberinde getirdiği güvenlik ve toplumsal sorunlarla henüz fazlasıyla tanışılmamış olmasının etkili olduğu düşünülebilir. Bunun yanında, ülkenin ekonomik, sosyal ve siyasal iç dinamikleri nedeniyle, bu tür sorunların dile getirilmesinin ekonomik kalkınma ve teknolojinin yaygınlaştırılması hedefleri açısından risk ve engel oluşturabileceği endişesinden kaynaklanmış olabilir. Bu çerçevede, henüz gelişmekte olan bilişim sektörünün ürkütülmesinden korkulması, İnternet düşmanı ilan edilme kaygısı, AB ile olan ilişkilerin yara alması endişesi gibi birçok sebep de akla gelebilir.

Bu temel yaklaşımın ve endişelerin, en azından bir kısmının, yoğunluğu azalsa da halen geçerliliğini sürdürmektedir. Zira, bilgi toplumu belgeleri için başlangıçta oluşturulan tema ve kurgu sonraki yıllarda çok fazla değişmeden süregelmiştir. O nedenle belgelerde yer alan strateji, eksen ve parametreler kısmen güncellenerek değişime uğrasa da bilgi toplumuna yönelik bu iyimser yaklaşım ve bunun üzerine inşa edilen idealleştirilmiş hedefler ve öncelikler büyük oranda korunmuştur.

Bununla birlikte, bilgi toplumu belgelerinin temelinde bu eksik yaklaşım göze çarparsa da, zaman içinde, önce bilişim suçlarından başlamak üzere, İnternet kaynaklı sorun alanlarının ve bu alanlara yönelik çözüm eylemlerinin bu tür belgelere girmiş olduğu görülmektedir. “Güvenli İnternet” bağlamında yasadışı ve zararlı içerikle mücadeleyi de öngören eylemlerin daha sonraki belgelerde yer almasını bu kapsamda değerlendirebiliriz. Biraz geç kalınmış ve yetersiz olsa da, bu ve benzeri konuların söz konusu belgelere girmiş olmasını, sorunların varlığının ve baştan beri sürdürülen eksik yaklaşımın zimmen kabul edilmesi ve daha dengeli bir yaklaşımın geliştirilmesi çabası olarak görülebiliriz.

Sonuç olarak, Türkiye, bütüncül bir bilgi toplumu stratejisi ve politikası oluşturma ve uygulama yolunda önemli bir adımı e-dönüşüm Türkiye Projesi kapsamında hazırladığı bilgi toplumu strateji ve eylem planı belgeleri ile atmıştır. Fakat, çıkarılan bu yolda, bilgi toplumunun beraberinde getirdiği risk, tehdit ve sorun alanlarının kısmen göz ardı edilmesiyle varlığını hissettiren eksik yaklaşım, gerçekçi ve isabetli bütüncül bilgi toplumu strateji ve politikaları oluşturulmasının önünde önemli bir engel olarak karşımıza çıkmaktadır.

O halde yapılması gereken, söz konusu belgelerde tek taraflı olarak, bilgi toplumunun sunmuş olduğu imkan ve fırsatlar üzerinden ekonomik kalkınma, refah devleti olma ve teknolojik gelişmişliği yakalama gibi sadece olumlu yönlere odaklanma yaklaşımından vazgeçerek, bilgi toplumuyla gündeme gelen risk, tehlike ve sorunlar tarafının da objektif bir şekilde strateji ve eylem planlarına yansıtılmasını sağlamaya çalışmaktır. Bu dengeli yaklaşımın belgelerde yer alması durumunda gerçek anlamda bütüncül bir bilgi toplumu stratejisi ve politikası oluşturulabilecektir.

Bu yaklaşımın ilk olarak İnternet strateji ve politikalarının temel referans metni olan bilgi toplumu strateji belgelerinde karşılığı olmalıdır. Bu yaklaşımın bilgi toplumu belgelerinde yer alması bize, İnternet içeriğinin düzenlenmesiyle ilgili konunun her yönünü ve aktörünü dikkate alacak, kuşatacak ve ona göre en uygun karar ve uygulamaları ortaya koymaya yarayacak sağlam bir zemin oluşturacaktır.

İkinci olarak, bahsi geçen yaklaşım içinde, Bilgi Toplumu Stratejisi ve Eylem Planı Belgesi'ne süre ve içerik olarak uyum gösteren, İnternetin tüm yön ve aktörlerini, dinamik yapısını ve özelliklerini içine alan ve bunları ülkemizin iç dinamikleri ve özellikleri ile harmanlayan bütüncül bir "İnternet Stratejisi ve Politika Belgesi" ve "Eylem Planı Belgesi" oluşturulmalıdır. Bu belgede, bilgi toplumu belgesinde yer alan çerçeve içerisinde konular detaylandırılmalı, alt stratejiler, politika ve eylemler yer almalıdır. Keza, bu metinde İnternetin diğer boyutları yanında içerik güvenliğinin sağlanmasına yönelik olarak yasadışı ve zararlı içeriklerle mücadele edilmesi konusu teknik, sosyal, ekonomik, yönetsel, hukuksal, eğitsel, polisiye, uluslararası işbirliği vb. yönleriyle strateji, politika ve eylemlere konu edilmelidir.

Üçüncü olarak ise, “İnternet Stratejisi ve Politika Belgesi” ve “Eylem Planı Belgesi”nde çerçevesi çizilen hususlara göre, tıpkı “Siber Güvenlik Strateji Belgesi” gibi ayrı bir “İnternet İçerik Güvenliği Stratejisi ve Eylem Planı Belgesi” hazırlanmalıdır. Bu belgede, içerik düzenlemesine ilişkin tüm konular, bütün yönleri ve aktörleri ile birlikte bulunmalıdır. Bu kapsamda, İnternetin güvenli kullanımı, katalog suçları da dahil olmak üzere diğer yasadışı ve zararlı içeriklerle mücadele, erişim engelleme ve filtreleme uygulamaları, özel anlaşmalar yapma, bilinçlendirme, İnternet etiği, İnternet okur-yazarlığı, pozitif yerli içerik oluşturma, öz düzenleme, ihbar merkezi, yardım hattı, hukuki düzenlemeler, uluslararası işbirliği çalışmaları vs. hepsiyle ilgili strateji, politika ve eylemler yer almalıdır.

2. İnternetin Sosyal Boyutu İle İlgili Araştırmalara Olan İhtiyaç

Görüldüğü gibi, İnternetin muharrik güç olduğu bilgi toplumu sürecinde çok önemli sosyal, kültürel, siyasal ve ekonomik değişimler ve dönüşümler yaşanmıştır. Keza, her değişim ve dönüşüm sürecinin, sunduğu imkanlara paralel olarak bazı riskler ve tehditler de taşıması beklenen bir durumdur. Adeta toplumların genetiğini değiştiren, başta çocuklar, gençler ve aileler olmak üzere toplumun bütün kesimlerini derinden etkileyen ve etkilemeye devam eden bu yeni sürecin sunmuş olduğu imkanlardan yararlanırken risklerinden korunmaya yönelik çabalar sarf etmek önem arz etmektedir. Sarf edilecek çabaların ise, belirlenecek strateji ve politikalara göre şekillendirilmesi gerekmektedir. Bu kapsamda, belirlenen strateji ve politikaların ve bunlara dayalı olarak gösterilen çabaların başarısı, söz konusu sürecin bütün unsurlarını ve bunların muhtemel tüm sonuçlarını sağlıklı bir biçimde ortaya koyan ciddi ve kapsamlı çalışmalarla elde edilen verilere ve bu verilerin doğru olarak okunmasına ve yorumlanmasına bağlıdır.

Diğer bir deyişle, her bir olgu veya olayın dayandığı siyasal, sosyal ve ekonomik arka plan ve gerçekliği vardır. Söz konusu olgu veya olaya ilişkin strateji ve politikalar bu arka plan ve gerçeklik üzerine bina edilir/edilmelidir. Strateji ve politikaların isabetliliğini ise, bahsi geçen olgu ve olay konusunda yapılacak ciddi ve

kapsamlı çalışmaların söz konusu arka plan ve gerçekliğe nüfuzu ile olgu veya olaya ilişkin elde edilen vukufiyetin derecesi belirleyecektir.

Dolayısıyla, çok yönlü ve çok aktörlü İnternet olgusunun özellikle insana ve topluma dokunan sosyal yönüne ilişkin olarak doğurduğu risk ve tehditlerin insan ve toplum üzerinde meydana getirdiği etkiler ve bu risk ve tehditlere karşı birey, aile, toplum, devlet ve uluslararası sistem olarak neler yapılabileceğine ilişkin sorun alanlarının multidisipliner bir yaklaşımla, ilgili bütün disiplinlerin birikimlerinin bir araya getirildiği güvenilir, ciddi ve kapsamlı çalışmalarla ele alınması ve elde edilen veri ve sonuçlara göre strateji ve politikalar oluşturulması gerekmektedir. Ülkemizin ve belki de tüm insanlığın geleceğini belirleme noktasında önemli bir potansiyele sahip olan İnternet olgusunun bu bağlamı içinde değerlendirilmesi bir zorunluluktur.

Bu kapsamda, İnternetle ilgili olduğu için konuyu sadece teknik boyutunun sınırları içine hapsedip teknik elemanların ve mühendislerin/mühendislik biliminin sorunu olarak görme yanlışından kaçınmaya çalışarak; söz konusu teknik boyutu yanında sosyal, siyasal, ekonomik, yönetsel, hukuksal, eğitimsel, psikolojik, kültürel, uluslararası ilişkiler gibi birçok yönünün bulunduğu farkında olarak hareket etmek gerekmektedir. Bunun için, söz konusu alanlarla ilgili farklı disiplinlerdeki araştırmacıları bir araya getirecek ekip çalışmaları yapılmalıdır.

Dolayısıyla, başta ülkenin yükseköğrenim kurumları olmak üzere bütün ilgili kurum ve kuruluşların, bu yeni olgu ve sorunların arka planı ve gerçekliğini ortaya çıkarmak üzere inceleme ve araştırmalar yapılması konusunda seferber olması ve işbirliği içinde hareket etmesi sağlanmalıdır. Bu kapsamda, ergenlerin ve gençlerin dijital davranışları, İnternetin çocuk, genç ve yetişkin olarak insana, aileye ve topluma etkileri, taşıdığı riskler ve sunduğu imkanlar, sebep olduğu sorunlar; güvenlik ve içerik sorunları, müstehcenlik, çocuk istismarı ve pornografisi, fuhuş, şiddet, vahşet, ırkçılık, ayrımcılık, nefret, kumar, bahis, intihara yönlendirme, uyuşturucuya teşvik içerikleri, siber zorbalık, bilgi kirliliği, yabancılaşıma, mahremiyet ihlalleri, bağımlılık, dijital oyunlar, sosyal ağlar, İnternet kafeler, güvenli İnternet kullanımı, bilinçlendirme faaliyetleri, İnternet okuryazarlığı, İnternet etiği gibi bir çok konuda

ciddi ve kapsamlı çok sayıda alan arařtırmaları yapmak, dönemsel olarak bunları tekrar ederek sonuçlarını karşılařtırmak gerekmektedir. Keza, tüm bunlarla ilgili bir veri tabanı oluřturmalı ve bu veriler tüm arařtırmacıların istifadesine sunulmalıdır.

Nitekim, bu konularda ölkemizdeki literatür çok sınırlıdır. Arařtırmalar ve yayınlar çok az ve cılızdır. Bu nedenle, kamu-özel-STK-üniversite ilgili tüm kurum ve kuruluşları, yazar, çizer, akademisyen, düşünce adamı, sanatçı vb. kişiler, bu konularla ilgili arařtırma ve incelemeler yapma, arařtırma ve uygulama projeleri geliřtirme, enstitüler ve arařtırma merkezleri açma, düşünce ve fikir kulüpleri kurma, seminer, panel, çalıřtaylar düzenleme, raporlar, kitaplar, makaleler yayınlama, yazılı, sözlü, işitsel ve görsel sanat eserleri üretme konularında teşvik edilmeli ve desteklenmelidir.

3. İnternet Yönetişiminin Gerçekleştirilmesi

İnternetin teknik işlerliğinin devamını sağlamak yanında, kötüye kullanılmasının önlemesi tüm devletlerin aktif katılımını, uluslararası işbirliği ve koordinasyonu zorunlu kılmaktadır. Zira, İnternetin teknik özellikleri ve coğrafi sınırları aşan yapısı nedeniyle bu tip konularda devlet düzenlemeleri sorunları çözmede çoğu zaman yetersiz kalmakta ve ulusal düzeydeki politikaların geliştirilmesinde uluslararası yetki konularının dikkate alınması ve uluslararası işbirliği gerekmektedir. Yasadışı ve zararlı içeriklerle mücadelede kritik öneme haiz olan bu konuda sonuç alabilmenin ön koşulu ise, İnternetin tamamı üzerinde söz sahibi olan, İnterneti her yönü ve tüm aktörleri ile bütünlüğü içerisinde ele alacak ve uluslararası sahipliğini yapacak gerçek anlamada yetkili ve etkili bir uluslararası merkezi bir kuruluşun bulunmasıdır. İnternetin uluslararası yönetişimini hayata geçirecek bu örgütten içerik düzenlemelerinin çerçeve politikalarını belirlemesi ve sakıncalı içeriklerle ilgili uluslararası işbirliğinin olanaklarını ve mekanizmalarını oluřturması beklenmelidir.

Türkiye, devlet ve tüm İnternet güç ve aktörleriyle, İnternetin ABD hakimiyetinden kurtarılarak, İnternet yönetişimi temelinde ölkelerin ve kullanıcıların üzerinde söz sahibi olduđu bir yapı içinde, BM'e baėlı ITU çatısı altında görev yapacak

uluslararası bir örgüt marifetiyle yönetilmesinin sağlanması konusunda, başta BM olmak üzere diğer tüm ulusal, bölgesel ve uluslararası girişimleri desteklemeli ve bu yönde yapılacak olan tüm çalışmalara aktif katılım sağlamalıdır. Tıpkı BM Güvenlik Konseyi'nin daimi üyelerinin veto haklarıyla ortaya çıkan gayri adil durumu değişik ulusal ve uluslararası platformlarda yüksek sesle dillendirdiği gibi, İnternetin yönetimine ilişkin uluslararası meşruiyet sorununu her fırsatta dile getirmelidir.

4. İnternet İçerik Güvenliği İçin Özel Bütçe Oluşturulması

İnternetin sosyal boyutu, içerdiği risk ve tehditlerin tespit ve önlenmesi, yasadışı ve zararlı içerikle mücadele edilmesi, bilinçlendirme, İnternet okur-yazarlığı ve İnternet etiği çalışmalarının geliştirilmesi, ihbar ve yardım hatlarının kurulması ve işletilmesi, pozitif İnternet içeriği oluşturulması, araştırma-geliştirme çalışmaları, projelerin desteklenmesi, bilimsel yayın, ulusal ve uluslararası aktivitelerin desteklenmesi, STK'larının güçlendirilmesi, teşvik ve destek sağlanması gibi konularda yapılacak çalışma ve faaliyetlerde kullanılmak üzere ayrı bir bütçe oluşturulması gerekmektedir. Söz konusu bütçe, BTK ve İnternet sektöründeki işletmelerin yıllık gelirlerinin %2-3'ü gibi bir oranda katkı sağlamaları ile oluşturulabilir. Ayrıca, sektör işletmelerine verilen idari para cezalarının %25-30'luk bir kısmı bu bütçeye dahil edilebilir. Bahsi geçen bütçenin kullanılmasına ilişkin usul ve esasların belirlenmesi, uygulaması, takip ve denetimi yönetim ilkelerine uygun olarak İnterneti Geliştirme Kurulu tarafından TİB nezaretinde gerçekleştirilebilir.

5. Pozitif Yerli İçerik Oluşturulmasının Teşvik Edilmesi

İnternet içerik düzenlemeleriyle ilgili negatif yaklaşım yasadışı ve zararlı içeriklerin önlenmesidir. Ülkeler bunu temin etmek için erişim engellemesi ve filtreleme, uyar-kaldır, büyük içerik sağlayıcılarla özel anlaşmalar yapma, bilinçlendirme ve İnternet etiği anlayışının yaygınlaştırılmasına yönelik faaliyetler gerçekleştirmektedir. İçerik düzenlemesiyle ilgili yeterince üzerinde durulmayan pozitif yaklaşım ise, pozitif içeriğin artırılması ve çoğaltılmasıdır.

Aslında, yasadışı ve zararlı içeriğin önlenmesine yönelik içerik düzenlemeleri ne kadar önemli ve bir o kadar antipatik ise, aynı amacı gerçekleştirmeye matuf pozitif içerik oluşturulmasını özendirmeye yönelik içerik düzenlemeleri en az onun kadar önemli ve sempattır. Keza, İnternetin kendine özgü dağıtık ve dinamik yapısından dolayı yasadışı ve zararlı içeriklerin önlenmesi maliyetli, zor ve kesin sonuç almaya uygun değilse, pozitif içerik oluşturulması daha az maliyetli ve çok daha kolaydır. O halde, İnternet içerik düzenlemesine ilişkin stratejide, yasadışı ve zararlı içerikle mücadele yanında pozitif içerik oluşturulması yaklaşımına da yer vermek gerekmektedir. Bu iki yaklaşım birbirinin alternatifi değil, birbirini tamamlayıcı iki unsur olarak görülmelidir.

O halde, ülkemizde yerli pozitif içerik üretmeyi özendirecek düzenlemeler yapmak gerekmektedir. Bu kapsamda, ilk olarak ilgili mevzuat geliştirilmelidir. Bu bağlamda öncelik, ilgili mevzuatta özel olarak İnternet içerik sağlayıcılığına yönelik düzenlemeler yapılmasına verilmelidir. BTK ve TİB mevzuatı bu yönüyle revize edilerek Türkiye’de içerik sağlayıcılık ayrı bir İnternet hizmeti ve işletmecilik tipi olarak hukuki bir statüye kavuşturulmalıdır.

Söz konusu mevzuat ile, ülkedeki İnternet kullanıcılarını küresel içerik sağlayıcılara (Facebook, Google, Youtube, Twitter gibi) mahkum olmaktan kurtarmak için içerik sağlayıcılığını ve özellikle pozitif içerik üretilmesine yönelik teşvik edici düzenlemeler yapılmalıdır. Bu kapsamda başta yerli arama motoru olmak üzere, sosyal paylaşım ve video siteleriyle e-posta sağlayıcıların yaygınlaştırılması desteklenmeli, bu türden içerik ve uygulama üretecek işletmelere enerji ve diğer altyapı maliyetlerine kolaylıklar ile vergi teşvikleri getirilmeli, büyük projelere devlet desteği sağlanmalıdır.

Bunun yanında, bahsi geçen mevzuat ile özellikle, sakıncalı içeriklerden korumaya çalıştığımız çocuklara ve gençlere yönelik olarak, onlara cazip gelecek, faydalı olacak, eğlendirirken eğitecek web sitelerini, web sayfalarını ve uygulamaları çoğaltmak için teşvik edici ve destekleyici tedbirler geliştirilmelidir.

Bu kapsamda, yayınlanacak genelgeler ile belirli kurum ve kuruluşlara pozitif içerik oluşturulmasıyla ilgili bazı zorunluluklar getirilebilir. Örneğin, bir Başbakanlık genelgesi ile web sitesi bulunma zorunluluğu olan kamu/özel/STK tüm kurum ve kuruluşların çocukla başlayan bir alt alan adı oluşturmaları ve çocuk web sayfası düzenlemeleri sağlanabilir. Bu çocuk web sayfasında ilgili kurum veya kuruluş yaptığı işle, verdiği hizmetle ve hizmet sunduğu alanla ilgili bilgileri daha görsel, kolay, sade, basit ve pratik bir şekilde çocukların anlayabileceği ve onların ilgisini çekecek bir tarzda sunabilir, bunlarla ilgili uygulamalar geliştirebilir. Hatta, çocuklara yönelik hizmet verebilme imkanları varsa, bunu söz konusu uygulamalarla temin edebilirler. Keza, faaliyet alanı ile ilgili olsun veya olmasın pozitif içerik barındıran diğer web adreslerine bağlantı linkleri koyabilirler.

Bunun yanında, mevzuat uygun hale getirilerek BTK'nın denetiminde belirli büyüklükteki içerik, yer ve erişim sağlayıcılar ile telefon işletmecilerine çocuk arama motoru yapma ve hizmete sunma yükümlülüğü getirilebilir. Keza, bu hizmet teşvik kapsamına alınabilir.

Benzer şekilde, yine bir Başbakanlık genelgesi ile kamu kurum ve kuruluşlarının kamuya açıklanmasında sakınca bulunmayan bilgi, veri, istatistik, araştırma, inceleme ve raporlarını İnternet siteleri üzerinden kullanıcılarla paylaşmaları sağlanabilir. Yine, kamu kurum ve kuruluşları görev alanları ile ilgili olarak yurtiçi ve yurtdışında yapılmış ve üretilmiş olan araştırma, bilimsel çalışma, yayın, rapor, işitsel ve görsel yararlı dokümanları resmi web sitelerinde yayınlamaya teşvik edilebilir. Örneğin, her kamu kurum ve kuruluşuna web sitesinde e-kütüphane hizmeti sunma mecburiyeti getirilebilir.

Ayrıca, bir nebze de olsa bilgi kirliliğinin önlenmesi için MEB tarafından ansiklopedik bilgi içeren ve bu bilgilerin sürekli güncellendiği resmi bir İnternet sitesinin hazırlanması temin edilebilir.

Diğer yandan, yerli pozitif içeriğin geliştirilmesi, İnternetin yerel ayağının güçlendirilmesi politikasının bir parçası görülmelidir. Bu politikanın diğer parçaları

ise; batılı teknolojilere bağımlılığı zayıflık kaynağı ve İnternet kullanımı için bir potansiyel güvenlik açığı olarak görerek, yerli teknolojinin, ürünlerin ve teknik kapasitenin geliştirilmesini teşvik etmektir. Bu kapsamda, yabancı menşeli filtreleme teknolojilerine olan bağımlılığı azaltarak, sakıncalı Web sitelerini tanımlamak ve engellemek için yurtiçinde üretilen filtreleme teknolojilerinin geliştirilmesi ve kullanımının artırılması da önem taşımaktadır.

6. Bilinçlendirme Çalışmalarının Artırılması

Çocukların, gençlerin, ebeveynlerin ve eğitimcilerin İnternetin doğru kullanımı konusunda farkındalıklarının arttırılması sağlanmalıdır. Ana-babalar ile eğitimciler özellikle sosyal ağlarda karşılaşılabilecek riskler ve önlemler konusunda öğrencilerini bilinçlendirmelidir. Bu kapsamda, Türkiye’de var olan İnternetin bilinçli, güvenli ve etkin kullanımına yönelik çalışmaların, ilgili tüm kurum ve kuruluşları, STK’ları ve özel sektörü içerecek şekilde geliştirilmesi, işbirliği ve koordinasyonun sağlanması gerekmektedir. Bu çalışmalarda özellikle çocukların ve gençlerin görüşlerine başvurulması faydalı olacaktır. Bu nedenle, bunu temin edecek “danışma kurulu” benzeri mekanizmalar oluşturulmalıdır.

Söz konusu çalışmaları koordine etmek üzere AB ülkelerinde ve diğer birçok ülkede olduğu gibi TİB İnternet Dairesi’nin nezaretinde, İnternetin güvenli kullanımı konusunda çalışan STK’lar ile ortaklaşa Güvenli İnternet Merkezi kurulmalıdır. Türkiye’deki bilinçlendirmeye dair tüm çalışmalar ve hizmetler buradan yönlendirilmelidir. Bu merkez tarafından, “İnternet İçerik Güvenliği Stratejisi ve Eylem Planı Belgesi”ni esas alan yıllık “İnternetin Bilinçli Kullanımı Programları” hazırlanmalı ve uygulanması takip edilmelidir.

Bu programlar çerçevesinde, bilinçli, güvenli ve etkin İnternet kullanımının geliştirilmesi için yapılan çalışmalar, yayınlar, kampanyalar, haberler, eğitim programları ilgili kamu kurumlarınca açıkça desteklenmeli ve teşvik edilmelidir. Bu konuda ilgili her kurum ve kuruluş üzerine düşen görevi yapmalı, özellikle STK’ları ve özel sektör kuruluşları özendirilmeli ve desteklenmelidir. Keza, konu ile ilgili

kamu-özel-STK tüm paydaşların işbirliği içerisinde çalışmalar yapması, projeler üretmeleri, ulusal ve uluslararası proje fonlarından faydalanarak büyük ve etkili projeleri hayata geçirmeleri sağlanmalıdır.

Bu kapsamda, AB Güvenli İnternet Programı'na ve dolayısıyla, her yıl düzenlenen Güvenli İnternet Forumu ve Güvenli İnternet Günü faaliyetlerine aktif katılım sağlanmalıdır. Yine, ITU'nun çocukların İnternet ortamında korunması amacıyla başlatmış olduğu COP girişiminde yer alınmalıdır. Söz konusu işbirliklerinde güçlü bir sivil toplum ayağının bulunmasına dikkat edilmelidir.

Bu konuda özellikle Aile ve Sosyal Politikalar Bakanlığı, MEB ve BTK aktif tutum sergilemeli; oluşturacakları proje destek birimleri ile kamu ve STK ortak projelerine veya STK projelerine maddi destek sağlamalıdır.

Bilinçlendirme konusunda en büyük görev, eğitimcilere; öğretmenlere ve ailelere düşmektedir. Bu yüzden bilinçlendirme çalışmalarında eğitimcilerin eğitimi öncelikli amaç olarak görülmelidir. Bu konuda FATİH projesi çok önemli bir adım ve imkandır. Proje kapsamında 17 milyon tablet dağıtımı yapılacaktır. Bu İnternet erişimini zıplatacaktır. Kullanıcının bunu nasıl değerlendireceği, hangi amaçla ve hangi içeriğe ulaşacağı önem taşımaktadır. Proje müthiş imkanlar sunarken, risk tarafını da aynı oranda büyütmektedir. Proje'nin en önemli ayaklarından birisini de İnternetin güveni, bilinçli ve etkin kullanımına yönelik farkındalık çalışmaları ve eğitim programları oluşturmalıdır.

Dijital vatandaşlık bilincinin toplumda oluşturulması ve yaygınlaştırılması gerekmektedir. Bu kapsamda İnternet okuryazarlığı eksikliğinin MEB, üniversiteler ve diğer eğitim kurumları ve STK'ların işbirliği ile giderilmesine yönelik çalışmalar yapılmalıdır. Bu çerçevede, "Medya okuryazarlığı" ve "Bilgisayar" dersleri müfredatı gözden geçirilmeli ve çocukların ve gençlerin medyanın olası zararlı etkilerinden korunması ve bilinçli İnternet kullanımı konularını da kapsayacak şekilde yeniden düzenlenmesi gerekmektedir. Bu içeriği ile, "Medya okuryazarlığı"

dersi ilkököl, ortaokul ve lisede zorunlu ders olarak okutulmalıdır. Ayrıca, ortaokul ve lise düzeyinde seçmeli olarak “Güvenli İnternet Kullanımı” dersi sunulmalıdır.

Okullar dışında da tüm kullanıcılara yönelik olarak medya/bilişim/teknoloji okuryazarlığını geliştirecek çözümler üretilmesi gerekmektedir. Bu tür eğitimler ebeveynler ve öğretmenler başta olmak üzere toplumun her kesiminde yaygınlaştırılmalı; okullarda ve STK’larda çocuklara ve ailelere bu konuda eğitimler verilmeli, bu eğitimlerde özellikle çocukların sakıncalı içeriklerden uzak tutulabilmesi amacıyla ebeveynler bilinçlendirilmelidir.

Keza, medyanın, genel olarak bilgi ve iletişim teknolojilerinin kullanımına, özel olarak ise, İnternete ilişkin olanakları ve riskleri dengeli bir şekilde sunması ve söz konusu bilinçlendirme faaliyetlerine etkin bir şekilde katılımı sağlanmalıdır.

7. Küresel Şirketler İle Özel Anlaşmalar Yapma

İnternetin çok aktörlü, dağıtık ve dinamik yapısı ülkelerin tek başına İnterneti ve dolayısıyla İnternet içeriğini kontrol altına almasını mümkün kılmadığı gibi, ülkelerin farklı kültürel kodları ve önemsedikleri suçlar, farklı yerel yasaları, karmaşık mevzuatlar, farklı çıkar hesapları ve siyasi ve ekonomik dengeler, dağıntık uluslararası yapılar bu konularda işbirliğini ve ortak politika belirlemeyi önemli ölçüde zorlaştırmaktadır.

Bütün bunların yanında, Web 2.0 uygulaması interaktiviteyi ve bu çerçevede farklı içeriklerin aynı konseptlerde toplanmasını sağlamış; Facebook ve Twitter gibi adeta her birisi İnternetin büyük bir kısmını yutan kendi özelinde “İnternetler” oluşturmuş ve dolayısıyla teknik ve yönetsel olarak kontrolü ve denetimi giderek çok daha zor uygulamalar meydana getirmiştir. Keza, devlet eli ile yapılan yasal düzenleme ve denetimlerin bu teknik sebeplerden dolayı çoğu zaman yetersiz kaldığı, öz düzenleme ve denetimlerin ise ekonomik çıkarlar devreye girdiğinde nasıl sulandırıldığı bilinmektedir. Bilinçlendirme çalışmaları ise, uzun soluklu ve etkinliği tartışmalı bir yöntemdir.

Bu durumda, devletler açısından İnternet içeriğinin ve uygulamalarının büyük kısmını oluşturan ve adeta İnterneti kendisinde toplayan Facebook, Google, Youtube, Twitter gibi büyük İnternet platformları ile işbirliği geliştirmek temel bir ihtiyaç olarak ortaya çıkmaktadır. Özellikle, yer sağlayıcılığı hizmetleri ve içerik üretiminin büyük ölçüde yurt dışı kaynaklı olduğu Türkiye gibi ülkelerde bu ihtiyaç daha fazla kendisini göstermektedir. Nitekim, dünyadaki yeni trend devletler ile bu büyük İnternet platformları arasında özel işbirliği anlaşmalarının yapılması yönündedir.

Nitekim, AB, ABD, Almanya, İngiltere, Brezilya gibi ülkeler sakıncalı içeriklerin engellenmesi konularında bu firmalarla özel işbirliği anlaşmaları yapmışlardır. Çin'in öteden beri bu tür işbirlikleri geliştirdiği bilinmektedir. Dolayısıyla, Türkiye'nin de benzer bir strateji ile hareket ederek, kullanımları ülkemizde oldukça üst düzeylerde olan bahsi geçen İnternet platformlarıyla özel anlaşmalar yapma yoluna gitmesi ve bu firmaları işbirliğine zorlaması gerekmektedir.

Her ne kadar söz konusu büyük İnternet platformları önemli bir çıkar kaybı veya kazancı görmedikleri sürece çoğu zaman devletlerden gelen bu tür özel anlaşmalar yapma veya işbirliği geliştirme taleplerini geri çevirseler veya cevapsız bıraksalar da, Türkiye, ekonomik ve siyasi olarak sahip olduğu tüm potansiyeli ve gücü kullanarak, ince bir ayar, akılcıca bir siyasetle ve kazan/kazan taktiği ile bir şekilde bu firmalar ile anlaşma ve işbirliğine razı etme yolu bulmalıdır. Çünkü, günümüzde yasadışı ve zararlı içerikle mücadelenin en etkili ve kestirme yolu bu gözükmektedir.

8. Erişim Engelleme Politikasının Gözden Geçirilmesi

Yasadışı ve zararlı içeriğin önlenmesine yönelik erişim engellemeye ilişkin uygulama belirli bir sistematik dahilinde gerçekleştirilmelidir. Öncelikle, erişim engellemeye konu suç türleri belirli ve oldukça sınırlı tutulmalıdır. Keza, erişim engelleme son çare olarak uygulanmalıdır. Öncesinde, uyar-kaldır mekanizmaları, öz düzenleme uygulamaları, özel anlaşma ve işbirliği geliştirme, yaş doğrulama benzeri önleyici tedbirler, tüketici tercihi dayalı alternatifli içerik sunumları gibi erişim engellemesi tedbiri almayı gereksiz kılacak doğrudan veya dolaylı içerik

düzenlemesi enstrümanları devreye sokulmalıdır. Erişim engellemesi kararının uygulanması kaçınılmaz ise, bu durumda ifade ve bilgiye erişim özgürlüğünü zedelemeyecek şekilde “orantılılık”, “ölçülülük” ve “suçun şahsiliği” ilkelerine uygun hareket edilmelidir.

Türkiye’deki erişim engellemesi uygulamaları incelendiğinde, 5651 sayılı Yasa’nın ana hatlarıyla, bu sistematığe uygun bir erişim engellemesi düzeni öngördüğü söylenebilir. Yasa’nın uygulaması bu sistematik bakımından değerlendirildiğinde ise, genel olarak eleştirilere konu olan sorunun alan adı ve IP engellemesinden kaynaklandığı görülmektedir. 5651 sayılı Yasa dışındaki erişim engellemelerinin bu sistematik açısından en zayıf noktası ise, engelleme uygulamalarının TİB’nin kontrolü dışında doğrudan İSS’lar üzerinden yapılması nedeniyle uyar-kaldır benzeri erişim engellemeyi önleyici mekanizmaların işletilmesine olanak vermemesidir.

O halde, erişim engellemelerine ilişkin sürecin daha demokratik ve eleştirileri en aza indirecek bir sistematik ile yürütülmesi açısından bazı hususlara dikkat edilmelidir. Birinci husus, erişim engellemesine konu katalog suçlarının çocukların, gençlerin ve ailelerin yasadışı ve zararlı İnternet içeriğinden korunması amacına yönelik mevcut konseptinin korunarak belirli ve sınırlı niteliğinin muhafaza edilmesidir. Dolayısıyla, özellikle bu konseptin dışına çıkmaya neden olabilecek ve uygulamada ifade ve bilgiye erişim özgürlüğü bağlamında eleştiri ve tartışmalara neden olabilecek yeni katalog suçları ihdas etmekten kaçınılmalıdır. Keza, daha etkin mücadele gerektiren yasadışı her tür İnternet içeriğini, bu konseptte uygunluğunu göz önünde bulundurmadan katalog suçlarına dahil etme kolaycılığına kaçılmamalıdır. Bu tür bir yaklaşımın mevcut katalog suçlarıyla mücadelenin meşruluğuna ve haklılığına halel getireceği, işleri daha da karmaşık ve içinden çıkılmaz bir hale getireceği unutulmamalıdır. Bunun yerine, zaman içerisinde daha etkin mücadeleyi gerekli kılan diğer yasadışı İnternet içeriklerinin ilgili mevzuatlarını güncelleyerek ve güçlendirerek sonuç almaya çalışmak daha doğru bir yöntem olacaktır.

Bu çerçevede, bazı çevrelerin ırkçılık, ayrımcılık ve nefret suçlarının katalog suçları kapsamına alınması yönündeki önerilerini isabetsiz görmekteyiz. Zira, bu içeriklerin

katalog suçları kapsamına alınarak sonu erişim engellemelerine giden bir kapının açılması Türkiye’de çok büyük siyasal ve sosyal tartışma, çatışma ve çalkantılara neden olacaktır. Bu durumda, birçoğunun akisleri uluslararası kamuoyunda görülecek anti semitizm, Ermeni düşmanlığı, İslamifobia, din düşmanlığı ve kutsal değerlere hakaret tartışmaları, farklı dinden ve mezhepten azınlık topluluklarına ve etnik gruplara yönelik söylemler, Kürt sorunu ve Alevilik meselesi, cinsiyet ayrımcılığı, eşcinsellik ve cinsel tercihlere yönelik eleştiri ve tartışmalar patlama yapacaktır. “Sansür”, “yasaklar”, “erişim engellemeleri” kelimelerinin sıkça dile getirileceği bu ortamda tüm bu tartışma ve eleştirilerin odağında 5651 sayılı Yasa ve TİB olacaktır. Dolayısıyla, tıpkı Youtube konusunda olduğu gibi, Türkiye’nin yasadışı ve zararlı içeriğe karşı yürüttüğü haklı mücadele zarar görecektir.

Hatta, yeni katalog suçları eklemek yerine süreç içerisinde uygulamalardan elde edilen sonuçlar ve AIHM’nin mevcut suçlara ilişkin erişim engellemeleri kararlarına göre katalog suçlarının tekrar gözden geçirilmesi ve azaltılmaya çalışılması düşünülmelidir. Nitekim, bu değerlendirmeler sonucunda çocukların, gençlerin ve ailenin korunması konseptine tam olarak uymadığı gibi ulaşılmak istenen sonuçlara hizmet etmeyen ve ifade özgürlüğü ve bilgiye erişim özgürlüğü konusunda uluslararası camiada Türkiye’yi zor durumda bıraktığı görülen ya da katalog suçları arasında bulunmakla birlikte, zaman içerisinde zararları konusunda etkisini ve güncelliğini yitiren suç türlerinin katalog suçlarından çıkartılması gerekmektedir. Zira, söz konusu suç türleri ne kadar az ve sınırlı olur ise, yasadışı ve zararlı içeriğe karşı verilen mücadelenin meşruiyeti ve haklılığı o kadar güçlü olacaktır.

Erişim engellemelerine ilişkin süreci daha demokratik kılacak ikinci husus ise, TİB’in erişim engellemelerinde kullandığı yöntemle ilgilidir. TİB, hakkında erişim engellemesi kararı bulunan ve uyar-kaldır yöntemiyle yayından kaldırılmasını sağlayamadığı yasadışı ve zararlı İnternet içeriğine erişim engellemesi uygularken söz konusu içeriğin niteliğine göre belirli bir sistematik içinde hareket etmelidir. Buna göre, herhangi bir IP veya alan adının tamamında yasadışı veya zararlı içerik bulunmuyorsa IP’den veya alan adından erişim engellemesi yapmamalıdır. Yani, IP’den veya alan adından engelleme, söz konusu IP veya alan adının tamamının

yasadışı ve zararlı içerik barındırılması durumunda uygulanmalıdır. Aksi takdirde, her halükarda URL üzerinden engelleme yöntemi tercih edilmelidir. Bu yöntem ifade ve bilgiye erişim özgürlüğünü zedelemeyecek şekilde “orantılılık”, “ölçülülük” ve “suçun şahsiliği” ilkelerine uygun hareket edilmesini temin edecektir.

Türkiye’deki erişim engelleme karar ve uygulamalarını daha demokratik hale getirecek diğer bir husus ise, erişim engellemesi kararını hangi mercii ne sebeple verirse versin erişim engellemesi uygulamasının TİB üzerinden yapılmasının sağlanmasıdır. Zira, 5651 sayılı Yasa kapsamı dışında değişik mevzuatlara göre mahkemelerce verilen erişim engellemesi kararlarının doğrudan İSS’lara gönderilmesi, söz konusu kararın uygulanması öncesinde TİB’inca uyar-kaldır mekanizmalarının işletilmesi olanağını ortadan kaldırmaktadır. Dolayısıyla, son çare olarak uygulanması gereken erişim engellemesi kararları TİB’nin bilgisi dışında hemen uygulamaya geçirilmiş olmaktadır. Bu sakıncanın ortadan kaldırılması ve uygulama birliğinin sağlanması açısından 5651 sayılı Yasa kapsamında olsun veya olmasın tüm erişim engellemesi kararlarının uyar-kaldır sisteminden geçmesini sağlamak adına TİB’na gönderilmesi gerekmektedir.

9. Öz Düzenleme Uygulamalarının Teşvik Edilmesi

Türkiye’de de dünyadaki trende paralel olarak, İnternetin tüm özel sektör aktörlerinin öz düzenleme ve denetim mekanizmalarını kurması, işletmesi ve bu yönde çaba ve gayret göstermesini sağlamaya çalışmak İnternet içerik politikalarımızın önceliklerinden birisi olmalıdır.

Kuşkusuz, Türkiye’de de yasadışı ve zararlı İnternet içeriği ile mücadele açısından; Almanya’daki içerik sağlayan/üreten şirketlerin çoğunun üyesi olduğu ve yasadışı içerik sağlamayacaklarına/ üretmeyeceklerine ve Derneğin kurallarına uyacaklarına dair bir anlaşma imzalayarak bunların uygulanmasını denetlemekte olan FSM, Fransa’daki hem öz düzenleme yaklaşımını hayata geçirmeye çalışan hem de bu yaklaşımın sektörde geliştirilmesi ve uygulamalarının artırılması yönünde faaliyet gösteren DYY, Japonya’daki sektör temsilcilerinin kurduğu öz denetim kuruluşu

olan ve özellikle güvenli İnternet ve İnternet etiği, filtreleme bilincinin geliştirilmesi gibi konularda araştırmalar ve eğitim çalışmaları yapan IAJ benzeri güçlü ve başarılı öz düzenleme kuruluşlarının varlığı gerekli ve önemlidir.

Keza, AB üyesi devletlerin interaktif oyun üreticilerinin gönüllü olarak kurdukları ve bütçesi üye aidatları ile karşılanan ve oyun derecelendirme ve sınıflandırma sistemi geliştiren PEGI, benzer şekilde, ABD’de de dijital oyun pazarındaki önemli şirketler tarafından kurulan ve oyun sektöründe önemli öz düzenleme uygulamaları geliştiren ESRB ülkemiz açısından incelenmesi gereken örneklerdir.

Yani, Türkiye’nin yasadışı ve zararlı İnternet içeriği ile mücadele konusunda öz düzenleme yaklaşımını ciddiye alan, samimiyetle bu tür uygulamaları hayata geçirmeye çalışan, etkin bir oto-kontrol öngören, işbirliğine açık, piyasanın hakim şirketlerinin de içinde yer aldığı güçlü içerik, yer ve servis sağlayıcı, sosyal ağ ve mobil operatör derneklerine ihtiyacı bulunmaktadır.

Diğer yandan, dünyadaki örneklerde görüldüğü gibi özel sektör kuruluşları çoğunlukla bu tür öz düzenleme girişimlerini ticari kaygılarla kendiliğinden gönüllülük anlayışı içinde uygulamaya geçirmeye çok fazla yanaşmamaktadır. Bu nedenle, birçok ülkede bu tür girişimler kamu otoritesinin destek, ikna ve yer yer zorlaması ile gündeme gelmekte ve uygulama alanı bulmaktadır.

Dolayısıyla, ülkemizde de içerik, yer ve servis sağlayıcılar, sosyal ağlar ve mobil operatörler gibi İnternet sektöründeki aktörlerin öz düzenleme ve denetim girişimlerinde bulunmaları, politika oluşturma, iç kontrol, kural, standart ve prensipler belirlemelerini ve uygulamalarını sağlamak için devlet desteği, yönlendirmesi ve bazen zorlaması gerekmektedir. Bu çerçevede, özellikle bu konu etrafında çalışmayı görev edinen özel sektöre ait STK’larının oluşturulmasına, öz düzenleme uygulamalarının geliştirilmesine hem kamusal hem de özel sektör desteği sağlanmalı ve toplum yararına projeler üretmeleri teşvik edilmelidir.

Yine, söz konusu öz düzenleme kuruluşlarının oto-kontrole dayalı düzenleme, uygulama ve denetimlerinin baskın bir şekilde ticari yaklaşımla değerlendirildiği ve

özel sektör işletmelerini harekete geçiren asli unsurun “kar” saiki olduğu unutulmamalıdır. Zira, örgütsel olarak nihai amacı İnternet piyasasını güçlendirmek ve daha çok para kazanılan bir yer haline getirmek olan meslek kuruluşlarından gönüllü olarak “İnternetin zararları” konusunda girişimde bulunmalarını beklemek çokta gerçekçi olmayacaktır.

Bu nedenle, özel sektörün ve onların temsilcisi olan öz düzenleme kuruluşlarının, İnternetin güvenli bir ortam haline getirilmesinin kendilerine daha fazla ekonomik getiri sağlayacağına ve bu mücadele sürecinde güvenlik ve filtreleme programları benzeri ürünlerden yeni gelir kaynakları elde edeceklerine ikna olmalarıyla sonuç alınabilecektir. Dolayısıyla, öz düzenleme kuruluşlarını kendi haline bırakmak ve onların belirleyeceği her nevi kural, standart ve değer yargısına piyasayı ve kullanıcıları teslim etmek doğru olmayacaktır. Sonuç olarak, öz düzenleme kuruluşlarının kamu otoritelerince akredite edilmesi, suistimallerin önlenmesi, kontrol ve denetiminin sağlanması dikkate alınması gereken bir konudur.

Diğer yandan, İnternetin ulusal sınırları aşan niteliği ve dolayısıyla yasadışı ve zararlı içerik ile mücadelede uluslararası işbirliği ve tecrübe paylaşımının gerekliliği de dikkate alınarak; uluslararası düzeyde ve hatta küresel boyutta öz düzenleme ve denetim girişimlerine, örgütlerine ve uygulamalarına ihtiyaç olduğu da bir gerçektir. Bu nedenle, hem ulus devletlerin hem de uluslararası sistemin bu tür uluslar üstü öz düzenleme arayışlarını desteklemesi ve teşvik etmesi önem taşımaktadır.

10. İnternet STK’larının Güçlendirilmesi

İnternetin sebep olduğu risk ve tehditlerin birlikte yönetim yaklaşımıyla bertaraf edilmesinde beklenen faydanın sağlanabilmesinin şartlarından birisi de denklemin STK tarafında güçlü kurumsal yapıların bulunmasıdır. Bu yapılar, hem özel sektör işletmelerini temsil eden meslek örgütleri, hem de içerisinde İnternet kullanıcıları ve tüketicilerinde bulunduğu tüm sivil toplumun temsilcisi olan örgütler bakımından bir gerekliliktir. Ama, ülkemizde özellikle başta kullanıcı ve tüketiciler olmak üzere toplumun değişik katmanlarını temsil eden, onların istek, beklenti ve menfaatlerini

savunan güçlü ve iyi organize olmuş dernek, vakıf vb. kar amacı gütmeyen kurum ve kuruluşlara duyulan ihtiyaç daha fazla kendisini hissettirmektedir.

Çünkü, genellikle, konunun tarafı olan STK'lerden sektör firmalarını temsil eden örgütler, tüm dünyada olduğu gibi, ekonomik ve siyasi güçlerini kullanarak daha kolay organize olmakta, etkin ve güçlü kurumsal yapılar oluşturmakta ve dolayısıyla çıkar ve menfaatlerini daha güçlü bir şekilde savunabilmektedir. Nitekim, Türkiye'de de mevcut durum bu yöndedir. STK'ların, ülke nüfusunun büyük çoğunluğunu oluşturan ve bunların yine büyük bölümü kullanıcı ve tüketici konumunda olan çocuklar ve gençlerden oluşan sivil toplumu temsil eden tarafında ise nitelik ve nicelik olarak bariz bir yetersizlik söz konusudur. Yani, denklemin sivil toplum kanadında önemli bir zayıflık ve eksiklik bulunmaktadır.

Bu durum, biraz da ülkemizdeki güçlü bir sivil toplum geleneğinin ve kültürünün gelişmemiş olmasından kaynaklanmaktadır. Az da olsa var olanlar ise, çok çabuk siyasallaşmakta ve farklı ideolojik angajmanlara teslim olmakta veya kısa sürede temsil ettiği kesimler yerine yöneticiler ve yakın çevrelerinin kişisel çıkarlarına hizmet eden küçük grupların eline geçmektedir. Dolayısıyla, ülkemizde çoğu zaman, gerçek anlamda sivil toplumu temsil eden ve sadece temsil ettiği toplumsal kesimlerin menfaatlerini savunan bir STK pratiği tam olarak gelişmemiştir.

Hal böyle olunca, sivil toplum adına İnternetin özellikle toplumsal risklerine ve tehditlerine dikkat çekecek, bununla ilgili sorunları, istek ve talepleri güçlü bir şekilde dile getirecek ve bu sorunların çözümü konusunda inisiyatif alarak birlikte yönetim süreçlerinde söz sahibi olabilecek yeterlikte ve yetkinlikte STK'larımız ortaya çıkmamıştır.

Bu nedenle, İnternet içerik düzenlemesine ilişkin süreçlerde birlikte yönetim yaklaşımının sağlıklı bir şekilde işletilebilmesi için bu denklemin içinde yer alan STK tarafının bu boyutu ile güçlendirilmeye ve geliştirilmeye ihtiyacı vardır. Bu amaçla, bir devlet politikası olarak İnternetin bilinçli, etkin ve güvenli kullanımı konularında çalışmalar yapmak isteyen STK'ları teşvik edilmeli, bütçe ve proje

desteđi verilmelidir. Bu kapsamda BTK bütçesinde münhasıran bu konuya özel ayrı bir harcama kalemi oluşturulabilir.

Hasılı, Türkiye'nin en kısa sürede, birlikte yönetim modeli içinde masanın STK tarafında yer alabilecek bütçe, örgütsel yapı ve etkinlik boyutları ile yeterli, sağlam ve güçlü, güvenilirliği ve bilinirliği yüksek vakıf veya derneklere ihtiyacı bulunmaktadır. İngiltere'deki IWF, Brezilya'daki SaferNet Brasil benzeri bir örgüt olacak bu STK, kısa zamanda geliştireceđi uluslararası işbirliği çalışmalarıyla yurtdışında da tanınan ve bilinen bir kuruluş haline gelmeli ve getirilmelidir.

11. Yer Sağlayıcılığın Geliştirilmesi ve Kayıt Altına Alınması

İnternet içerik düzenlemesi konusuyla ilgili olarak yerli içerik üretiminin özendirilmesini tamamlayıcı diğerk bir İnternet politikası da ülkemizde barındırma ve yer sağlayıcılığı hizmetinin gelişmesini sağlamak ve içerik sağlayıcılığı hizmeti veren kişi ve şirketleri kayıt altına almaktır. Çünkü, yasadışı ve zararlı içerikler ile mücadelede yasadışı içeriklerin çoğunun yurtdışında barındırıldığı görülmektedir ve bu durum söz konusu içerikler ile mücadeleyi zorlaştırmaktadır.

Yerli veya yabancı menşeli İnternet içeriklerinin yurtdışında barındırılmasının ana sebebi yurtdışına oranla Türkiye'de yer sağlama hizmetlerinin daha pahalı olmasıdır. Bu fiyat pahalılığı da ağır vergi yükü ve enerji fiyatlarından kaynaklanmaktadır. Türkiye, üretilen yerli içeriğin yurt içinde tutulabilmesi, yurt dışında üretilen içeriğin ülkemizde barındırılması ve yurt dışında faaliyet gösteren şirketlerin de barındırma hizmetlerini Türkiye'den sağlamayı tercih etmesi için yer sağlayıcılığını teşvik etmeli, barındırma ve yer sağlayıcılığı hizmeti sunan şirketlere gereken güvenli ve cazip ortamı oluşturmalıdır. Bunun için ihtiyaç duyulan enerji ve diğerk altyapı maliyetlerinin azaltılması ve yer sağlayıcılığı hizmetlerinden alınan vergilerin düşürülmesi yanında, Kişisel Verilerin Korunmasına İlişkin Kanun'un bir an önce yasalaştırılması gerekmektedir. Bunun yanında, kamu kurum ve kuruluşlarının içeriklerinin yurt içinde tutulması zorunlu hale getirilebilir.

Diğer yandan, yer sağlayıcıların kayıt altına alınarak yasadışı ve zararlı içerikle mücadeleyi öngören 5651 sayılı Yasa ile getirilen hukuki düzene yeterince işlerlik kazandırılmadığı; az sayıdaki yer sağlayıcının faaliyet belgesi aldığı, belge alanların da iletişim bilgileri değişikliklerini düzenli bir şekilde bildirmediğinden acil bir içerik çıkarma durumunda çaresiz kalındığı görülmektedir. Yer sağlayıcıların tamamının faaliyet belgesi almasını ve iletişim bilgilerini düzenli olarak güncellemelerini sağlamak için konuyla ilgili caydırıcı bir ceza sistemi bulunmalı ve uygulanmalıdır.

12. Yaş Doğrulama Uygulamasının Genişletilmesi

Çocukların İnternette yer alan zararlı içeriklerden korunması için birçok ülke tarafından uygulanan, bu tür içeriklere erişim için yaş doğrulaması mekanizmalarının kullanılmasına ilişkin önleyici tedbirlerin alınmasına ülkemizde de öncelik verilmelidir. Buna göre, özellikle ülkemizde 18 yaşından küçük çocukların erişiminin suç olduğu müstehcen içerikle ilgili olarak sektörün kendi belirleyeceği mekanizmalarla yaş kontrollerine benzer önleyici tedbirlerin alınması zorunlu hale getirilmelidir. Bu kapsamda günümüzde kullanıcıların yaşını doğrulamak için kredi kartları, kimlik kartları ve hatta yüz-yüze doğrulamayı içeren yöntemler uygulanabilmektedir.

Bunlar içerisinde kuşkusuz en güvenilir olanı, Almanya ve İngiltere’de de yaygın olarak kullanılan yüz yüze yaş doğrulama sistemidir. Benzer bir yöntem ülkemiz için de kullanılabilir gözükmektedir. Keza, Güvenli İnternet Hizmeti’nin de kısmen benzer bir işlev gördüğü söylenebilir. Fakat, bu uygulamada müstehcenlik açısından yetersiz olan bir yön bulunmaktadır. Şöyle ki, abone talepte bulunmadığı müddetçe geçerli olan profil müstehcenlik açısından herhangi bir kısıtlamayı öngörmediği için çocuklar açısından söz konusu içerikle muhatap olma tehlikesi her zaman bulunmaktadır. Çünkü, İnterneti kullanan kişinin çocuk mu yetişkin mi olduğunun tespiti neredeyse imkansızdır. Bu imkansızlık nedeniyle, yaş doğrulama sisteminin mantığı açısından aslolan, 18 yaşından büyük olduğunu kanıtlamayanların müstehcen içeriğe erişiminin mümkün olmamasıdır. Dolayısıyla, müstehcenlik açısından doğru

olan öncelikle tüm abonelere bu tür içeriğe erişimin kısıtlı olmasıdır. Bu durumdan hoşnut olmayanlara daha sonra, abonelik bilgileri ile kimliklerini ve dolayısıyla reşitlik durumlarını doğrulayarak talepleri üzerine bu tür içeriklere erişimlerine yönelik imkan tanınmalıdır. Halbuki, mevcut Güvenli İnternet Hizmeti müstehcenlik açısından bu sisteme uygun bir uygulama sağlamamaktadır. Fakat, abonenin müracaatı ile müstehcenliğinde içinde bulunduğu yasadışı ve zararlı içeriklerin kısıtlandığı aile ve çocuk profilini seçebilmeye imkan tanınması yönü ile, eksik ve tersinden de olsa kısmi bir yaş doğrulama sistemi getirdiği iddia edilebilir.

Nitekim, İngiltere’de gelecek yıldan itibaren başlamasına karar verilen müstehcen içeriğe erişimin her yeni abone için kısıtlanmasına ve daha sonra talebi olursa bu tür içeriğe erişimine izin verilmesine ilişkin uygulama yaş doğrulama sisteminin mantığına daha uygun düşmektedir. Dolayısıyla, Güvenli İnternet Hizmeti’nde yer alan profil seçeneklerinin çeşitlendirilerek, özellikle, sadece müstehcen içerik açısından yaş doğrulama sisteminin mantığı çerçevesinde ülkemizde de müstehcenliğe yönelik içeriğin kısıtlandığı ve serbest kılındığı iki farklı profil oluşturulabilir. Keza, aynı İngiltere’nin yaklaşımı ile, aksini talep etmedikleri sürece, yeni abonelere müstehcenliğin kısıtlı olduğu İnternet profili sunulabilir.

13. İnsan ve Toplum Merkezli Yaklaşım

İnternet içerik düzenlemesiyle ilgili konuyu ele alırken, çok daha gerilere giderek, öncelikle, İnternete ilişkin insani varoluşumuzun ontolojik temelleri bağlamında sağlıklı ve isabetli bir yaklaşım ve bakış açısı geliştirmeye ihtiyaç vardır. Bu kapsamda İnterneti, insan hayatında ve insanlık tarihi içinde ait olduğu doğru yere oturarak işe başlanmalıdır. İnsanda hayranlık uyandıran ve kendisine metfun kılan etkileyici, sarsıcı, değiştirici ve dönüştürücü gücü ile İnsanlık tarihinin en önemli buluşu sayılan İnternet, netice olarak, insan için, insanın faydası ve mutluluğu için yine insan tarafından bulunan ve geliştirilen, insanlık tarihinin belli bir aşamasında sahneye çıkan teknolojik bir “araç”tır. Dolayısıyla, “İnternet hayattır”, “İnternet su ve hava gibidir”, “İnternetsiz yaşanılmaz” gibi İnternetin cazibesini, gücünü ve vazgeçilmezliğini anlatmak için üretilen ve kullanılan, çoğu zaman da İnterneti “mit”

haline getiren, yücelten ve kutsayan ifade ve sloganlar İnternetin insan/insanlık için bir “araç” olduğu gerçeğini unutturmamalıdır.

Zira, İnternet “hayat” değil, hayatın içinde bir “araç”tır. İnternet, insan “hayat”ının içinde, onu kolaylaştırmak ve insanın ihtiyaçlarını karşılamak için icat edilmiş, insan ile, insanın varlığı ile değer bulan ve anlamı olan bir “araç”tır. Çünkü, hayatın “özne”si “insan”dır ve onun dışındaki her şey bu “özne”ye nispetle değer bulur ve anlam kazanır. Aksi taktirde, İnternetin bu bağlamından kopartılıp gerçekliğinden uzaklaştırılması, gereğinden fazla yüceltilerek her şeyin merkezine alınması ve “hayatın öznesi” haline getirilmesi, insani varoluşun ontolojik temelleri ile bağdaşmayan, insan hayatına ve hayatının anlamına dair çarpık bir anlayışın ortaya çıkmasına neden olacaktır.

Başka bir ifade ile bu durum, insanın eşya ile arasında kurmuş olduğu “amaç-araç” ilişkisini tersyüz ederek “araç”ı “amaç”, “amaç”ı “araç” haline getirecek, anlam ve değerler hiyerarşisini ve sistemini büsbütün bozacaktır. Yani, insan hayatının iyiliği ve mutluluğu için bir “araç” olarak görülmesi gereken İnternet, “araç” olma konumundan hızla uzaklaşarak hayatın “amacı” haline dönüşürken, insan ve hayatı İnternetin yaşaması, iyiliği ve geliştirilmesi için bir “araç” konumuna gelecektir. Dolayısıyla, akliselim olan herkesin itiraz edeceği çarpık bir durum ortaya çıkacaktır.

Bu noktada, biraz garip olmakla birlikte şu kritik sorular gündeme gelecektir; “İnternet insana hizmet için mi vardır? Yoksa, insan İnternete hizmet için mi vardır?” ya da “İnternet insan için midir? Yoksa, insan İnternet için midir?”. Biraz, düz ve kaba bir kıyaslama ve mantık yürütme olarak görülebilecek bu değerlendirme ve sorular, eleştirilere açık yönleriyle birlikte, özünde önemli bir tezata ve traji-komik bir çarpıklığa işaret etmektedir.

Burada dikkat çekilmek istenen konuyla, günümüz devlet-vatandaş ilişkilerinin ve kamu yönetimi anlayışının insan ve vatandaş odaklı yaklaşımları ile ilişkilendirilmesi ve bu bağlamda İnternet içerik düzenlemelerinde göz önünde bulundurulması gereken bazı hususlara atıfta bulunulması mümkündür. Nitekim, genel bir çerçeve

olması bakımından, tüm diğer alanlarında olduğu gibi, İnternet alanının da insan odaklı olarak değerlendirilerek, vatandaş menfaatlerini ve taleplerini merkeze alan yaklaşımlarla düzenlemelere konu edilmesi beklenmelidir. Bu çerçevede, İnternet içerik düzenlemelerinde de kullanıcı odaklı, vatandaş menfaat, istek ve taleplerini önceleyen, kişisel tercih ve beklentilere cevap veren çeşitlilikte hizmet sunumuna imkan tanıyan düzenlemelere gitmek gerekmektedir.

Dolayısıyla bu yaklaşımın gereği olarak, insanın veya insanların genel menfaatleri veya genel istek ve talepleri ile soyut olarak İnternetin veya İnternet sektörünün genel menfaati veya genel istek ve talepleri karşı karşıya geldiğinde “insan ve toplum” tarafına öncelik vermek, insanı ve toplumu korumak gerekmektedir. O halde, içerik politikalarını, düzenleme ve uygulamalarını insan odaklı ve öncelikli olarak belirlemelidir. Benzer şekilde, “İnternetin özgürlüğü” ile “insanların özgürlüğü”nü karşı karşıya getirmemeye çalışmakla birlikte, karşı karşıya geldiklerinde de “insanların özgürlüğü” tercih edilmelidir.

Bu yaklaşım, bilgi toplumu ile gündeme gelen “gözetim toplumu” olma, sayısız uçurum, güvenlik ve risk kaygıları, yabancılaşma ve tüketim, bilgi kirliliği ve enformatik cehalet gibi sorunlar ile, İnternetle gelen yasadışı ve zararlı içerik, siber güvenlik, mahremiyet ihlalleri ve tüm bunların sebep olduğu sosyal problemlere önlem alma, mücadele etme ve çözüm bulma konularında daha etkin politikaların geliştirilmesi gereğine ve gerçeğine önemli bir katkı ve arka plan sağlayarak, doğru bir projeksiyon sunacaktır.

14. Tüketicilere Seçme ve Tercihle Bulunma Özgürlüğü Sunulması

İnternet hizmetlerinin giderek içerik sunumu açısından kullanıcılara/tüketicilere seçmeye ve kişisel tercihte bulunmaya olanak tanıyacak şekilde çeşitlendirilmesi ve bu yönde geliştirilmesi gerekmektedir. Bunun sağlanması da ancak, tıpkı diğer birçok bilgi teknolojisi, elektronik haberleşme ve yayıncılık hizmetinde olduğu gibi, İnternet hizmetlerinde de nihai noktada tüketicilerin taleplerinin belirleyici olmasıyla mümkün olacaktır. Halbuki, günümüzde İnternet hizmetleri büyük oranda Facebook,

Google, Youtube, Twitter gibi küresel İnternet platformlarının belirlediği standart ve içeriklere göre şekillenmektedir. Bu standart ve içerikler ise genellikle üretici veya iletilici firmaların ticari motivasyonlarına ve kaygılarına göre biçimlenmektedir. Diğer bir deyişle, bahsi geçen küresel içerik sağlayıcıların hazırlayıp sunduğu içerikler İSS’ların belirlediği standartlarla servis edilmekte ve bir noktada dayatılmaktadır. Bu süreçte tüketicilerin değerleri, talepleri, tercihleri ve beklentileri çoğunlukla gözardı edilmekte, seçme ve tercih etme özgürlükleri ellerinden alınmaktadır. Bu sistemde kullanıcı hakları ve tüketici iradesi nerdeyse yok sayılmaktadır.

Halbuki, tüketici diğer yayın mecralarında olduğu gibi belirleyici olmalı, içeriği ve hizmet standartlarını seçebilme özgürlüğüne sahip olmalıdır. Aslolan tüketici olarak insandır. İnsanın istek, talep ve beklentileridir. Hizmet sunucular, azami olarak bu istek ve talepleri yerine getirmeye, insanın seçebilme özgürlüğünü genişletmeye çalışmalıdır. Nasıl, televizyon yayını alan bir tüketici TV veya uydu alıcısının teknik özelliklerini kullanarak beğenmediği yayın içeriklerine sahip kanalı silerek yayından kaldırıyor veya şifre koyarak erişimi engelliyor, istediği yayını öndeki veya arkadaki kanallara taşıyarak içerikte, erişimde ve sunumda kişisel tercihlerine göre değişiklikler yapabiliyor ise; İnternet hizmetlerinde de benzer şekilde seçme ve tercihte bulunmaya olanak verecek hizmet çeşitliliğini sağlayacak düzenlemelere gidilmesi gerekmektedir. Yani, bir tür herkesin kendisine özel içeriğe sahip olacağı bir İnternet toplumuna doğru gidilmesinin yolu açılmalıdır. Bu kapsamda kullanıcı hakları ve seçme özgürlüğünün güçlendirilmesi yaklaşımıyla güvenli İnternet paketlerinin çeşitlendirilmesi bu yolda atılacak önemli adımlardan birisi olacaktır.

15. “İnternet Erişim Hakkı” ve “İçerik Seçme Hakkı”na Anayasal Güvence

Tüm dünyada İnternet artık temel bir İnsan hakkı olarak algılanmaktadır. Bu nedenle Anayasa’da yer alan diğer demokratik hak ve hürriyetlerle birlikte “İnternete erişim hakkı” da Anayasa metinlerinde yer almalıdır. Diğer yandan, seçme ve tercihte bulunabilme olanağının sağlanması, farklılıkların ve çeşitliliğin korunması, kişilerin istek ve beklentilerinin karşılanmasını esas alan insan odaklı bir yaklaşım günümüz dünyasının en çok değer verilen özellikleri arasında yer almaktadır. Buna göre,

tüketici hakları bağlamında İnternet kullanıcısının korunması ve üreticinin belirlediği tek tip bir hizmet sunumuna mahkum olmaması; kişisel ihtiyaç, istek ve beklentilerini karşılayabileceği farklı alternatif hizmetler veya sunumlar oluşturulması ve kullanıcıya seçme ve tercihte bulunabilme imkanı sağlanması gerekmektedir. Dolayısıyla, “İnternete erişim hakkı” ile birlikte “içerik seçebilme hakkı” da Anayasa’da temel bir hak olarak düzenlenmelidir.

B. Kurumsal Yapılar

Bu bölümde İnternet içerik düzenlemesiyle ilgili bütüncül bilgi toplumu ve İnternet politikalarının oluşturulmasında ve uygulamasında görev alması uygun görülen kurumsal yapılara kısaca değinilmiştir.

1. Bilişim ve Yayıncılık/Bilişim Bakanlığı

İnternetin hayatın her alanına girmesi ve giderek aratan bir değer haline gelmesi onu en önemli stratejik kaynaklardan birisi haline getirmiş ve ülkeleri bütüncül bilgi toplumu ve İnternet politikaları oluşturma ve uygulamaya yöneltmiştir. Ülkeler bunu da genellikle bilgi toplumu ve bu bağlamda İnternet konusundan sorumlu tek bir yönetsel otoriteye görev, yetki ve sorumluluk vererek gerçekleştirmektedir.

Ülkemizde de stratejik olarak kabul edilen konularla ilgili farklı bakanlıkların çatısı altındaki kurum ve kuruluşların bir araya getirildiği ve oluşturulan bütüncül politikaların, söz konusu bu yeni örgütsel yapılarca hayata geçirilmesinin temin edilmeye çalışıldığı görülmektedir. Nitekim, ailenin stratejik önemi fark edildiği için sosyal hizmetler ve aileyle ilgili görevleri bulunan bir çok farklı kurum ve kuruluş 2011 yılında çıkarılan bir KHK ile Aile ve Sosyal Politikalar Bakanlığı çatısı altında birleştirilmiştir. Oluşturulan bu yeni Bakanlık’a aileyle ilgili bütüncül politikalar oluşturma ve uygulama görevi verilmiştir. Keza, Bakanlık’ın yapmış olduğu çalışmalar sonucunda aralarında Dışişleri, İçişleri, MEB, Sağlık, Maliye, Ulaştırma ve Ekonomi gibi bakanlıkların bulunduğu 9 bakanlıkla aileye yönelik politika

oluşturmak ve aileye yönelik hizmetleri geliştirmek konusunda işbirliği protokolü imzalanmıştır.¹³⁴

Türkiye’de benzer bir yaklaşımın İnternet konusunda da ortaya konulması gerekmektedir. İnternet konusunun sahibi ve sorumlusu bir bakanlık olmalıdır. Bütüncül İnternet politikalarının hazırlanması ve uygulamasını bu bakanlık takip etmeli, diğer bakanlıkların İnternetle kesişen çalışma alanlarıyla ilgili işbirliği süreçlerini yürütmelidir. Fakat, ülkemizde İnternetle ilgili İnterneti tüm boyutlarıyla ele alan ve kucaklayan, ona sahiplik yapan kurum bulunmamaktadır. Keza, buna paralel, bütüncül bir İnternet politikası oluşturulmuş değildir. Çünkü bununla ilgili bir örgütsel yapılanma yoktur. Var olanlar, İnternetin farklı boyutları ve aktörleri ile ilgili ve sorumludurlar.

Nitekim, TİB Başkan V. Ve İnternet Dairtesi Başkanı Şen çarpıcı bir şekilde, söz konusu eksiklik yüzünden, İnternet Dairesi’nin göreve başladığı tarihten bu yana en az uğraştığı konunun İnternet içerik düzenlemesi konusu olduğunu beyan etmektedir. Zira, İnternetle ilgili en elle tutulur birim olduklarından görev alanlarına girmese dahi, İnternetle ve İnternet politikası ile ilgili bütün konu ve sorunların kendilerini bulduğunu ve önlerine geldiğini, dolayısıyla takip etmek zorunda kaldıklarını dile getirmektedir.

Halbuki, ülkemizde doğrudan bilgi toplumu ve İnternetle ilgili görevleri olan iki bakanlık bulunmaktadır. Bunlardan UHD Bakanlığı özellikle BTK ile İnternet üzerinde en çok söz sahibi olan Bakanlık konumundadır. Diğer yandan, Kalkınma Bakanlığı’na bağlı Bilgi Toplumu Dairesi Başkanlığı “bilgi toplumu” çalışmaları çerçevesinde e-Dönüşüm Türkiye Projesi’nin koordinasyonunu yapmakta, bilgi toplumu strateji ve eylem planı belgelerinin hazırlanmasını koordine etmektedir.

Halbuki, bilgi toplumu ve İnternet konusunun birbirinden ayrılarak iki farklı Bakanlık arasında pay edilmesi, bütüncül bir bilgi toplumu ve İnternet politikası

¹³⁴ “Aile Olmak Projesi İşbirliği Protokolü İmzalandı”, 18.06.2013, <http://www.turkiyeegitim.com/aile-olmak-projesi-isbirligi-protokolu-imzalandi-47739h.htm>

oluşturmanın ve uygulamanın önündeki en önemli engellerden birisidir. Bu nedenle, ülkemizde diğer birçok gelişmiş ülkede olduğu gibi, bütüncül bir bilgi toplumu ve İnternet politikası oluşturmak ve uygulamasını takip ve koordine etmek için bilgi ve iletişim teknolojileri, elektronik haberleşme ve yayıncılık sektörlerine ilişkin alanlarda görevli tek bir bakanlık teşkilatı kurulmalıdır.

Bu kapsamda, bilgi toplumu ve İnternetle ilgili ulusal ve küresel gelişmeleri yakından takip ederek riskleri, fırsatları ve tehditleri analiz ederek bütüncül politika ve stratejiler geliştirme, ulusal koordinasyonu sağlama ve izleme, söz konusu sektörlerin potansiyellerini harekete geçirme ve bu sektörlerin dinamizmine uygun bir şekilde, gerekli ihtiyaçlara hızlı reaksiyon verebilme becerisine sahip bir bakanlık örgütlenmesi sağlanmalıdır. Bu yeniden yapılandırmada Bilgi Toplumu Dairesi'nin konumunun güçlendirilerek, mevcut görevlerinin yanında bilgi toplumuyla ilgili başka bazı görevlerde verilerek, söz konusu bakanlık bünyesinde “Bilgi Toplumu Genel Müdürlüğü” olarak örgütlenmesi daha uygun olacaktır. Nitekim, daha önce bu birimin güçlendirilmesiyle ilgili ihtiyaçlardan dolayı Bilgi Toplumu Dairesi'nin genel müdürlük düzeyine çıkartılmasıyla ilgili akim kalan bir çalışma da yapılmıştı.

Kurulmasını önerdiğimiz bu yeni bakanlığa “Bilişim ve Yayıncılık Bakanlığı” veya kısaca “Bilişim Bakanlığı” gibi isimler verilebilir. Bakanlık, bahsi geçen görev ve sorumluluklarını yerine getirirken bağlı, ilgili ve ilişkili kurum ve kuruluşlarıyla birlikte kurumsal yönetim ilkelerine uygun olarak; ilgili özel sektör, sivil toplum ve akademik camia ile işbirliği ve yardımlaşma içerisinde hareket etmelidir.

Yayıncılık sektörünün bu yeni bakanlığın görev alanına girmesinin nedeni ise, daha önce değinildiği gibi, yakınsama teknolojilerindeki gelişme ve yayıncılığın giderek dijital mecraya evrilmesi ve İnternet altyapısına entegre olmasıdır.

2. Bilgi Teknolojileri, İletişim ve Yayıncılık/Bilişim Kurumu

Bilgi ve iletişim teknolojileri, yayıncılık ve elektronik haberleşme sektörlerinin sınırlarının giderek belirsizleşmesi ve ortadan kalkması, medya içeriklerinin giderek İnternet ve mobil servis aracılığıyla taşınmaya ve dağıtılmaya başlaması nedeniyle,

söz konusu alanlardaki bütünleşme, kalite ve çeşitliliği sağlamak için İnternet üzerinden dağıtılan içeriğin daha kompleks ve rafine düzenlemelere ihtiyaç duyması sonucunu doğurmuştur. Bu nedenle, İnternet içerikleri de dahil olmak üzere tüm yazılı, sesli, görüntülü medya içeriklerinin “yayıcılık” kapsamı içinde değerlendirilerek tek bir kurumsal yapı altında toplanması ve içerik düzenlemesine tabi tutulması gerekmektedir. Böylece, söz konusu içeriklerin benzer ölçütlere göre tek bir elden düzenlenmesi ve denetlenmesi mümkün olacak, yasadışı ve zararlı içeriklerle mücadelede uygulama birliği sağlanacaktır.

Bu çerçevede, bu alanda yetkili iki düzenleyici ve denetleyici özerk kurum olan RTÜK ve BTK’nın birçok gelişmiş ülke uygulamasında görüldüğü gibi tek bir çatı altında birleştirilmesi gerekmektedir. Bu birleşme yeni bir düzenleyici kurum ihdası ile mümkün olabileceği gibi, mevcut kurumlardan birisinin çatısı altında da gerçekleştirilebilir. Bu durumda, yayıncılığın giderek sayısal yayıncılığa ve İnternet altyapısına kaydığı göz önünde bulundurularak bu bütünleşmenin BTK bünyesinde gerçekleşmesinin daha uygun olacağı öngörülebilir. Bütünleşme BTK çatısı altında gerçekleştirilirse; Kurumun yeni ismi “Bilgi Teknolojileri, İletişim ve Yayıncılık Kurumu”, “Bilişim Teknolojileri Kurumu” veya kısaca “Bilişim Kurumu” olabilir.

Böylece, Avustralya’daki ACMA, Almanya’daki KJM, Güney Kore’deki KCSC, Singapur’daki MDA benzeri, İnternetin sektörel düzenlemesi yanında, İnternet içerikleri de dahil olmak üzere tüm yazılı, sesli ve görüntülü yayıncılık içeriklerini tek elden benzer ölçüt ve standartlara göre düzenleyen ve denetleyen, yasadışı ve zararlı içeriklerle mücadele eden güçlü ve etkin bir kurum oluşturulmuş olacaktır. Bu kurumun yönetim anlayışına göre yapılandırılması ve karar organlarında özel sektör, STK’ları ve üniversite temsilcilerine yer vermesi önemli taşımaktadır.

3. İnternet İçerik Güvenliği Başkanlığı

İnternet içerik düzenlemeleri konusunun çok boyutlu, çok aktörlü ve birçok grift sorunu içinde barındıran bir özelliğe sahip olduğu açıkça görülmektedir. Dolayısıyla, böylesine zor ve karmaşık bir konunun yükünü, bambaşka bir amaçla kurulan bir

kuruma sonradan monte edilmek suretiyle oluşturulan bir daire başkanlığının sırtına yüklemek başlangıçta isabetli olarak görülse de bugün için doğru bir yaklaşım olarak görülemez. Nitekim, TİB İnternet Daire Başkanlığı, 5651 sayılı Yasa'nın kendisine bu konuyla ilgili vermiş olduğu görev ve yetki alanlarının bir kısmına örgütsel imkansızlıklar nedeniyle ya hiç girmemiş ya da yeterince ilgi gösterememiştir.

Bu nedenle, İnternet içerik düzenlemesi özelinde ülkenin en yetkili otoritesi olacak bir daire başkanlığından daha büyük ve güçlü bir kurumsal yapıya ihtiyaç vardır. Keza, bu kurum, İnternet gibi dinamik bir yapının yine dinamik bir yönetsel yapıya sahip daha esnek ve hareket kabiliyeti yüksek bir kurum tarafından yönetilmesi gerektiği gerçeğinden hareketle yapılandırılmalıdır.

İnternet içerik düzenlemesi konusunun sahibi ve sorumlusu olacak bu kurum, ülkede bu alanda strateji ve politika belirlenmesi ve uygulamasından, bu çerçevede ilgili tüm ulusal veya uluslararası kamu/özel/STK'larıyla birlikte yönetim anlayışı içinde ilişki ve işbirliği içinde olmalıdır. Dolayısıyla, daha önce bahsi geçen sistematik içerisinde, bütüncül politikalar oluşturmak ve uygulamak amacıyla hazırlanacak olan "İnternet İçerik Güvenliği Stratejisi ve Eylem Planı Belgesi"nin hazırlama ve uygulamasından bu kurum sorumlu olmalıdır.

İnternet içerik güvenliğinin sağlanmasını kendine misyon edinen bu kurum, bunun en önemli unsuru olarak bütüncül, gerçekçi, doğru ve uygulanabilir bir ulusal strateji ve politika oluşturulmasını kendisine en önemli görev bilmelidir. Bu çerçevede, kurumsal deneyim ve birikim yanında, tüm ilgili kamu/özel/STK kurum ve kuruluşların, üniversitelerin, İnternet kullanıcılarının, yazar ve fikir adamlarının bilgi ve birikimini, istek ve beklentilerini bu sürece dahil edecek yönetim mekanizmalarını kurmalı ve işletmelidir. Bu konuda özellikle, kurulmasını önermiş bulunduğumuz "Veri Değerlendirme ve Analiz Daire Başkanlığı"ı aktif olarak kullanılmalıdır.

Söz konusu kurumun, İnternetin güvenli kullanılması, yasadışı ve zararlı İnternet içeriğinin oluşturduğu risk, tehdit ve tehlikeler ile bunlarla mücadele edilmesi

konusunun öneminin tüm toplum kesimleri, karar verici ve ilgili tüm kamu/özel/STK kurum ve kuruluşlarınca iyi anlaşılması ve bu konuda yeterli bir duyarlılık ve farkındalık oluşması için yoğun çaba sarf etmesi ve çok yönlü çalışmalar yapması gerekmektedir. Bu kapsamda, özel sektör kuruluşlarını öz düzenleme yolu ile kendi içlerinde veya birlikte girişimde bulunma konusunda ikna etmeye ve zorlamaya çalışırken, STK'larını bu konularla ilgili çalışmalar yapmaya ve faaliyetlerde bulunmaya teşvik etmelidir.

Bunun yanında, başta Aile ve Sosyal Politikalar Bakanlığı Aile ve Toplum Hizmetleri Genel Müdürlüğü olmak üzere, MEB ve YÖK, Adalet Bakanlığı, İçişleri Bakanlığı ile yakın işbirliği içinde çalışmalıdır. Aile ve Toplum Hizmetleri Genel Müdürlüğü ile aileyi ve çocukları İnternet'in olası zararlarından korumaya yönelik çalışmalar, MEB ve YÖK ile; konunun eğitim boyutu ile ilgili olarak bilinçlendirme, medya okur-yazarlığı veya İnternet etiği konularında yapılabilecekler, üniversitelerin bu konulardaki akademik araştırma ve çalışmalara yönlendirilmesi, eğitim programlarının bu manada gözden geçirilmesi gibi konularda, Adalet Bakanlığı ile; bu tür suçlarla mücadelenin hukuksal ve adli boyutu konularında, İçişleri Bakanlığı ile İnternet kafelerin sorunları ve denetimleri boyutu ile ilgili işbirliği geliştirmelidir. Bu kapsamda, söz konusu kurum tarafından, bütüncül bir İnternet içerik politikası oluşturulması ve uygulanmasının gerekliliğine ilişkin karar verici siyasiler ile konuyla ilgili diğer kamu kurumlarının ortak bir fikir ve iradeye sahip olmalarının sağlanması en önemli hedef olarak görülmelidir.

Söz konusu kurum, tüm bu çalışmalarla ve kurumun diğer yapacağı işlerle ilgili olarak birçok kurum ve kuruluşla yoğun bir kurumsal ilişki ve iletişim içinde olacaktır. Bu nedenle, bu ilişki ve iletişimin sağlıklı ve doğru bir şekilde yürütülebilmesini sağlayabilmek için kurum bünyesinde "Kurumsal İletişim ve Koordinasyon Daire Başkanlığı" oluşturulması düşünülebilir.

Tüm bu görevleri yerine getirecek İnternet içerik düzenlemesinden sorumlu söz konusu kurumun müstakil bir Başkanlık olarak yapılandırılması ve isminin "İnternet İçerik Güvenliği Başkanlığı" olarak belirlenmesinin uygun olacağını öngörmekteyiz.

Nitekim, başlangıçta da benzer bir düşünceyle, 5651 sayılı Yasa'ya kaynaklık eden hükümet tasarısında TİB İnternet Dairesi Başkanlığı'nın adının yer almadığı, Yasa'nın verdiği görevlerle ilgili olarak yeni kurulacak “Bilişim Güvenliği Başkanlığı”nın sorumlu olacağının belirtildiği bilinmektedir.

Diğer yandan, TİB'na daha sonra verilen siber güvenlikle ilgili görevler ve USOM'un burada kurulması, Başkanlığın görev ve sorumluluk alanını tahminlerin üzerinde büyük oranda artırmıştır. Siber güvenlik konusunun da en az İnternet içerik düzenlemeleri konusu kadar geniş, zor, çetrefilli ve büyüme istidadı gösteren bir konu olması nedeniyle kısa bir zamanda daha büyük bir örgütsel yapıya ihtiyaç duyacağı kaçınılmazdır. Bu nedenle, siber güvenlikle ilgili çalışmaların da kurulacak ayrı bir “Siber Güvenlik Başkanlığı” çatısı altında kurgulanması ve organize edilmesinin daha doğru olacağı düşüncesindeyiz.

Böylece, hali hazırda TİB'na verilmiş olan İnternet içerik düzenlemesi ve siber güvenlikle ilgili görevlerin yeni kurulacak başkanlıklara devredilmesinden sonra Başkanlık, asli kuruluş amacına geri dönmüş olacaktır. Bu şekilde, aynı teknik altyapıyı kullanan TİB ile yeni kurulacak olan “İnternet İçerik Güvenliği Başkanlığı” ve “Siber Güvenlik Başkanlığı” BTK'ya bağlı olarak görevlerini sürdürebilirler. Bu başkanlıkların, İnternet sektörünü düzenleyen ve sektördeki işletmeleri denetleyen kurum olan BTK'nın bünyesinde kalması daha doğru gibi gözükse de, bu durumda teşkilat yapısının oldukça karmaşık bir hale geleceği ve hantallaşacağı düşünülebilir.

Keza, TİB'in, BTK'nın organizasyonel yapısına sonradan, doğrudan Kurum başkanına bağlı müstakil bir başkanlık olarak eklemesi, zaten klasik Türk kamu yönetimi örgütlenmesi açısından çokta örneği bulunmayan alışık olunmadık yeni bir durum iken ve bu yeni yapı ile ilgili sorunlar daha yeni yeni çözüme kavuşturuluyorken, yeni iki başkanlığın daha yapıya dahil olması yeni başka sorunlara neden olabilme potansiyeli taşımaktadır.

Bu nedenlerle, alternatif olarak, bahsi geçen üç başkanlığın BTK benzeri, kamu tüzel kişiliğine sahip idari ve mali özerkliğe sahip özel bütçeli düzenleyici yeni bir üst

kurul bünyesinde daire başkanlığı olarak yapılandırılmaları söz konusu olabilir. Bu yeni kurumun ismi “Bilişim Güvenliği Kurumu” olabilir. Üst kurula bağlı müstakil başkanlıkta bir daire başkanlığı olarak yapılandırılmak ile, bir üst kurulda doğrudan oluşturulan daire başkanlığı olarak yapılandırılmak arasında önemli farklar olacağı için, bu durum, Başkanlık kurulmasına yönelik önerimizin temel gerekçesi olan “güçlü örgüt” talebini büyük oranda karşılayacaktır. Bilişim güvenliğini sağlama amacına yönelik olarak kurulacak ve bahsi geçen üç başkanlığın fonksiyonlarını yerine getirecek bu yeni kurum, bilişimle ilgili yeni bir Bakanlık kurulur ise; bu bakanlıkla, bu gerçekleştirilmez ise; mevcut Ulaştırma, Denizcilik ve Haberleşme Bakanlığı ile “ilişkili” kurum olarak görev yapabilir.

4. İnternet Geliştirme Kurulu

İnternet Geliştirme Kurulu, İnterneti, kamu/özel/STK’larının “birlikte düzenleme” yaklaşımının en önemli somut uygulaması olarak kurgulanmalıdır. Dolayısı ile Kurul, örgütsel, işlevsel ve bütçe yönü ile güçlendirilerek, İnternet politikalarının belirlenmesinde ve uygulanmasında en etkili ve yetkili üst düzey danışma organı olarak yapılandırılmalıdır. Bu çerçevede, yönetim ilkesine tam bir uyum gözetilerek üye sayısının artırılması ve İnternet alanındaki tüm kamu-özel-STK paydaşlarının adil ve dengeli temsili sağlanacak bir yapının oluşturulması temin edilmelidir. Kurul’da özel sektörden içerik, yer, erişim ve ticari toplu kullanım sağlayıcıların temsilcileri yanında Türkiye Dijital Oyunlar Federasyonu Başkanı ve gerekli görülen diğer İnternet alt sektörlerine ait temsilciler yer almalıdır.

Aynı şekilde, Kurul’un STK ayağının güçlendirilmesi ve özellikle tüketici STK’larının da Kurul’da temsili sağlanmalıdır. Kamu tarafında ise, mevcut üyeler yanında TİB Başkanı veya İnternet Dairesi Başkanı ile Aile ve Sosyal Politikalar Bakanlığı Aile ve Toplum Hizmetleri Genel Müdürü, Bilgi Toplumu Dairesi Başkanı ve MEB’nden bir temsilci bulunmalıdır. Ayrıca, akademik camiadan konuyla ilgili bir kişi mutlaka yer almalıdır.

İnternet Geliştirme Kurulu, Türkiye’de ve dünyada İnternete ilişkin gelişmeleri yakından takip ederek bütüncül İnternet politikalarının oluşturulması ve uygulamasına ilişkin en etkili ve yetkili üst düzey danışma organı olarak; ülkemizde İnternet teknolojisinin gelişmesi, İnternet kullanımının daha da yaygınlaşması ve bilinçli, güvenli ve etkin kullanımının sağlanması konularında araştırma, inceleme ve raporlama çalışmaları yapmalı veya yaptırmalı, strateji, görüş, öneri ve teklifler geliştirmelidir. Bu kapsamda, İnternetin sosyal etkileri, içerdiği risk ve tehditlerin tespit ve önlenmesi, yasadışı ve zararlı içerikle mücadele edilmesi, öz düzenleme uygulamalarının özendirilmesi, İnternete ilişkin toplumsal farkındalığın oluşturulması, İnternet okur-yazarlığı ve İnternet etiği bilincinin geliştirilmesi, pozitif İnternet içeriği üretilmesi, araştırma-geliştirme ve projelerin desteklenmesi gibi konularda çalışmalar yapmalı ve yapılmasını teşvik etmelidir.

Bu bağlamda, Kurul, resmi web sitesi üzerinden İnternete ait muhtelif konularda tartışma formları açabilir. Bu formlarda diyalog zemininde ortaya çıkan görüşlerle birlikte yürütülen çalışmaların sonuçlarını öneriler, teklifler ve raporlar olarak yayınlatabilir ve ilgililerin ve kamuoyunun dikkatine sunulmasını sağlayabilir.

Keza, Kurul, bilgilendirme ve bilinçlendirme faaliyetleri kapsamında web sitesinde kullanıcılara yönelik içerikler yayınlatabilir. Burada genel kullanıcılardan profesyonel kullanıcılara kadar her düzeye ve kesime uygun eğitici ve bilgilendirici materyaller yanında, akademik makaleler, mevzuat bilgileri, haberler ile İnternet kullanıcılarının günlük kullanımda karşılaşılabilecekleri tüm hukuki konularda pratik cevaplar veren servis hizmetleri sunabilir.

Bu bağlamda İnternet Geliştirme Kurulu, Kurul’da yer alan üyelerin temsil ettikleri kurumsal yapılar çerçevesinde diyalog sağlama, işbirliği ve yardımlaşmanın zeminini oluşturabilme kabiliyetine sahip olabilecektir. Keza, diğer ülkelerde yer alan benzeri yapılarla uluslararası işbirliği ve koordinasyon sağlamalıdır.

5. Sınıflandırma Kurumu

Yasadışı ve zararlı İnternet içerikleriyle mücadelede gündeme gelen filtreleme ve erişim engelleme, bilinçlendirme, öz denetim vb. uygulamalarında destekleyici ve tamamlayıcı bir unsur olarak içeriğin sınıflandırılması uygulaması tüm dünyada giderek daha fazla benimsenmekte ve kabul görmektedir. Bu kapsamda sınıflandırma faaliyetleri, uluslararası kuruluşlarca bu konuda küresel standartlar oluşturmayı hedefleyen sektördeki firmalara ait PICS ve ICRA gibi girişimler yanında, AB, ABD, Avustralya, İngiltere, Almanya, Hollanda, Danimarka, Singapur ve Güney Kore gibi birçok ülkede müstakil sınıflandırma kurum veya kurullarınca gerçekleştirilmeye çalışılmaktadır.

Nasıl her ülke kendine özgü içerik düzenlemesi uygulamalarına sahipse, sınıflandırma konusunda da kendi ahlaki, kültürel ve sosyal yapısına göre içerikleri değerlendirmekte ve sınıflandırmaktadır. Bu nedenle ülkelerin kendilerine özgü sınıflandırma kurum, kural ve uygulamalarına rastlanılmaktadır. Keza, ülkeler içerik düzenlemesi konusundaki yaklaşım, tutum ve politikalarına uygun olarak ve kendilerine özgü ahlaki, kültürel ve sosyal yapılarına göre içerikleri değerlendirmekte ve sınıflandırmakta; buna göre, kurallar, ölçütler ve uygulamalar geliştirmektedir. Dolayısıyla dünya üzerinde farklılıklar göze çarpmaktadır.

Bu türden çalışmalar, etiketleme sistemiyle siteleri kategorilere ayrılmakla ebeveynlerin site erişimlerine ilişkin kararlarına kaynaklık ederken, filtreleme programlarına da kara listelerin oluşturulması konusunda yardımcı olmaktadır. Sınıflandırmalar, içeriği değerlendirmeye alarak konularına (çıplaklık, cinsel içerik, şiddet vb.) ve yaş gruplarına göre kategorize etmeye ve buna göre farklı işaret veya sembollerle tarif ve tasnif etmeye dayanmaktadır. Böylece kullanıcıların daha başlangıçta herhangi bir içeriğin ne tür özellikler taşıdığı ve hangi yaş grubuna uygun olduğu konusunda bilgi sahibi olması temin edilmektedir. Diğer yandan, bu içeriklerin özelliklerine göre serbest veya sınırlı erişime açık olmalarını belirleme ve denetleme konusunda uygulayıcılara büyük bir kolaylık sağlamaktadır. Bu yönleriyle sınıflandırmanın, İnternet sitelerini düzenlemek ve İSS'ların müdahalesi olmaksızın

içeriğin kontrol edilmesini sağlamak şeklinde önemli bir görev üstlendiği söylenebilir.

Türkiye’de ise, İnternet içerik sınıflandırmasıyla ilgili olarak yakın zamanda oluşturulan yapı Çocuk ve Aile Profil Kriterleri Çalışma Kurulu’dur. Kurul, Güvenli İnternet Hizmetinde yer alan Çocuk ve Aile Profil listelerinin oluşturulmasına ilişkin kriterleri belirlemek üzere meydana getirilmiştir. BTK koordinasyonunda sivil kökenli üyelerin çoğunlukta olduğu 11 üyeden oluşan Kurul’da, İnternetin tarafı olan tüm kesimlere söz hakkı tanınması amacıyla, konunun bağımsız uzmanları ile STK temsilcilerine de yer verilmiş olması oldukça önemlidir. Bu yaklaşım, regülasyon çalışmalarının yönetim ilkesine göre “birlikte düzenleme” anlayışıyla yapılmasına yönelik beklentilere uygun düşmektedir. Nitekim, söz konusu Kurul çocuk ve aile profillerinin kıstaslarını belirleyerek bunu deklare etmiştir. Bu kıstaslara göre web sitelerini tasnif etme görevini ise TİB görevlileri yapmaktadır.

Söz konusu uygulama İnternet içeriğinin derecelendirilmesi konusunda önemli bir adım olmakla birlikte yeterli değildir. Ülkemizde yasadışı ve zararlı İnternet içeriği ile mücadeleyle yönelik olarak içeriğin sınıflandırılmasıyla ilgili daha kapsamlı çalışmaların yapılması gerekmektedir. Bu çerçevede, Türkiye’nin bir an önce, sadece İnternet içeriğini değil, tüm basılı, sesli ve görüntülü medya içerikleri ve dijital oyunları sınıflandırma ile ilgili çalışmaları yürütecek müstakil güçlü bir düzenleyici “Sınıflandırma Kurumu”na ihtiyacı vardır.

İşlevi açısından Almanya’daki KJM, İngiltere’deki BBFC, Avustralya’daki Classification Board, Hollanda’daki NİCAM benzeri olacak bu kurum, yayıncılık türlerine göre oluşturulacak çalışma komitelerinde kamu görevlileri yanında, ilgili yayıncılık türlerinin meslek temsilcilerine, tüketici temsilcilerine, STK’larından ve üniversitelerden temsilcilere, hukukçu, psikolog, sosyolog ve pedagog gibi uzman meslek gruplarının temsilcilerine ve ilgili alanlarda söz sahibi yazar, sanatçı ve düşünce adamlarına yer vermelidir.

Nitekim, Türkiye’deki işitsel ve görsel yayın içeriklerini değerlendirme, derecelendirme veya sınıflandırma benzeri işlerle ilgili olarak, Çocuk ve Aile Profil Kriterleri Çalışma Kurulu, Küçükleri Muzır Neşriyattan Koruma Kurulu, Sinema Genel Müdürlüğü Değerlendirme ve Sınıflandırma Kurulu ile RTÜK gibi farklı Bakanlıklara bağlı farklı statü, yapı, ölçüt ve çalışma usullerine sahip kurumların bulunduğu görülmektedir. Söz konusu farklılıklara rağmen, yapılan işin özü ve işlevi açısından birbirine benzer işlerle meşgul olan bu kadar farklı kurum yerine; tüm bu kurumların mevcut görevlerini ifa ettiği gibi, bu konularla ilgili mevcut ve gelecekteki diğer talep ve ihtiyaçlara cevap verecek şekilde her tür yayın içeriğini değerlendirip sınıflandırma veya derecelendirme kriterlerini belirleyecek ve yapacak ihtisaslaşmış bir “Sınıflandırma Kurumu”nun daha faydalı olacağı açıktır. Bu sistem, tüm yayın içeriklerinin tek bir elden, benzer kriterlere ve yöntemlere göre değerlendirilip sınıflandırmasını temin ederek konuyla ilgili uygulama birliği sağlayacak ve zaman içinde birçok tartışma ve eleştirinin önüne geçecektir.

Söz konusu “Sınıflandırma Kurumu”nun yeni kurulacak bilişim ve yayıncılıktan sorumlu bakanlığın ilişkili kurumu olarak görev yapmasının doğru olacağını düşünmekteyiz.

6. İnternet Etik Kurulu

Eğitim ve pratik uygulamalarla etik anlayışın her sınıftan ve her yaştan bireye aşılması, özellikle İnternet etiğinin düzenli ve sürekli kampanyalarla teşvik edilip özendirilmesi gerekmektedir. Bu kapsamda; İnterneti düzenleyen mevzuat çalışmalarında, İnternet etiği konusuna dikkat çekmek ve atıfta bulunmak faydalı olacaktır. Dolayısıyla, Kamu Etik Kurulu’na benzer bir İnternet Etik Kurulu oluşturulabilir. İlgili kamu kurumları ile sektör firmaları ve STK’nın temsilcilerinden oluşturulacak bu bağımsız ve sivil karakterli Kurul, İnternet etiği ile ilgili tüm çalışmaları teşvik ve koordine edebilir. Kurul, yapacağı çalışmalar ile paydaşların üzerinde uzlaştığı İnternet etiği prensip ve kurallarını belirleyen bir metni ortaya çıkartabilir. Keza, Kurul, İnternet etiği konusunda ölçülebilir göstergelerin elde edilebilmesi, etik konusunda izlenecek politikaların belirlenebilmesi için yol

gösterici olabilir. Bu kapsamda, ilgili kurum ve kuruluşlarla ve üniversitelerle işbirliği içerisinde İnternet etiği üzerinde araştırmalar yapılmasını sağlayabilir. Bu araştırmalar sonucunda hazırlanacak raporların kamuoyu ile paylaşılması, toplumda bir İnternet etiği bilincinin oluşturulması ve geliştirilmesi için faaliyetler yürütebilir. Teorik ve pratik alanda İnternetin güvenli kullanımıyla ilgili bilinçlendirme faaliyetleriyle İnternet etiği konusunun entegrasyonuna ilişkin çalışmalar yapabilir. Bu bağlamda, eğitim müfredatlarında İnternet etiği konusunun yer almasına yönelik çalışmaları takip edebilir.

7. İnternet Arabuluculuk Kurulu

Ülkemizde İnternet içerik düzenlemesiyle ilgili olarak gündeme getirilmesi gereken konulardan birisi de “Arabuluculuk Kurulu”dur. Fransa’da, kamu kurumları, STK’ları ve özel şirketlerden müteşekkil bir öz düzenleme kuruluşu olarak faaliyet gösteren İnternet Hakları Formu (Forum Des Droits Sur L'internet) benzeri kar amacı gütmeyen bir örgütsel yapı ile hayata geçirilebilecek olan arabuluculuk mekanizması Türkiye açısından da faydalı olacaktır. Gönüllü üyelik, diyalog ve işbirliği iradesi temelinde İnternet aktörlerinin ve paydaşların bir araya gelerek İnternet kullanımıyla ilgili sorunları arabuluculuk mekanizmasıyla çözmeyi amaçlayan bu örgütsel yapı, yasadışı ve zararlı içerikle mücadele konusunda önemli bir avantaj sağlayabilecektir. Bu mekanizma ile bir tür gönüllü uyar-kaldır sistemi işletilebilecektir.

İnternet kullanımı veya İnternet hizmetiyle ilgili olarak kişilerarası veya kişiler ile şirketler ya da şirketler arası anlaşmazlıkları yargıya taşımadan çözmeyi hedefleyen, diyaloga dayalı ve esnek, tarafsız bir kişi ve merciin müdahalesine imkan tanıyan bu mekanizma ile sektördeki düzenleyici kurumlar yanında sektörde yer alan firmalarla işbirliği geliştirilerek sorunlar çözülmeye çalışılmaktadır. Süreç içerisinde, Fransa’da olduğu gibi, arabuluculuk hizmetinin bir tür etik ilke ve kuralı olarak saygı gösterilmesini güvence altına alan mevzuat düzenlemelerine ve “tüketici heyeti” benzeri formülasyonlara konu yapılması da mümkündür.

Bu arabuluculuk mekanizması ve bunu sağlayacak örgütsel yapı, yeni bir bağımsız ve sivil inisiyatif ile gönüllülük esasına göre oluşturulabileceği gibi, başka bir öneri olarak ortaya konan “İnternet Etiği Kurulu” bünyesinde veya İnternet Geliştirme Kurulu’nun çatısı altında bir alt yönetsel birim olarak uygulamaya geçirilebilir.

8. Veri Değerlendirme ve Analiz Dairesi Başkanlığı

Konunun bir diğer yönü ise, İnternetin güvenli kullanımıyla ilgili olarak bahsi geçen kaçınılmaz zorunlulukların uygulama alanına geçirilmesini teşvik etmek, ilgili özel-kamu-STK tüm kurum ve kuruluşlarda bu yönde bir farkındalık oluşturmak, bu konulardaki çalışmaları ve işbirliği girişimlerini koordine etmek, ortaya çıkan bilgi, veri, araştırma, rapor benzeri ürünleri toparlayarak değerlendirilmesini sağlamaya çalışmakla görevli bir idari birimin gerekliliği gerçeğidir.

Bu amaçla, TİB bünyesinde ayrı bir "Veri Değerlendirme ve Analiz Dairesi Başkanlığı" oluşturulmalıdır. Bu birim, söz konusu çalışmalar yanında, yapılan yurtiçi ve yurtdışı araştırma, inceleme yayınlanan veri, yazı, rapor vb. dokümanlarla birlikte, bu çerçevede kurum içi üretilen benzer materyallerin toplanmasını, değerlendirilebilir hale getirilmesini ve değerlendirilmesini sağlamak, bunlarla ilgili bir veri tabanı oluşturularak tüm araştırmacıların istifadesine sunulmasını temin etmekle de görevli olmalıdır.

Nitekim, TİB, görevi gereği yapmış olduğu iş ve işlemlerden mütevellit elinde İnternetle ve mobil ve sabit telefonların suç aracı olarak kullanılmasıyla ilgili çok sayıda bilgi ve istatistiki veriye sahiptir. Türkiye’nin her yerinden TİB’na, telefon ile birey arasındaki ve İnternet ile birey arasındaki ilişki biçimlerine dair sürekli veri akışı olmaktadır. TİB, bu ilişkilerin veri havuzu konumundadır. Hiç bir kurumda, suç teşkil eden eylemlerle telefon ve İnternet arasındaki bağlantıya dair böylesine zengin veri tabanı mevcut değildir ve söz konusu verilerin Türkiye genelinde birleştirilmiş hali TİB dışında hiç bir kurumda yoktur. Bunlar, suç unsurlarıyla teknoloji arasında bağ kuran önemli veriler içermektedir. Bu itibarla, TİB’nın elindeki bu zengin veri tabanının, kişisel ve kurumsal gizlilik sınırlarını gözeterek, anonim bilgi haline

getirilip hem bahsi geçen İnternete ilişkin arařtırmalarda, hem de telefon üzerinden gerekleřtirilen yasadıřı eylemlerin su sosyolojisi, adalet, asayiş ve güvenlik hizmetlerine ilişkin stratejisi ve politikalar bakımından analizlerde kullanılabilir hale getirilmesi önemli bir konudur. Dolayısıyla, bu verilerin hem kurum içi hem de ilgili diğeri tüm kurum ve kuruluşların istifadesine sunulması ülke yararına değeriendirilmesi açısından önemli bir hizmet olacaktır.

TİB, veri havuzunda toplanan verilerden özellikle görev ve ilgi alanına girenlerin, bazı programların da yardımıyla analiz edilmesi, anlamlandırılması, değeriendirilmesi ve raporlandırılmasını temin edebilir. Raporlanan bu sonuçlar, uygun görülecek başka kiři, kurum ve kuruluşlarla katkı amaçlı paylaşılabilir gibi, kurumsal görevlerin ve sunulan hizmetlerin nitelik ve niceliğini artırmak için ve kurum içinde daha geniş çaplı proje üretme odaklı çalışmalarda kullanılabilir.

Diğeri taraftan, TİB'nin yasakları uygulama görevinden dolayı sürekli sansür ile birlikte anılması ve özel hayatın gizliliğinin kamu menfaatine devlet tarafından sınırlanması görevi nedenleriyle kurumsal imajı çok olumlu bir konumda değildir. Topluma, üniversitelere, diğeri ilgili kamu/özel/STK kurum ve kuruluşlara kendisi tarafından veya diğeri kiři ve kurumların ürettiğeri söz konusu verileri sağlıklı olarak ulařtırması ve bu verilerin değeriendirilmesi konusundaki çalışmaları, TİB'nin mevcut kurumsal imajına olumlu yönde önemli bir katkı da sağlayacaktır. Ayrıca, yapacağeri bu türden çalışmalar TİB'nin yürüttüğeri faaliyetlere ilişkin bilimsel ve akademik bir bakış açısı ve derinlik kazanmasına da temin edecektir.

9. İhbar Merkezi

TİB İnternet Bilgi İhbar Merkezi'nin daha kullanışlı, işlevsel ve amacına daha uygun bir içeriğeri ve yapıya sahip olması için önerilerimiz şunlardır:

1) İhbar Merkezi'nin diğeri birçok ülkede olduğeri gibi nihai olarak sivil bir yapıya kavuřturulması gerekmektedir. Geçiş sürecinde STK/STK'ların da içinde bulunduğeri kamu-sivil karma bir yapı oluşturulabilir. Fakat, İhbar Merkezi bir an önce İnternet konusunda faaliyet gösteren, toplumsal bilinirliğeri ve güvenilirliğeri yüksek, bu işi

yapabilecek STK/STK'ların çatısı altında çalışmalarını sürdürmelidir. Tüm dünyada yaygın eğilim bu yöndedir ve INHOPE da bunu teşvik etmektedir.

Bunun birkaç yönden faydasının olacağı öngörülebilir. Birincisi, içerik düzenlemeye ilişkin sistemin en önemli ayaklarından birisini oluşturan ihbar merkezi uygulamasının sivil toplum eliyle yapılıyor olması, söz konusu sistemin gönüllülük ve katılımcılık temelinde daha demokratik ve özgürlükçü bir yapıda olduğunun göstergesi olacaktır. İkincisi ise, biraz da birinci konuyla ilintili olarak, ihbar yapacak kişiler açısından rahatlatıcı bir etki doğuracaktır. İhbar merkezinin resmi bir kamu kurumu olması, bazı kullanıcıların ihbarda bulunma konusunda çekinceli davranmasına neden olabilmektedir. Üçüncüsü ise, finansal avantajlar sağlama yönü ile ilgilidir. Dünyadaki örneklerinde görüldüğü gibi ihbar merkezleri genellikle İnternet sektörü tarafından bağışlar yolu ile finanse edilmektedir. Merkez'in bir STK bünyesine geçişi mümkün olursa, yakın bir zamanda katılım öngördüğümüz EC Safer Internet Plus Program vasıtası ile AB fonlarından yararlanma yolunda büyük bir avantaj ve kolaylık sağlanmış olacaktır.

Diğer yandan, ihbar merkezi kurulmasının yasal dayanağını oluşturan 5651 sayılı Yasa bu merkezin kamu tarafından işletilmesini zorunlu kılmamıştır. Yasa, “gerekli her türlü teknik altyapıyı kurmak veya kurdurmak, bu altyapıyı işletmek veya işletilmesini sağlamak” şeklindeki düzenleme ile bu merkezin kamu dışında da kurulması ve işletilebilmesine olanak sağlamıştır. Dolayısı bu merkezin STK'lara devri bugün dahi mümkündür.

2) Bilgi İhbar Merkezi'nin hizmet sunumu mümkün olduğunca açıklık ve şeffaflık ilkeleri üzerine inşa edilmelidir. Bu politikanın bir gereği olarak da web sitesinde ihbarların alındıktan sonra hangi değerlendirme süreçlerinden geçtiği, nasıl değerlendirildiği, yapılan iş ve işlemlerin neler olduğu mümkün olduğunca açık bir şekilde, şekiller ve tablolar da kullanarak açıklanmalıdır. Bu çerçevede, içerik düzenlemesi, amacı, mantığı, mevcut mevzuat, nasıl uygulandığı, Bilgi İhbar Merkezi'nin bunun içerisinde nerede yer aldığı ve hedefinin ne olduğu herkesin anlayabileceği bir şekilde detaylı olarak izah edilmelidir.

Bu kapsamda, ihbardan sonra ihbarın sonucu ile ilgili olarak ihbar yapana geri dönüş yapılırken, bilgi mesajında ihbarın incelenme süreçleri ve incelemenin sonuçları ayrıntılı olarak anlatılabilir. Bu çerçevede, diğer bazı ülkelerin ihbar merkezlerinde yapıldığı gibi, her ihbara tekil bir ihbar numarasının verilmesi ve bu numaranın ihbarı yapan kişiler ile paylaşılması temin edilerek, bu kişinin daha sonra bu numara ile web sitesi üzerinden ihbarın değerlendirilme süreçleri ve akıbeti ile ilgili sorgulama yapabilmesi sağlanabilir. Böylece, ihbar yapan kişi anonim bir ihbarda bulunsada dahi, ihbarı ve ihbar süreçleri ile ilgili bilgilere kolaylıkla ulaşmış olacaktır.

3) Bilgi İhbar Merkezi'nin yine şeffaflık politikasının bir gereği olarak, faaliyet raporları, aylar ve yıllar itibarıyla ihbar istatistikleri, ihbar türleri, hangisinden ne kadarının erişim engellemeye sonuçlandığı açıklanmalıdır. İstatistiki veriler analiz yapmaya ve trendleri ortaya koymaya imkan verecek şekilde, dönemsel karşılaştırmaları da içerecek grafik, şekil ve tablolarla ortaya konulmalıdır. Hatta, diğer ülkelerin ihbar merkezlerine ait istatistiki verilerin de burada paylaşılması faydalı olacaktır.

4) İhbar Merkezi'nin etkinliğinin artırılmasıyla ilgili gündeme alınması gereken diğer bir konu da katalog dışı ihbarların durumudur. İhbar istatistikleri, yapılan ihbarların yaklaşık 1/3'nün katalog dışı olduğunu göstermektedir. Önemli bir yekün tutan bu katalog dışı ihbarların değerlendirilmesi gerekmektedir.

Bunun için önce bu ihbarlarda yer alan katalog dışı suçlarla ilgili şikayet konuları kendi içinde tasnif yapıp kategorize edilebildikten sonra ihbar alınan konularla ilgili olarak nereye müracaat edilebileceği ve ne yapılabileceği ile ilgili detaylı bilgiler web sitesinde yayınlanabilir. Yani, web sitesinde katalog dışı suçlar ve olaylara ilişkin olarak ilgili mevzuatın ve yapılabileceklerin açık ve anlaşılabilir bir şekilde izah edildiği ayrı bir bölüm oluşturulabilir ve buradaki içerik, genel bilinen İnternet suçlarının dışında, ihbarlardan gelen şikayetlere cevap olabilecek şekilde belirlenebilir. Böylece, işlem yapılamayan ihbarlarda yer alan konularda nereye başvurulacağı, neler yapılması gerektiği hususlarda yönlendirmede bulunulmuş olur.

Bunun dışında, bu ihbarlar aynı zamanda kullanıcıların birebir yaşadığı sorunları ve toplumsal talepleri yansıttığı için kullanıcıların nabzını tutan, İnternet toplumunun basıncını ölçen “İnternet barometreleri” olarak değerlendirilebilir. Dolayısıyla, İnternet kullanıcılarından gelen bu katalog içi ve dışı kategorize edilmiş ihbarlar dönemsel projeksiyonlarla analizlere konu edilerek, İnternet ve İnternet içerik politikalarının oluşturulmasında sosyolojik veri olarak kullanılabilir. Yani, ihbarlarla, İnternet kaynaklı şikayetlerin ve suçların hangi konularda yoğunlaştığı bilgisi üzerinden, bu alanı daha doğru anlama ve anlamlandırma; buna göre daha isabetli gelecek projeksiyonları çizme, yol ve yön belirleme mümkün hale gelebilir. En basitinden, bu analizlerden hareketle ortaya çıkan suç türleri ile mücadeleye öncelik verilebilir. Bu şekilde tespit edilen suç türleri üzerinde yoğunlaşarak, bu çerçevede alınması gereken sosyal, siyasal, hukusal önlemler hayata geçirilebilir.

Bu bağlamda, bir önceki maddede bahsi geçen ihbarların yayınlanması kapsamı içine katalog suçları dışındaki ihbarlara ait istatistiklerin de alınmasında fayda olacaktır. Bu ihbarların da kategorize edilmiş ve analizlere imkan sağlayacak şekilde diğer ihbar istatistikleri gibi işleminden geçirilerek paylaşılmasının, yukarıda söz konusu edilen süreçlerin daha sağlıklı ve şeffaf işlemesi açısından katkısı olacağı gibi, bu konularda çalışma yapan veya yapmak isteyen tüm araştırmacıların kullanımına imkan verecektir. Bu ise, alanla ilgili daha çok bilimsel veri, bilgi, bulgu, döküman, değerlendirme ve öneri demektir.

5) Mevcut hali ile Bilgi İhbar Merkezi’nin web sitesi büyük oranda sadece “İhbar” işlevini görmektedir. Merkez’in adında yer alan “Bilgi” kelimesinin karşılığı olan hizmet sunumu web sitesinde çok az bulunmaktadır. Halbuki, diğer ülkelerin benzer işlev gören ihbar merkezlerinin web sitelerinde, söz konusu merkezlerin isminde “Bilgi” kelimesi geçmemesine rağmen, özellikle bilinçlendirme ile ilgili bilgi ve dökümanlara çokça rastlanılmaktadır. Ülkemizde, bu önemli görevi yerine getiren tek kurum olan Bilgi İhbar Merkezi’nin resmi web sitesinde İnternetin güvenli kullanımına dair çocuk, genç, yetişkin, yaşlı, öğrenci, öğretmen, ana-baba toplumun her kesimine hitap eden cazip, kaliteli, doyurucu ve ilgi çekici her tür bilgi ve dökümanı yayınlamasında fayda vardır. Bilinirliliği ve tanınırlılığının artmasına

paralel olarak reytingi de yükselen bu web sitesinin, toplumda güvenli İnternet bilincinin geliştirilmesine yönelik içeriklerle kullanıcıyı tanıştırma ve buluşturma noktasında bir imkan olarak görülmesi gerekir.

Yine bu kapsamda dünyada ve Türkiye’de İnternet trendleri, kullanıcı eğilimleri, içerik düzenlemeleri, konuları, uygulamalar, yaklaşımlar, tartışmalar, bilimsel çalışmalar, araştırmalar, raporlar, anketler, istatistikler; özellikle katalog suçlar içinde yer alan içeriklere ilişkin veriler, bu içeriklerin sosyal zararları, riskler ve tehlikeler, ekonomik büyüklükleri vs. konularında yayınlanmış rapor ve bilimsel çalışmalar ayrı bir bölümde kullanıcıların ve araştırmacıların istifadesine sunulmalıdır.

Böylece, bu öneride bahsi geçenlerle birlikte, açıklık ve şeffaflık politikası gereği sunulan diğer bilgi ve dokümanların web sitesinde yer alması, Bilgi İhbar Merkezi’nin isminde geçen “Bilgi” kelimesinin hizmet sunumunda bir karşılığının bulunmasını da sağlamış olacaktır.

10. Yardım Hattı

Türkiye’de en kısa zamanda, İnternet ortamından ve içeriklerinden zarar gören ve yardıma muhtaç duruma düşen çocuklar ve gençlere hitap edecek ve psiko-sosyal, hukuki, teknik ve sağlıkla ilgili mağduriyetlerin hızlıca giderilebilmesi konusunda hizmet sunacak İnternet yardım hattı ve merkezi kurulması gerekmektedir. Bu merkezin STK’larca kurulup işletilmesi ideal olanıdır. Fakat, belki başlangıçta TİB bu konuda inisiyatif alarak, merkezi ve hattı açıp geçici bir süre işletebilir, fakat bir süre sonra mutlaka STK’larına devredilmelidir.

Kurulacak İnternet yardım hattı ve merkezi, 7/24 esasına göre ücretsiz olarak telefonla ve online çok yönlü hizmet sunmalıdır. Bu merkez, her yaştan kullanıcıya İnternet konusunda danışmanlık hizmeti ve yardım sağlamalıdır. Bu kapsamda katalog suçları yanında sanal güvenlik, siber dolandırıcılık, phishing, hacking, gizlilik ihlalleri, sanal zorbalık, ırkçılık, ayrımcılık, hakaret, iftira, tehdit, karalama, şiddet, vandalizm gibi konularda uzmanlarla görüşme ve bilgilendirme hizmeti sunulabilir. Bunun yanında, taciz, bağımlılık, zararlı içerik, pedofili, vb. sorunlarla

ilgili çocuklara, gençlere, ailelere, eğitimcilere, tüm özel ve kamu kurumlarına destek ve danışmanlık hizmeti sağlanabilir.

Ayrıca, merkez içinde ayrı bir hizmet alanı olarak, özellikle çocuklara ve gençlere yönelik olarak kaçırılma, cinsel istismara maruz kalma, sanal taciz, grooming, çocuk seks turizmi, kötü muammele gibi konularda hem ihbar alıp, hem de mağdurlara ve müptelalara profesyonel destek sunulabilir. Merkez, verdiği hizmetlerle ilgili etkin bir müdahale ve takip sistemi kurmalı; her arayan kişiye danışmanlık, gerekli ise acil yardım ve uzun dönemli rehabilitasyon desteği sağlamalıdır.

AB, bu nevi İnternet yardım merkezlerinin kurulmasını teşvik ettiğinden yardım merkezinin kurulması ve işletilmesi için katılım aşamasında olduğumuz EC Safer Internet Plus Program vasıtası ile AB'den finansal destek sağlanabilir. Keza, tüm çocuk yardım hattı merkezlerini bir araya getiren kuruluş olan CHI (Child Helpline International), çocukların cinsel istismarına ve kayıp çocuklara yönelik küresel mücadele veren ICMEC ve Avrupa'da kayıp ve istismara uğrayan çocuklar için çalışmalar yapan Missing Children Europe ile yaygın bir uluslararası çocuk hakları sivil toplum kuruluşu olan Save The Children gibi örgütlerle üyelik, işbirliği ve yardımlaşma imkanları aranabilir.

11. İhtisas Mahkemeleri

Bilişim teknolojilerinin hızla gelişmesi ve giderek daha kompleks ve karmaşık hukuki sorunlara neden olması yanında, çoğu zaman hızlı biçimde çözüme kavuşturulması gereği “Bilişim İhtisas Mahkemeleri”nin kurulmasını gerekli kılmaktadır. Özellikle bilişim, elektronik haberleşme ve siber suçlarla ilgili ihtisas sahibi hakim ve savcıların görev alacağı söz konusu mahkemeler, İnternet içerik düzenlemesiyle ilgili ihtilafların çözümünde ve erişim engellemeye ilişkin konularda da İnternetin kendine özgü teknik özelliklerini göz önünde bulundurarak daha makul, etkin ve isabetli kararların alınmasını temin edecektir.

EK-2: MÜLAKAT SORULARI

1. İnsanlık tarihi açısından bilgi toplumunu ve bu perspektif içinde “İnternet” olgusunu nasıl okumak gerekir? Bir değerlendirme yapar mısınız?
2. Türkiye’nin bilgi toplumu konusunu fayda-zarar/olumlu-olumsuz tüm yönleriyle bütüncül bir yaklaşım içinde ele aldığını ve bu yaklaşım içinde bilgi toplumu ve İnternet politikaları oluşturduğunu düşünüyor musunuz?
3. Dünyada ve Türkiye’de İnternetin yarar ve zararlarının objektif olarak yeterince ele alınıp değerlendirilerek İnternet politikaları oluşturulduğunu düşünüyor musunuz?
4. İnternetin düzenlenmesi tabirinden ne anlamak gerekir? İnternetin düzenlenmesi ile ilgili konuları (bilişim suçları ve fikri mülkiyet hakkı ile ilgili olanlar, içerikle ilgili olanlar, alan adı düzenlemeleri gibi) nasıl tasnif edebiliriz? Bunların aralarındaki sınırları nasıl belirleyebiliriz?
5. İnternet güvenliği veya güvenli İnternet kavramından ne anlıyorsunuz? İçerik güvenliği ile kullanım güvenliğini birbirinden ayırmak gerekir mi?
6. İnternet içerik düzenlemesi nedir? İnternet içerik düzenlenmesi mümkün müdür? İnternet bir özgürlük alanı olarak görülerek hiçbir düzenlenmeye tabi olmamalı mıdır?
7. İçerik düzenlemesinin kapsamı ve konuları neler olabilir? Bu çerçevede Dünyadaki ve Türkiye’deki durumu genel olarak değerlendirir misiniz?
8. İçerik düzenlemelerini kim, nasıl, hangi yöntemle yapabilir? Bu bağlamda devletlerin pozisyonu ve yaklaşımı nasıl olmalıdır? Bu konuda “yönetişim” modeli çözüm için uygun mudur?

9. Dünyada içerik düzenlemesi politikalarını nasıl buluyorsunuz? Ülkeler zararlı ve sakıncalı içeriklerle yeterince mücadele ediyor mu? Uluslararası işbirliği yeterli mi? Bu çerçevede İnternetin uluslararası yönetimini değerlendirir misiniz?
10. Türkiye'nin içerik düzenlemesi politikasını nasıl buluyor sunuz? Ülkemiz de zararlı ve sakıncalı içeriklerle yeterince mücadele yapıldığını düşünüyor musunuz? Bu kapsamda 5651 sayılı Yasa'yı ve TİB'nın uygulamalarını değerlendirir misiniz?
11. İnternet içeriğinin önemli bir kısmını oluşturan müstehcenlik ve pornografi barındıran içerikleri sosyal yapı için tehlike görüyor musunuz? Bu tür içeriklerle mücadelede neler yapılabilir? Nasıl bir yol izlemek gerekir?
12. İnternet içeriğinin düzenlenmesi ve bu kapsamda sakıncalı ve zararlı içerikle mücadele konusunda nasıl bir yasal çerçeve ve idari mekanizma önerirsiniz? Bu konuyla ilgili Türk kamu yönetimi sistemi içinde örnek bir yönetsel model teklifiniz var mı?

ÖZGEÇMİŞ

Adı ve Soyadı : Ahmet KILIÇ
 Doğum Tarihi ve Yeri : 01.04.1968 - Çorum
 Medeni Durumu : Evli ve 4 Çocuklu
 İletişim : Ahi Mesut Mh. 1865/1 Sk. No:3/2 Etimesgut/ANKARA
 İş Tel: 312 5865122, GSM: 0536 3356977
 e-Mail: akilic1990@gmail.com

Eğitim:

Yüksek Lisans : Sakarya Ünv., Sosyal Bilimler Ens., Kamu Yönetimi ve Siyaset Bilimi Anabilim Dalı-Yönetim Bilimleri Bilim Dalı, 1996-1998
 Lisans : Ankara Ünv., Siyasal Bilgiler Fak., Kamu Yön. Böl, 1986-1991
 Lise : Ankara Yenimahalle Teknik Lisesi, Elektronik Bölümü, 1982-1986
 Ortaokul : Trabzon Fatih Ortaokulu
 İlkokul : Trabzon Fatih İlkokulu

İş Deneyimi:

2007 - Devam : Telekomünikasyon İletişim Başkanlığı (Ankara), Uzman
 2005 - 2007 : Sağlık Bakanlığı Strateji Geliştirme Başkanlığı, (Ankara)
 2005 : Kamu Araştırmaları Vakfı (Ankara)
 2000 - 2005 : Ankara Ünv. Sos. Bil. Ens. (Ankara), Araştırma Görevlisi
 1999 - 2000 : Yüzüncü Yıl Ünv. İ. İ. B. Fak. (Van), Araştırma Görevlisi
 1994 - 1999 : Yüzüncü Yıl Ünv. Eğitim Fak. (Van), Araştırma Görevlisi
 1991 - 1994 : Gazetecilik, Askerlik