T.C.
GAZİ ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
KAMU HUKUKU ANABİLİM DALI

KAMU HUKUKU AÇISINDAN İNTERNET İÇERİĞİNİN DÜZENLENMESİ VE BU ALANDA DEVLETİN İDARİ YAPTIRIM UYGULAMA YETKİSİ

DOKTORA TEZİ

Hazırlayan
Yasin SÖYLER

Tez Danışmanı
Prof. Dr. Murat SEZGİNER

Ankara – 2013

T.C.
GAZİ ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
KAMU HUKUKU ANABİLİM DALI

KAMU HUKUKU AÇISINDAN İNTERNET İÇERİĞİNİN DÜZENLENMESİ VE BU ALANDA DEVLETİN İDARİ YAPTIRIM UYGULAMA YETKİSİ

DOKTORA TEZİ

Hazırlayan
Yasin SÖYLER

Tez Danışmanı
Prof. Dr. Murat SEZGİNER

Ankara – 2013

ONAY

Yasin SÖYLER tarafından hazırlanan *"Kamu Hukuku Açısından İnternet İçeriğinin Düzenlenmesi ve Bu Alanda Devletin İdari Yaptırım Uygulama Yetkisi"* başlıklı bu çalışma, *25.10.2013* tarihinde yapılan savunma sınavı sonucunda *oybirliği/oyçokluğu* ile başarılı bulunarak jürimiz tarafından Kamu Hukuku Anabilim Dalı'nda *Doktora tezi* olarak kabul edilmiştir.

Prof. Dr. Murat Soyer
Başkan

Prof. Dr. ANIL ÇEÇEN
Üye

Üye

Prof. Dr. Hasan TUNG
Üye

Prof. Dr. Cumhur ŞAHİN
Üye

Prof. Dr. Bahtiyar Akyılmaz

ÖZET

SÖYLER, Yasin. Kamu Hukuku Açısından İnternet İçeriğinin Düzenlenmesi ve Bu Alanda Devletin İdari Yaptırım Uygulama Yetkisi, Doktora Tezi, Ankara, 2013.

Devletin interneti düzenlemesi birçok eleştiriyi de beraberinde getirmektedir. Özellikle kamu hukuku kapsamında yürürlüğe konulan düzenlemeler, temel hak ve özgürlük ihlali iddialarının ileri sürülmesine neden olabilmektedir. Bu çerçevede, internet içeriğine ilişkin devlet tarafından yapılan düzenlemelerin kamu hukuku ekseninde incelenmesini konu alan bu çalışmada, genel olarak devletin internete yaklaşımı tespit edilmeye çalışılmış ve temel hak ve özgürlük alanına ilişkin ortaya çıkan çatışmaların çözümünde, düzenleme konusunda hassas bir dengenin gözetilmesi gerekliliği ortaya konulmuştur. Bu gereklilik ortaya konulurken, internet ve devlet denildiğinde ilk akla gelenin sansür mü olması gerektiği, internetin devlet tarafından hiç müdahale edilmemesi gereken bir alan mı olduğu, yoksa devletin bu konuda bir düzenleme hakkının mı bulunduğu, interneti kimin yönettiği, internetin ortaya çıkardığı hukuksal sorunların çözümünde devletin nerede olduğu, devletlerin interneti düzenleme konusundaki uluslararası girişimlerinin ne anlam ifade ettiğine yönelik değerlendirmeler yapılmıştır. Ayrıca, bilişim suçlarıyla mücadele, internet ortamında kişisel verilerin korunması, önleme amaçlı internet iletişiminin denetlenmesi, ulusal siber güvenliğin sağlanması, internet içeriğine erişimin engellenmesi, filtreleme, içeriğin yayından çıkarılması ve cevap hakkı, internet servis sağlayıcıların cezai ve idari sorumlulukları, alan adlarının yönetimi gibi konuların devlet ve internet ilişkisinde nerede yer aldığı, ülkemizde internetin düzenlenmesi konusunda yürürlüğe konulan kanunların sansür içerikli kanunlar mı olduğu ve bu kanunların getirmiş olduğu düzenlemelerin demokrasi ve insan hakları bağlamında ne anlam ifade ettiğine yönelik konular üzerinde de durulmuştur. Bu ve benzeri sorulara cevap bulmayı

amaçlayan bu çalışmada kamu hukuku açısından bir bakış açısı ortaya konulmaya çalışılmıştır.

Anahtar Sözcükler

1. İnternetin düzenlenmesi.
2. Kamu hukuku ve internet.
3. Erişimin engellenmesi.
4. İfade özgürlüğü ve internet.
5. İnternet sansürü.

ABSTRACT

SÖYLER, Yasin. State's Competence of Internet Regulation and Imposing Administrative Sanctions With Regards to Public Law, Doctoral Thesis, Ankara, 2013.

Regulation of the Internet by the state brings about many criticisms. Especially regulations which are put into action within the context of public law may cause assertions regarding violations of the fundamental rights and freedoms. Starting from this point of view, in this study which discusses examination of the regulations made by state concerning the content of Internet within the context of public law, as a general thing, it is attemted to determine the approach of the state to the Internet and put forth the necessity of establishing a sensitive balance regarding regulation in the process of solving the conflicts with relation to the field of the fundamental rights and freedoms. While this requirement is presented, it is evaulated whether censorship must come to mind when the subjects are state and Internet, Internet is a field in which state should never intervene or state does have a regulation right in the area of Internet, who rules the Internet, where state stands in the process of solving legal problems caused by Internet, what the international initiatives concerning the regulation of Internet do mean. Besides it is put empasis on where the subjects such as struggle with cyber crimes, storing personal data, control of Internet communication with the aim of interception, providing national cyber security, prevention of access to the content of Internet, filtering, removal of content from transmission and right of reply, criminal and administrative liabilities of Internet service providers, conduct of Internet domain names, do take place concerning the relation between state and Internet, whether laws which are put into effect regarding the regulation of the Internet in our country are cencorship themed and finally what the regulations made by these laws does amount to in the context of democracy and human rights. In this study which aims at finding answers for

these issues, it is made an attempt on manifesting a perspective from the point of public law.

Key Words

1. Regulation of Internet.
2. Public law and Internet.
3. Filtering.
4. Freedom of expression and Internet.
5. Internet censorship.

ÖNSÖZ

Devletin interneti düzenlemesi birçok eleştiriyi de beraberinde getirmektedir. Özellikle kamu hukuku kapsamında yürürlüğe konulan düzenlemeler, temel hak ve özgürlük ihlali iddialarının ileri sürülmesine neden olabilmektedir. İnternet içeriğine ilişkin devlet tarafından yapılan düzenlemelerin kamu hukuku ekseninde incelenmesini konu alan bu çalışmada, genel olarak devletin internete yaklaşımı tespit edilmeye çalışılmış ve temel hak ve özgürlük alanına ilişkin ortaya çıkan çatışmaların çözümünde, düzenleme konusunda hassas bir dengenin gözetilmesi gerekliliği ortaya konulmuştur.

İnternetin kamu hukuku açısından düzenlenmesi ve devletin bu alanda temel hak ve özgürlüklere yaklaşımının gösterilmesi şeklinde spesifik bir bakış açısıyla ele alınmış olsa da, devletin düzenleme öngördüğü alanların geniş olması nedeniyle bu çalışmada birçok kamu hukuku konusunun ele alınması gerekmiştir. Bilişim suçlarından kişisel verilerin korunmasına, ulusal siber güvenliğin sağlanmasından önleme amaçlı internet iletişiminin denetlenmesine kadar geniş bir yelpazede spesifik bir amaç ortaya koymak zaman zaman çalışmanın kapsamını netleştirmek açısından sıkıntılı olabilmiştir. Ancak, "*kamu hukuku açısından devletin interneti düzenleme yetkisi"* gibi spesifik bir bakış açısıyla bu konulara yaklaşıldığından çalışmanın kapsamı zamanla yerine oturmuştur.

Bu çalışmanın hazırlanmasında;

Danışmanım olarak çalışmam boyunca bana rehberlik eden ve ışık tutan değerli Hocam Sayın Prof. Dr. Murat SEZGİNER'e

Tez İzleme Komitesi üyesi olarak çalışmamı başından sonuna takip eden ve değerli katkılarıyla çalışmanın verim kazanmasını sağlayan saygıdeğer hocalarım Sayın Prof. Dr. Anıl ÇEÇEN'e ve Sayın Prof. Dr. Hasan TUNÇ'a,

En içten duygularla teşekkürlerimi sunarım.

İÇİNDEKİLER

İKİNCİ BÖLÜM
İNTERNET VE DÜZENLEME

ÜÇÜNCÜ BÖLÜM
DÜZENLEME ALANLARI

DÖRDÜNCÜ BÖLÜM
DEVLETİN İNTERNETİ DÜZENLEME ARAÇLARI

KISALTMALAR

AB : Avrupa Birliği
ABD : Amerika Birleşik Devletleri
ACMA : The Australian Communications and Media Authority
a.g.e. : Adı geçen eser
a.g.m. : Adı geçen makale
AİHM : Avrupa İnsan Hakları Mahkemesi
AİHS : Avrupa İnsan Hakları Sözleşmesi
ARPANET : Advanced Research Projects Agency Network
AÜHFD : Ankara Üniversitesi Hukuk Fakültesi Dergisi
AÜSBFD : Ankara Üniversitesi Siyasal Bilgiler Fakültesi Dergisi
AYM : Anayasa Mahkemesi
BBC : British Broadcasting Corporation
Bkz. : Bakınız
BM : Birleşmiş Milletler
BTK : Bilgi Teknolojileri ve İletişim Kurumu
C. : Cilt
ccTLDs : Country code top level domains
CIA : Central Intelligence Agency
CIPA : Children's Internet Protection Act
CMK : Ceza Muhakemesi Kanunu
COPPA : The US Children's Online Privacy Protection Act
DDoS : Distributed Denial of Service
DEÜHFD : Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi
DİDDK : Danıştay İdari Dava Daireleri Kurulu
DHS : Department of Homeland Security
DOD : Department of Defense
DOJ : Department of Justice
DoS : Denial of Service
E : Esas

EC : European Community
EJIL : European Journal of International Law
EÜHFD : Erzincan Üniversitesi Hukuk Fakültesi Dergisi
FBI : Federal Bureau of Investigation
FTP : File Transfer Protocol
FSEK : Fikir ve Sanat Eserleri Kanunu
GÜHFD : Gazi Üniversitesi Hukuk Fakültesi Dergisi
gTDLs : Generic top level domains
HIPAA : The Health Insurance Portability and Accountability Act
HTTP : Hyper Text Transfer Protocol
HMK : Hukuk Muhakemeleri Kanunu
IANA : Internet Assigned Numbers Authority
ICANN : Internet Corporation of Assigned Names and Numbers
IETF : Internet Engineering Task Force
IP : Internet Protokol
Iss. : Issue
IT : Information Technology
ITU : International Telecommunication Union
İÜHFM : İstanbul Üniversitesi Hukuk Fakültesi Mecmuası
K : Karar
KHK : Kanun Hükmünde Kararname
LICRA : La Ligue Contre Le Racisme et L' Antisemitisme
md. : Madde
MASAK : Mali Suçları Araştırma Kurulu
MERNİS : Merkezi Nüfus İdaresi Sistemi
NATO : North Atlantic Treaty Organization
NSA : National Security Agency
ODTÜ : Orta Doğu Teknik Üniversitesi
OECD : Organization for Economic Co-operation and Development
Ö : Örnek
RG. : Resmi Gazete
S. : Sayı

s. : Sayfa
SLDs : Second level domains
SMTP : Simple Mail Transfer Protokol
TAAD : Türkiye Adalet Akademisi Dergisi
TBB : Türkiye Barolar Birliği
TCK : Türk Ceza Kanunu
TCP/IP : Transmission Control Protokol / Internet Protokol
TİB : Telekomünikasyon İletişim Başkanlığı
TLDs : Top level domains
TMG : Telemedia Act
TRABİS : .tr ağ bilgi sistemi
TÜBİTAK : Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
UYAP : Ulusal Yargı Ağı Projesi
vd. : Ve devamı
Vol. : Volume
WWW : World Wide Web

TABLOLAR

GİRİŞ

Ülkemizde *internetin düzenlenmesi (Internet regulation)* konusunda ulusal ve uluslararası gelişmele ri ve teoriyi genel bir yaklaşım içerisinde ortaya koymaya çalışan hukuksal çalışma, oldukça az sayıdadır. Spesifik olarak internetin bazı alanlarına yönelik yapılan çalışmalarda ise genel eğilim, devleti internet alanında bir baskı ve sansür unsuru olarak gösterme yönündedir. Arama motorlarında "*internet ve düzenleme"* kelimesi arandığında devleti hedef alan ve sansür iddiasında bulunan onlarca yazı bulunabilecektir. Peki gerçekten, internet ve devlet denildiğinde ilk akla gelen yasakçılık ve sansür mü olmalıdır? Bu dünyanın her yerinde böyle midir? ABD, AB ve Avrupa devletlerinin internete hukuksal yaklaşımı nasıldır? İnternet devlet tarafından hiç müdahale edilmemesi gereken bir alan mıdır? Yoksa devletin bu konuda bir düzenleme hakkı bulunmakta mıdır? İnternet üzerinde egemen güçler kimlerdir? İnterneti kim yönetmektedir? İnternetin ortaya çıkardığı hukuksal sorunların çözümünde devlet nerede olmalıdır? Devletlerin interneti düzenleme konusundaki uluslararası girişimleri ne anlam ifade etmektedir? Bilişim suçlarıyla mücadele, internet ortamında kişisel verilerin korunması, önleme amaçlı internet iletişiminin denetlenmesi, ulusal siber güvenliğin sağlanması, internet içeriğine erişimin engellenmesi, filtreleme, içeriğin yayından çıkarılması, cevap hakkı, internet servis sağlayıcıların cezai / idari sorumlulukları, alan adlarının yönetimi gibi konular devlet ve internet ilişkisinde nereye oturmaktadır? Ülkemizde internetin düzenlenmesi konusunda yürürlüğe konulan kanunlar sansür içerikli kanunlar mıdır? Bu kanunların getirmiş olduğu düzenlemeler demokrasi ve insan hakları bağlamında nerede yer almaktadır? Bu ve benzeri sorulara cevap bulmaya yönelik bu çalışmada kamu hukuku açısından bir perspektif ortaya konulmaya çalışılmıştır.

İnternet ile ilgili konular, kapsadığı hukuksal alan itibariyle oldukça geniş bir yelpaze oluşturmaktadır. Bu geniş alan içerisinde, internet ile ilgili spesifik bir konuda çalışma yapmak en çok başvurulan yöntemlerdendir. Fakat, bu tür çalışmaların karşılaştığı zorluk, internetin bir bütün olarak değerlendirilememesinden dolayı sadece spesifik bir konunun çözümüne

yönelik getirilen formüllerin, internet ile ilgili diğer alanlarda geçerlilik bulamamasıdır. Bu yaklaşım, getirilen çözümleri gerçeklikten uzaklaştırmakta ve olumlu bir internet gelişiminin sağlanamaması sonucunu doğurmaktadır. Bu çalışmada en azından kamu hukuku perspektifinden, internet bir bütün olarak değerlendirilmeye ve spesifik bir alana yönelik olarak bir çözüm getirildiğinde bunun diğer çözümlere yapacağı etki göz önünde bulundurulmaya çalışılmıştır.

Doktrinde internet ile ilgili olarak yapılan çalışmalar genellikle bilişim suçları ve fikri mülkiyet haklarının korunması hukuku bağlamında ele alınmıştır. İnternet alanının anayasa ve idare hukuku bakış açısından incelendiği çalışma sayısı ise oldukça azdır. Halbuki, internetin düzenlemesini öngören hukuk kuralları kamu düzeni, kamu yararı, ulusal güvenlik, ailenin korunması ve çocuk hakları, gençliğin korunması, temel hak ve özgürlükler ve bunların sınırlanması, kişisel verilerin korunması gibi kamu hukuku konuları ile ilgili olduğu gibi bir taraftan da yapılan düzenlemeler bilgi ve iletişim teknolojileri sektörünün regülasyonu mahiyetindedir. Devlet bu sektörü düzenlemekte ve gerekli gördüğü yerlerde yaptırımlar öngörmektedir.

İnternetin düzenlenmesi konusunu kamu hukuku açısından incelemek, internet ile ilgili konuların genel olarak hukuk içerisinde nerede yer aldığının belirlenmesine de katkı sağlayacaktır. Bu çerçevede kamu hukuku içerisinde değerlendirilebilecek internet ile ilgili konular bir bütün içerisinde analiz edilebilecektir. İnternet ile ilgili çoğu konu, kamu hukuku – özel hukuk ayrımında herhangi bir tarafa tam olarak yerleştirilememektedir. Bu nedenle internet ile ilgili yapılan hukuksal çalışmalar çoğu zaman bu ayrımı gözden kaçırmakta ve iki farklı hukuk alanının kendine özgü yaklaşım ve kurallarının internet alanında uygulanamaması sonucunu doğurmaktadır. Örneğin, internet alan adlarının yönetiminin incelendiği çalışmalarda kamu hukuku – özel hukuk ayrımının bu konuya yaklaşımı gözden kaçırılmaktadır. Aslında internet alan adlarının yönetimi her şeyden önce bir kamu hukuku konusudur ve bu yönüyle ele alınması gerekir. İnternet alan adlarının yönetiminde bir kamu gücü kullanılmaktadır. Alan adlarının marka hukuku çerçevesinde ortaya çıkardığı hukuksal sorunlar ise bir özel hukuk konusudur ve bu, kamu

hukuku alanı dışında kalan bambaşka bir konudur. Internet alan adlarının yönetimine ilişkin bir çalışma bu ayrımı mutlaka yapmak zorundadır. Fakat doktrinde genellikle alan adlarının yönetimine ilişkin yapılan çalışmalarda konunun kamu hukuku boyutu ihmal edilerek, konu sadece alan adı - marka uyuşmazlıklarına indirgenmekte ve incelenmektedir.

İnternet ile ilgili konularda kamu hukuku – özel hukuk ayrımı yaparak bir çalışma yapmanın bazı faydaları da bulunmaktadır. Örneğin, kişisel verilerin korunması, kamu hukuku konusu olarak telakki edildiğinde kişisel verilerin işlenmesine ilişkin ortaya çıkan bir uluslararası hukuksal sorunda devlet, kolayca yetki iddiasında bulunabilecektir. Kamu hukuku ile ilgili konular devletin egemenlik yetkisi ile ilgili bir boyut taşımaktadır ve devletler egemenlik yetkilerini her durumda kullanmaktadır.

Kamu hukuku açısından internetin düzenlemesine ilişkin yaklaşımların incelenmesi, genel olarak devletin internete yaklaşımını göstermesi açısından da önemlidir. Devletin internete yaklaşımını görmek ancak konunun kamu hukuku açısından incelenmesi ile görülebilir. Kamu hukuku açısından yapılan düzenlemelerin internet içeriğine müdahalesi, getirilen sınırlandırmalar ve öngörülen yaptırımlar, devletin interneti düzenlerken demokratik bir yaklaşım sergileyip sergilemediğini göstermektedir.

Bazı ülkelerde idare, internet üzerinde araya bir yargı kararı girmeksizin doğrudan yetki kullanabilmekte ve internet içeriğine erişimi engelleyebilmektedir. Böyle bir durumda erişimi engellenen içerik sahibi, idarenin uygulamış olduğu yaptırımı haksız buluyorsa yargı mercilerine başvurarak hakkını arayabilmektedir. Bazı ülkelerde ise idarenin doğrudan internet üzerinde böyle bir yetki kullanması mümkün değildir. Bu ülkelerde, hukuka aykırı içerik taşıdığı düşünülen internet içeriğine erişimin engellenebilmesi için bir mahkeme kararına ihtiyaç duyulmaktadır. Bu iki farklı sistemin karma bir şekilde uygulandığı ülke örnekleri de bulunmaktadır. Bu çerçevede, araya herhangi bir yargı kararı girmeksizin idarenin internet üzerinde doğrudan idari yaptırım uyguladığı sistem, ülkemizin bu sistemi belli bir ölçüde uygulayan bir ülke olması nedeniyle özellikle ilgi alanımıza girmektedir.

İnternet alanı hızlı bir gelişim göstermektedir. Bu nedenle bu alana ilişkin yapılan çoğu hukuksal çalışma kısa süre içerisinde güncelliğini yitirebilmektedir. Bu çalışma internet alanındaki güncel gelişmelerin ortaya konulması açısından da faydalı olacaktır.

Çalışmanın kapsamı bazı açılardan sınırlandırılmıştır. İlk sınırlandırma, "*internet"* kavramına ilişkindir. İnternet ortamı dışında kalan kişisel veya kurumsal bilgisayar sistemlerinin, televizyon, radyo ve basın gibi kitle iletişim araçlarının, telefon, telgraf ve fax gibi kişisel haberleşme araçlarının düzenlenmesine ilişkin konular çalışma alanı dışında kalmaktadır. İnternet kavramı ile bağlantılı bir diğer sınırlandırma, internet içeriğinin düzenlenmesine ilişkin konuların incelenecek olmasıdır. Bu çerçevede internet iletişim altyapısının düzenlenmesine ilişkin konular inceleme alanımız dışında kalmaktadır.

İkinci sınırlandırma "*kamu hukuku"* açısından internete yaklaşımdır. Bu çerçevede özel hukukun alanına giren, internet ortamında tüketicinin korunması, e-ticaret, fikri mülkiyet haklarının korunması, hukuksal sorumluluk, elektronik imza, rekabet hukuku kuralları ve ticari markalar ile ilgili konular bu çalışma kapsamında incelenmemiştir. Bununla birlikte, söz konusu alanları birbirinden kesin bir çizgi ile ayırmanın mümkün olmadığı noktalarda ilgili olduğu ölçüde söz konusu bazı konulara da ilgili bölümlerde değinilmiştir.

Diğer bir sınırlandırma, "*devlet"* kavramına ilişkindir. Özel hukuk tüzel kişilerinin kendi bünyelerinde interneti düzenleme yaklaşımları çalışmanın kapsamı dışında kalmaktadır.

Nihayet, son sınırlandırma incelemenin yapılacağı ülkeler itibariyledir. İnternet ile ilgili bir konuda araştırma yapmak, mutlaka konuyu bir ülke tekelinden çıkararak incelemeyi gerektirmektedir. İnternet her yerdedir ve sorunlar ve çözümler aynı ya da benzerdir[1]. Ayrıca, internetin ortaya çıkardığı sorunların ve çözümlerin büyük bir kısmı uluslararası bir nitelik de

[1] Dan Svantesson, "A Legal Method for Solving Issues of Internet Regulation", **International Journal of Law and Information Technology,** Vol. 19, No. 3, Oxford University Press, 2011, s. 245.

taşımaktadır. Bu çerçevede, devletlerin interneti düzenleme ve yaptırım uygulama yaklaşımları mümkün olduğunca karşılaştırmalı bir çerçevede analiz edilmeye çalışılmıştır. Bir diğer deyişle, devletlerin interneti nasıl algıladığı, düzenlediği, yaptırım öngördüğü, hangi alanlara önem verdikleri ve bu düzenlemeleri nasıl uyguladıklarına ilişkin konular bu çalışmaya yön vermiştir. Bununla birlikte, devletlerin internet ile ilgili kamu hukuku konularına yaklaşımları sistematize edilerek, ortaya çıkan yaklaşımlar veya ilkeler ekseninde bir değerlendirme yapılmaya çalışılmıştır. Bu yapılırken de ABD, Almanya ve İngiltere gibi batı ülkelerinin düzenlemeleri esas alınmıştır. İnternet düzenlemesinde anti-demokratik gösterilen ülke düzenlemeleri incelenmemiştir. İncelenecek ülke itibariyle bir sınır getirilmesi ihtiyacı sınırsız bir alanda uğraş vermekten kaçınma düşüncesinden kaynaklanmıştır. Ayrıca, aksi yönde bir yaklaşımın başarılı bir sonuç ortaya çıkaramayacağı düşünülmüştür.

Bu çerçevede, çalışmanın birinci bölümünde internet ve hukuk ilişkisi ele alınmış; internetin gelişimi, teknik yönetimi, bilgi toplumuna etkisi, hukuksal açıdan önem taşıyan fonksiyonları ve farklı hukuk disiplinleri ile ilişkisi incelenmiştir. İkinci bölümde, internetin düzenlenmesi konusunda uluslararası yetki, düzenleme konusundan ileri sürülen teoriler, düzenlemenin insan haklarına etkisi ve idarenin düzenleme yetkisi ile ilişkisi incelenmiştir. Üçüncü bölümde devletin interneti kamu hukuku açısıdan düzenlediği alanlara girilmiş ve bu çerçevede bilişim suçlarıyla mücadele, internet ortamında kişisel verilerin korunması, önleme amaçlı internet iletişiminin denetlenmesi ve ulusal güvenliğin sağlanması konuları ele alınmıştır. İnternette yükümlülük öngörülen sujeler, bunların cezai ve idari sorumlulukları, internet içeriğine erişimin engellenmesi ve filtreleme konuları ise devletin interneti düzenleme araçları olarak dördüncü bölümde incelenmiştir.

BİRİNCİ BÖLÜM
İNTERNET VE HUKUK

I. İNTERNET

"*İnternet",* İngilizce bir terimdir. Kavramsal olarak, birbirine bağlı ağ (interconnected networks) anlamına gelmektedir. İnternet, bilgisayar ağları içerisindeki özel bir ağı ifade etmektedir. Dünya çapında bilgisayar ağlarının birbirine bağlanması ile oluşmuş evrensel bir iletişim ağı olarak internet dünyanın en hızlı gelişen ve belki de toplumları en fazla etkileyen teknolojilerinden biridir. İnternet, ağların ağı (network of networks) olarak da tanımlanmaktadır.

İnternet, küresel yapıda bir iletişim ağıdır. Günümüzde dünyanın her tarafından insanlar internete bağlanmakta ve etkinliklerini internet üzerinden yürütebilmektedir. Haziran 2012 tarihi itibariyle dünyada 2.405.518.378 internet kullanıcısı bulunmaktadır[2]. Bir bilgi internette yayınlandığı an, artık o bilgi dünyada internet üzerinden herkesin ulaşabileceği ve görebileceği bir bilgi haline gelmektedir.

İnternetin, merkezi olmayan bir yapısı vardır[3]; tek bir elden kontrol edilmesi mümkün değildir[4]. Ancak, ICANN ve ABD'nin internet üzerindeki etkinliği bu yargıyı tartışmaya açmaktadır. Bu tartışma, aşağıda internetin teknik yönetimi bölümünde yapılmıştır.

İnternet, sahip olduğu özellikler ile günümüz dünyasının vazgeçilmez teknolojileri arasında yer almaktadır. İnternet, gizli iletişime imkan tanımaktadır; nispi olarak ucuz bir iletişim aracıdır ve her geçen gün kullanım maliyeti düşmektedir; herkesin kullanımına açıktır; kişilerin birçok faaliyeti üzerinde gerçekleştirebildiği çok yönlü bir kullanım özelliğine sahiptir. Diğer birçok bilişim teknolojisinden farklı olarak internet kişilere araştırma, bilgi edinme, ifade etme, siyasal katılımcılık, eğlence, kültürel etkinlikler, kişisel

---

[2] http://www.internetworldstats.com/stats.htm, 28.12.2012.

[3] Yaman Akdeniz, Kerem Altıparmak, **İnternet: Girilmesi Tehlikeli ve Yasaktır Türkiye' de İnternet İçerik Düzenlemesi ve Sansüre İlişkin Eleştirel Bir Değerlendirme**, İmaj Yayınevi, Ankara, Kasım 2008, s. 1.

[4] Julie, L. Henn, "Targeting Transnational Internet Content Regulation", **Boston University International Law Journal**, Vol. 21: 157, 2003, s. 160.

iletişim, e-devlet hizmetleri, bankacılık, ticari faaliyetler gibi hizmetlerden yararlanma ve aktif katılım imkanı sağlamaktadır.

A. İnternetin Gelişimi ve Teknik Altyapısı

ABD Savunma Bakanlığı bünyesinde oluşturulan DARPA (Defence Advanced Research Project Agency) isimli birim, mühtemel bir nükleer saldırı sonrasında askeri birimler arasındaki iletişiminin kesilmesi durumunda alternatif bir iletişim ağı oluşturmayı amaçlayan bir proje başlatmıştır. ARPANET (Advanced Research Projects Agency Network) olarak adlandırılan bu proje ile ilk kez 1969 yılında birkaç Amerikan üniversitesinde bulunan merkezi bilgisayarlar arasında bağlantı gerçekleştirilmiştir. Zaman içerisinde diğer üniversitelerin de sisteme bağlanmasıyla ARPANET'in kapsamı oldukça genişlemiştir. 1972 yılında sistem içerisinde elektronik posta kullanılmaya başlanmıştır. 1971 yılında Ağ Kontrol Protokolü (Network Control Protocol-NCP) ile gelişen sistem, 1983 yılında farklı özelliklere sahip bilgisayar ve bilgisayar ağlarının internette ortak bir dil üzerinden iletişime geçebilmelerine imkan tanıyan TCP/IP Protokolünün geliştirilmesiyle birlikte internet iletişimine ivme kazandırmıştır. Aynı yıl ARPANET, askeri (MILNET) ve sivil olmak üzere iki ayrı ağa ayrılmış ve sivil ağ diğer üniversiteler, kamu ve özel sektör kuruluşlarının katılımına açılmıştır. World Wide Web (WWW)'in ilk kez Tim Berners Lee tarafından 1990 yılında CERN (European Laboratory for Particle Physics)'de keşfedilmesi ve bu yıllarda internetin ticari kuruluşlarca kullanılımına izin verilmesi ile birlikte, internetin ticari değeri de yükselmeye başlamıştır.

İnternet iletişiminin sağlanması için bazı protokoller oluşturulmuştur. Protokoller sayesinde internet üzerinden bilgi iletimi ve paylaşımı gerçekleştirilebilmektedir. Farklı donanım ve yazılım özelliklerine sahip bilgisayarların birlikte çalışabilmeleri (interoperability) için ortak bir dil kullanmaları gerekir. Bunu sağlayan kurallar bütününe protokol denilmektedir. Bu protokoller, internet protokolleri veya TCP/IP (Transmission Control Protokol/İnternet Protokol) protokoller ailesi olarak adlandırılmaktadır. TCP/IP protokoller ailesi içerisinde birçok protokol bulunmaktadır. Bunlardan en

önemlileri TCP ve IP olduğu için bu isim kullanılmaktadır. TCP gönderilen verilerin yerine ulaşmasına; IP ise gönderilen bilginin istenilen adrese yollanmasına imkan tanımaktadır. Yine bu protokoller içerisinde yer alan FTP (file transfer protocol), dosya aktarımını; SMTP (simple mail transfer protocol), elektronik dosya iletimini; HTTP (hyper text transfer protocol), WWW ortamında bilgi aktarımının kural ve yöntemlerini belirleyen sistemlerdir. TCP/IP protokolünün diğer iletişim ağlarında da kullanılması mümkündür.

İnternete bağlanan her bilgisayarın bir IP numarası vardır ve bu numara sadece o bilgisayara aittir. IP adresleri, internet üzerinde iletişime geçen alıcı ve göndericiyi tanımlar. Günümüzde aktif kullanımda olan IPv4 ve IPv6 olmak üzere iki IP adresi versiyonu bulunmaktadır. IPv4, 1983 yılında kullanılmaya başlanmıştır. Bunlar, 32 bitlik düzene sahiptir. IPv4 sistemi yaklaşık 4 milyar farklı adrese imkan tanıyan bir protokol olmasına rağmen günümüzde bu sistem yetersiz kalmış ve IPv6 sistemi geliştirilmiştir. IPv6 versiyonu 1999 yılında kullanılmaya başlanmıştır. IPv6 adresleri 128 bitlik bir düzenden oluşmaktadır[5]. IPv6 ile daha fazla adresin kullanılması mümkün olacaktır.

İnternete bağlanabilmek için bir bilgisayar, modem, telefon bağlantısı ve bağlantı sağlayacak internet servis sağlayıcının bulunması yeterlidir. İnternete bağlandığımız zaman web sayfalarını görüntülemeye yarayan web tarayıcılarına (web browser), web adreslerinin yazılması ile ulaşılmak istenen web sayfaları açılmaktadır.

Ülkemizde 1991 yılında, Türkiye'nin internet bağlantısını gerçekleştirmek amacıyla ODTÜ ve TÜBİTAK tarafından TR-NET isimli bir proje oluşturulmuş ve ilk internet bağlantısı 1993 yılında ODTÜ'nün Washington ağına bağlanması ile sağlanmıştır.

[5] http://www.iana.org/numbers, 28.01.2012.

B. İnternetin Teknik Yönetimi

Bu bölümde internetin uluslararası ve ulusal teknik yönetimi incelenmiştir. Teknik yönetim, internet alan adları, IP adresleri ve ana sunucu (root server) yönetimi ile ilgili olarak ele alınmıştır. Teknik yönetiminin internet altyapısı ile ilgili bir yönü bulunduğu gibi içerik düzenlenmesi ile ilgili dolaylı bir yönü de bulunmaktadır. İçerik üzerinde uluslararası düzeyde düzenleyici bir otorite bulunmamaktadır. Ancak, internetin teknik yönetimi ile internet içeriğinin etkilenmesi mümkündür. İnternetin teknik yönetimi, uluslararası ve ulusal bir boyut içermektedir. Uluslararası boyut açısından İnternet Tahsisli Sayılar ve İsimler Kurumu (Internet Corporation of Assigned Names and Numbers - ICANN); ulusal boyut açısından da her devletin ulusal hukuk düzenlemelerine göre oluşturdukları yapılanmaların ve düzenlemelerinin ele alınması gerekir.

İnternetin teknik yönetiminin hem kamu hem de özel hukuk yönü bulunmaktadır. Kamu hukuku açısından bu yönetim, internet üzerinde uluslararası bir yetkinin kullanılması açısından özellikle önem taşımakta, özel hukuk açısından ise e-ticaretin en önemli noktalarından birisini oluşturmaktadır. Bu bölümde internetin teknik yönetimi, kamu hukuku açısından ele alınmıştır.

1. İnternet Tahsisli Sayılar ve İsimler Kurumu (ICANN)

İnternet alan adlarının yönetimi, 1993 yılında ABD Ulusal Bilim Vakfı (NSF) tarafından beş yıllık bir süre için Network Solutions Inc. (NSI) şirketine verilmiştir. IP adreslerinin tahsisi ise internetin ilk ortaya çıktığı yıllardan beri DARPA tarafından finanse edilen İnternet Tahsisli Sayılar Kurumu (Internet Assigned Numbers Authority - IANA) tarafından gerçekleştirilmiştir[6].

Alan adları ile marka sahipleri arasında ortaya çıkan hukuksal uyuşmazlıkları çözmedeki yetersizlik, alan adlarının önem kazanması ve bunun rekabeti daha çok etkilemeye başlaması, yeni birinci derece alan adlarına ihtiyaç duyulması, bunların belirlenmesinin daha katılımcı ve

[6] Hasibe Işıklı, **İnternet Alan İsimleri Sistemi Markalar ve Alan İsimleri Arasındaki İlişki**, http://ekutup.dpt.gov.tr/, Şubat 2001, s. 15.

demokratik bir yapılanma ile gerçekleştirilme talepleri, alan adları ve IP adresleri yönetiminin daha katılımcı, özerk, rekabete dayanan ve daha meşru bir kuruluşa devrini zorlamıştır[7]. Bu gelişimde, alan adları yönetiminin özel sektöre bırakılmasının internetin geleceği ve ABD'nin ekonomik çıkarları açısından daha faydalı görülmesi, alan adları yönetiminin ABD'nin kontrolünde olmasına uluslararası çevrelerden yükselen itirazların dozunu artırmaya başlaması gibi hususlar da etkili olmuştur. Bu gelişmelerin bir sonucu olarak 1998 yılında ABD Ticaret Bakanlığı ile ICANN tarafından imzalanan bir mutabakat metni ile alan adları ve IP adreslerinin yönetiminden sorumlu kar amacı gütmeyen bir özel sektör kuruluşu olarak ICANN kurulmuştur[8].

ICANN'ın vizyonu internet sitesinde "*one world, one Internet"* olarak açıklanmıştır.

a. ICANN'ın Yapısı

ICANN'ın hukuksal statüsü 1998 yılında yayımlanan bir yönetmelikle düzenlenmiştir. Günümüze kadar birçok kez değişikliğe uğrayan[9] söz konusu yönetmelik ile ICANN'ın yapısı, organları, çalışma usulleri ve görevleri oldukça ayrıntılı bir şekilde düzenlenmiştir.

Yönetmeliğe göre, ICANN Yönetim Kurulu 16 tane seçilmiş üyeden ve beş tane de atanmış irtibattan oluşur. Sadece seçilmiş üyelerin oyu, aranan oy çoğunluğunda göz önünde bulundurulur. Yönetim Kurulu üyelerinden sekiz üye Aday Belirleme Komitesi (Nominating Committee), iki üye Adres Destek Kuruluşu (Address Supporting Organization), iki üye Ülke Kodu Adları Destek Kuruluşu (Country-Code Names Supporting Organization), iki üye Jenerik Adlar Destek Kuruluşu (Generic Names Supporting Organization), bir üye Temsili Üyelik Danışma Komitesi (At-Large Advisory Committee) tarafından seçilmektedir. İrtibat üyelerinin her biri ise Hükümet Danışma

[7] Işıklı, **a.g.e.**, s. 16.
[8] Memorandum of Understanding Between the U.S. Department of Commerce and Internet Corporation for Assigned Names and Numbers, http://www.icann.org/en/about/agreements/mou-jpa/icann-mou-25nov98-en.htm, 27.01.2013.
[9] Bylaws for Internet Corporation For Assigned Names and Numbers, http://www.icann.org/en/about/governance/bylaws/bylaws-16mar12-en.htm, 27.01.2013.

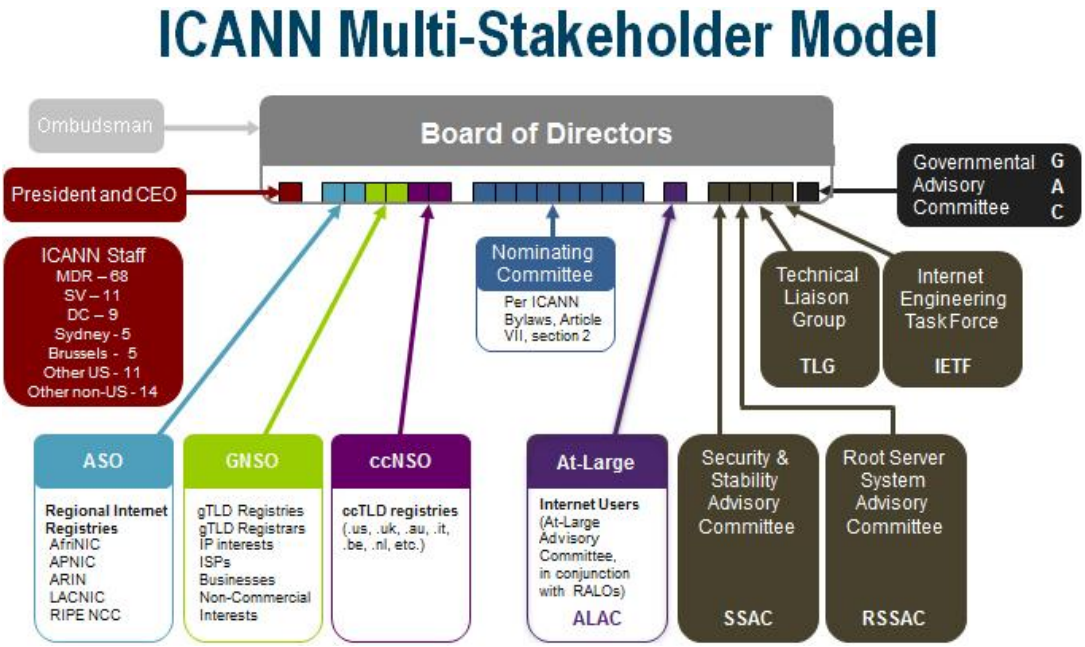
Komitesi (Govermental Advisory Committee), İnternet Mühendislik Görev Gücü (Internet Engineering Task Force), Ana Sunucu Sistemi Danışma Komitesi (Root Server System Advisory Committee), Güvenlik ve Süreklilik Danışma Komitesi (Security & Stability Advisory Committee) ve Teknik İrtibat Grubu (Technical Liaison Group) tarafından belirlenmektedir.

Aday Belirleme Komitesi Yönetim Kuruluna sekiz üyeyi seçmek, Adres Destek Kuruluşu internet adreslerinin fonksiyonunu yerine getirmesi, tahsisi ve yönetimi ile ilgili politika konularında Yönetim Kuruluna önerilerde bulunmak, Ülke Kodu Adları Destek Kuruluşu ülke kodu birinci derece alan adlarını geliştirmek ve Yönetim Kuruluna önerilerde bulunmak, Jenerik Adlar Destek Kuruluşu jenerik birinci derece alan isimlerini geliştirmek ve Yönetim Kuruluna önerilerde bulunmakla görevli ve sorumlu kılınmıştır. Diğer taraftan, Temsili Üyelik Danışma Komitesi bireysel internet kullanıcılarının ilgi alanları açısından öneriler geliştirmek, Hükümet Danışma Komitesi ICANN' ın faaliyetlerinin hükümet konuları ve uluslararası sözleşmeler ile ilgili olduğu noktada öneriler geliştirmek, Güvenlik ve Süreklilik Danışma Komitesi internet alan adları ve IP adresleri sisteminin güvenliği ve bütünlüğü konusunda öneriler geliştirmek, IETF internetin daha iyi çalışması için internet protokol ve standartlarını geliştirmek ve Ana Sunucu Sistemi Danışma Komitesi alan adları ana sunucu sisteminin işleyişine ilişkin öneriler geliştirmek görev ve sorumluluğunu haizdir.

ICANN'ın yapısını oluşturan herbir kuruluş ve komitenin oluşumu Yönetmelikte ayrıntılı bir şekilde ayrıca düzenlenmiştir. Her bir kuruluş ve komitenin oluşumu kendine özgü özellik göstermekte, internet kullanıcıları, internet servis sağlayıcıları, sivil toplum örgütleri, akademisyenler, uzmanlar vs. katılımı ile geniş bir yelpaze oluşturmaktadır.

ICANN'ın yapısı aşağıdaki tabloda ayrıntılı bir şekilde gösterilmiştir[10].

[10] http://www.icann.org/en/groups/chart, 27.01.2013.



b. ICANN'ın İnternet Üzerindeki İşlevi

İnternette bir başka kişiye ulaşabilmek için bilgisayarına ulaşılmak istenen kişinin adresinin yazılması gerekir. İstenilen bilgisayara ulaşılabilmek için bu adres her bilgisayar açısından tek bir adres olarak tasarlanmıştır. Numara veya isimlerden oluşabilir. ICANN tüm dünyada bu tek olan adresler arasındaki koordinasyonu sağlayarak kişilerin internet üzerinden birbirleri ile iletişim kurmalarına imkan sağlayan bir kuruluştur[11]. Bir diğer deyişle, ICANN dünyada en üst düzeyde tek tanımlayıcıların global internet sistemlerini koordine etmek ve bu sistemlerin düzenli ve güvenli bir şekilde çalışmasını sağlamak işlevini yerine getirmektedir. Bu çerçevede ICANN'ın işlevi, alan adları, IP adresleri, özerk sistem adresleri, protokol port ve parameter numaralarının belirlenmesi ile tahsisinde gerekli olan koordinasyonu sağlamaktır. Kuruluş ayrıca, alan adları ana sunucu sisteminin işleyişi ve geliştirilmesinden de sorumludur. Söz konusu sistemlerin daha iyi işleyebilmesi için geliştirilen politikaları da ICANN koordine etmektedir[12].

"İnternet alan adı", internet üzerinde bulunan bilgisayar veya internet sitelerinin adreslerini belirlemek için kullanılan internet protokol numarasını

[11] http://www.icann.org/en/about/welcome, 06.09.2012.
[12] http://www.icann.org/en/about/governance/bylaws, 27.01.2013.

tanımlayan adı; "*internet alan adı sistemi"* ise okunması ve akılda tutulması kolay olan ve genelde aranan adres sahipleri ile ilişkilendirilebilen simgesel isimlerle yapılan adreslemede, karşılığı olan internet protokolü numarasını bulan ve kullanıcıya veren sistemi ifade etmektedir[13]. Bu imkan sayesinde kişiler ulaşmak istedikleri internet sitelerine o sitenin IP numarası yerine alan adını yazarak kolayca ulaşabilmektedir[14]. Örneğin, bir kişi Başbakanlık internet sitesine ulaşmak istediğinde tarayıcıya bu sitenin IP numarasını değil, Başbakanlık internet sitesinin alan adı olan "*www.basbakanlik.gov.tr"* adresini yazarak kolayca ulaşabilmektedir.

İnternet alan adları, birinci (top level domains - TLDs) ve ikinci (second level domains - SLDs) derece alan adlarından oluşmaktadır. www.basbakanlik.gov.tr örneğinde, *gov.tr* birinci derece alan adı, *basbakanlik* ikinci derece alan adıdır. Birinci derece alan adları, ülke kodu içeren (country code top level domains -ccTLDs) ve içermeyen (generic top level domains - gTLDs) alan adları olarak iki alt kategoriye ayrılmaktadır. Jenerik birinci derece alan adları .com, .net, .org .biz gibi uzantılardan; ülke kodu birinci derece alan adları ise .uk, .fr, .nl ve .tr gibi ilgili ülke isimlerinin kısaltmalarından oluşmaktadır. Jenerik birinci derece alan adlarının kişilere tahsisi ICANN tarafından akredite edilmiş kayıt kuruluşlarınca yapılmaktadır[15]. Ülke kodu içeren birinci derece alan adlarının yönetimi ise devletlere bırakılmıştır. Devletler bu yetkiyi doğrudan kendileri kullanabildikleri gibi akademik kurumlar ile kar amacı güden veya gütmeyen özel kuruluşlara da kullandırabilmektedir.

---

[13] "*İnternet alan adı"* ve "*internet alan adı sistemi"* kavramları, 5809 sayılı Elektronik Haberleşme Kanununda tanımlanmıştır. Anılan Kanuna göre, internet alan adı, internet üzerinde bulunan bilgisayar veya internet sitelerinin adresini belirlemek için kullanılan internet protokol numarasını tanımlayan adlar; internet alan adı sistemi ise okunması ve akılda tutulması kolay olan ve genelde aranan adres sahipleri ile ilişkilendirilebilen simgesel isimlerle yapılan adreslemede, karşılığı olan internet protokolü numarasını bulan ve kullanıcıya veren sistemdir (md. 3).

[14] İnternet Alan Adları Yönetmeliğinde IP adresi kavramı, belirli bir ağa bağlı cihazların birbirini tanımak, birbirleriyle iletişim kurmak ve veri alışverişinde bulunmak için kullandıkları İnternet Protokolü standartlarına göre verilen adres olarak tanımlanmıştır (md. 3).

[15] Birinci derece alan adlarının tahsisinde ICANN'ın akredite ettiği bir kuruluş listesi için bkz. http://www.icann.org/registrar-reports/accredited-list.html, 27.01.2013.

Alan adları yönetiminin e-ticaret üzerindeki etkisinden dolayı bu alan özellikle ticaret, marka ve fikri mülkiyet hukukunun ilgi alanına girmekte[16] ve birçok hukuksal uyuşmazlığın ortaya çıkmasına neden olmaktadır[17]. İnternet alan adları yönetimi, özel hukuk uyuşmazlıklarına neden olmakla birlikte kamu hukuku ile ilgili önemli sorunların ortaya çıkmasına da neden olmaktadır. Kamu hukuku açısından her şeyden önce, alan adlarının tahsisi kamusal bir yetkinin kullanılması anlamına gelmektedir ve yetkinin demokratik meşruiyetinin araştırılması önem taşımaktadır. Diğer taraftan, tahsisi yapılan kimi alan adları doğrudan kamu hukuku sorunlarının ortaya çıkmasına neden olmaktadır. Örneğin, devletlerin kullandığı internet adresleri hep ilgili ülkenin isminin kısaltılması ile alınabilirken - ülkemiz açısından örneğin Başbakanlığın web sitesi "*www.basbakanlik.gov.tr"* iken – Amerikan kamu kurumları doğrudan .gov uzantısını kullanmaktadır. Örneğin, Amerikan Başkanlığı, "*www.whitehouse.gov"* uzantılı internet adresi ile internet yayını yapmaktadır. Yine örneğin, bir terör örgütü, örgüt ismini kullanabilecek bir internet alan adı alabilir mi? Kime göre terör örgütü? Bunu hangi hukuk kuralı belirleyecek? Bir başka örnek, Kuzey Kıbrıs Türk Cumhuriyeti Cumhurbaşkanlığı, Başbakanlığı ve diğer kamu kurumlarının web sitelerine ilişkindir. Bu web sitelerinin adresi .gov uzantılı değildir. Cumhurbaşkanlığı internet yayınını, "*http://www.kktcb.org/"* uzantılı internet adresinden, Başbakanlık ise "*http://www.kktcbasbakanlik.org/"* adresinden yapmaktadır. Güney Kıbrıs Rum Yönetiminin web adresi ise .gov uzantılıdır (*http://www.presidency.gov.cy/*). İskoçya'nın ülke kodu içeren birinci derece alan adı talebi reddedilmiş, Filistin'e "*http://www.palestinecabinet.gov.ps/"* adresi verilmiştir[18]. Bütün bunlar aslında alan adları sistemi yönetiminin

---

[16] Işıklı, **a.g.e.**, s. 43 vd.

[17] Örneğin, "*ilk gelen ilk alır"* kuralı gereği ünlü marka ve kişilerin adlarını erken davranarak kendi adlarına kayıt ettiren kişiler, sonrasında bu adları yüksek meblağlar karşılığında marka sahiplerine veya ünlü kişilere satmaya çalışmaktadır (cybersquatting). Bkz. Tamer Soysal, "İnternet Alan Adları Sistemi ve Tahkim Kuruluşlarının UDRP Kurallarına Göre Verdikleri Kararlara Eleştirel Bir Yaklaşım – 1", **Erciyes Üniversitesi Sosyal Bilimler Enstitüsü Dergisi**, Sayı: 21, 2006, s. 483.

[18] Jochen von Bernstorff, "Democratic Global Internet Regulation? Governance Networks, International Law and the Shadow of Hegemony", **European Law Journal**, Vol. 9, No. 4, September 2003, s. 514.

uluslararası kamu hukuku açısından da ne kadar önemli olduğunu göstermektedir.

Diğer taraftan, alan adlarının sadece Latin karakterlerden oluşması beraberinde birçok sorunu da getirmektedir. Türkçe alfabe açısından ç, ğ, j, ö, ş ve ü harfleri internet alan adlarının belirlenmesinde kullanılamamaktadır. Aynı durum, örneğin Arap ve Çin alfabesi açısından da geçerlidir. Bu durum devletler açısından ciddi bir ekonomik rekabet, bu ülke vatandaşları açısından da iletişim sorunu ortaya çıkarmaktadır[19].

ICANN'ın, internet içeriği üzerinde düzenleyici bir otorite konumunda olmadığını da bu noktada belirtmemiz gerekir. Ancak, alan adlarının yönetimi ile internet içeriği etkilenmektedir.

İnternet protokol numaralarının tahsisi ve istikrarı ise IANA tarafından yapılmaktadır. IANA, ICANN'ın bir bölümüdür. İnternetin merkezi bir yönetimi bulunmamasına rağmen işlevini yerine getirebilmesi için bazı teknik konularda da koordinasyon ihtiyacı bulunmaktadır ve bu ihtiyaç IANA tarafından yerine getirilmektedir. IP adresleri kullanıcılara, internet servis sağlayıcıları tarafından tahsis edilmektedir. İnternet servis sağlayıcıları ise IP adreslerinin tahsisini, yerel internet kayıt kuruluşları, ulusal kayıt kuruluşları ve bölgesel kayıt kuruluşlarından yapabilmektedir. Bölgesel kayıt kuruluşlarına IP adreslerinin tahsisi blok halinde IANA tarafından yapılmaktadır[20].

IP adresleri internet servis sağlayıcılara AfriNIC, APNIC, ARIN, LACNIC, RIPE NCC bölgesel internet kayıt kuruluşları tarafından tahsis edilmektedir. Türkiye, coğrafi olarak RIPE NCC bölgesinde yer almakta ve Türkiye'ye IP adreslerinin tahsisi bu kuruluş tarafından yapılmaktadır.

c. Demokratik Meşruiyet Sorunu

İnternet alan adlarının yönetimi konusunda uluslararası bir sözleşme bulunmamaktadır. ICANN, faaliyetlerini ABD ile IANA arasında yapılmış

[19] Mustafa Alkan, Cafer Canbay, "İnternet Alan Adları Yönetimi, Mevcut Sorunlar ve Çözüm Önerileri",http://www.tk.gov.tr/kutuphane_ve_veribankasi/raporlar/arastirma_raporlari/dosyalar/WEB_DE_YAYINLANAN_RAPOR.pdf, 06.09.2012, s. 1-24.
[20] Işıklı, **a.g.e.**, s. 57.

sözleşmeye göre yürütmektedir. Bu sözleşmenin hukuksal dayanağı ise ABD California hukukundan kaynaklanmaktadır. ICANN'ın Amerikan yönetimi, hukuku ve yargı yetkisi çerçevesinde faaliyet gösteren özel bir Amerikan kuruluşu olduğu ifade edilmektedir[21]. Bu durum, ICANN'ın demokratik meşruiyet sorununu gündeme getirmektedir. Bir görüş, ICANN'ın oluşumunda demokratik bir meşruiyet sorununun bulunmadığını savunmaktadır. Bu görüş, ICANN'ın klasik uluslararası kuruluşların devletler dışındaki diğer sivil toplum kesimlerini dışlayan anti-demokratik ve hantal yapısı yerine "*network governance"* modeli ile yönetildiğini ve bu modelin hem toplumun her kesiminin yönetime katılımını sağladığından daha demokratik hem de daha verimli bir model olduğunu ileri sürmektedir. Bu çerçevede ICANN'ın aşağıdan yukarı, consensusa dayalı ve çok paydaşlı yönetim modeli ile yönetildiği belirtilmektedir.

Diğer bir görüş ise ICANN'ın oluşumunda demokratik bir meşruiyet sorununun bulunduğunu savunmaktadır. Bu görüşe göre, ICANN'ın network governance modeli ile oluşturulduğu ve faaliyetlerini yürüttüğü iddiasının geçerliliği ve doğruluğu bir tarafa internet gibi bugün tüm insanlığı ve devletleri ilgilendiren ve etkileyen bir alanda devletlerin eşit katılımını öngören bir yapı *(one-state one-vote principle)* dışındaki her oluşum demokratik meşruiyetten uzak olmaya mahkum olacaktır[22]. Ayrıca, devletlerin eşit katılımı ve oy hakkını sağlayamamış ve uluslararası hukuki çerçeve içine oturtulamamış bir uluslararası yapının her şekilde alanındaki güçlü aktörlerin hegemonyasına girmesi kaçınılmaz bir olgudur[23]. Doktrinde, ICANN'ın bünyesinde barındırdığı demokratik meşruiyet sorununun ortadan kaldırılması için bu yapının lağvedilip, sahip olduğu görevlerin Uluslararası Telekomünikasyon Birliği'ne (International Telecommunication Union-ITU) devredilmesi gerektiği hararetle savunulmaktadır[24].

---

[21] Antonio Segura-Serrano, "Internet Regulation and the Role of International Law", **Max Planck Yearbook of United Nations Law**, Volume 10, 2006, s. 232.
[22] Alkan / Canbay, **a.g.m.**, s. 1-24.
[23] Bernstorff, **a.g.m.**, s. 513.
[24] Alkan / Canbay, **a.g.m.**, s. 1-24.

ICANN'ın network governance modeli ile yönetildiği ve ilgili her aktörün temsilini sağlayacak şekilde demokratik bir meşruiyete sahip olduğu iddiası da gerçeği yansıtmamaktadır. IANA, IETF ve ABD Ticaret Departmanından gelen bir grup mühendis ve bunların temsil ettiği güçler bu yapı içerisinde önemli noktalardaki egemenliklerini sürdürmektedir[25]. İnformal, uluslararası hukuk dışı ve esnek bir yapının oluşturulması, bu alandaki güçlü aktörlerin sistem içerisindeki hegemonyalarını sürdürebilmelerinin bir formülü olarak değerlendirilmektedir[26].

ICANN'ın California hukuku ve yargı yetkisi altında faaliyet göstermesi eleştirilen bir diğer noktadır[27]. ICANN hakkında bir California yargı merciinin veya ABD yasama organının karar alması bu kuruluşu bağlayacaktır[28]. O halde hangi demokratik meşruiyetten bahsedilebilir? İnternet ile ilgili ortaya çıkan hukuksal uyuşmazlıklarda çözüm devletten beklenirken ve devlet, bu sorunların çözümüne yönelik düzenleme yaptığında her seferinde hedef alınırken, internet alan adları ve IP adreslerinin yönetiminde söz hakkına sahip olamamaktadır[29].

ICANN'ın sahip olduğu yetkilerin ITU'ye devredilmesi bu kuruluşun demokratik meşruiyetine ilişkin tartışmaları ortadan kaldıracaktır.

2. İnternet Alan Adlarının Tahsisinde Ulusal Yetki

Ülke kodu birinci derece alan adlarının yönetimi, ilgili ülke yetkili makamlarınca yapılmaktadır. Bu yetki, hükümet kuruluşlarınca kullanılabildiği gibi üniversiteler veya özel sektör kuruluşlarınca da kullanılabilmektedir. Ülkemizde .tr uzantılı alan adlarının yönetimi bu yetkinin Elektronik Haberleşme Kanunu ile Ulaştırma, Denizcilik ve Haberleşme Bakanlığına verildiği 2010 yılına kadar Orta Doğu Teknik Üniversitesi tarafından bu üniversite bünyesinde bulunan "*Nic.tr"* sistemi üzerinden yapılmıştı. Elektronik Haberleşme Kanunu ile internet alan adlarının tahsisini yapacak

[25] Bernstorff, **a.g.m.**, s. 517.
[26] Bernstorff, **a.g.m.**, s. 523.
[27] Franz C. Mayer, "Europe and The Internet: The Old World and The New Medium", **EJIL**, Vol. 11, No. 1, 2000, s. 166.
[28] Alkan / Canbay, **a.g.m.**, s. 1-24.
[29] Alkan / Canbay, **a.g.m.**, s. 1-24.

kurum veya kuruluşun tespiti ile alan adı yönetimine ilişkin usul ve esasların Ulaştırma, Denizcilik ve Haberleşme Bakanlığınca belirleneceği öngörülmüştür (md. 35). Bu çerçevede, anılan Bakanlıkça internet Alan Adları Yönetmeliği[30] yürürlüğe konulmuştur. Bu Yönetmelik .tr uzantılı internet alan adları yönetimine ilişkin usul ve esasları düzenlemek amacıyla yürürlüğe konulmuştur. Yönetmelik ile .tr uzantılı internet 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 gerçekleştirilmesini sağlayan bir sistem oluşturulması öngörülmüştür (*.tr ağ bilgi sistemi - TRABİS*). Yönetmelik ile BTK'ya birçok görev verilmiştir. Yönetmeliğe göre BTK'nın görevleri şunlardır:

1. TRABİS'i kurmak ve işletmek veya belirlediği usul ve esaslar çerçevesinde TRABİS'in üçüncü bir tarafça kurulması ve işletilmesini sağlamak,

2. Uyuşmazlık çözüm hizmet sağlayıcıları ve kayıt kuruluşlarını belirlemek ve bunların iletişim bilgilerini internet sitesinde yayımlamak,

3. Alan adı tahsis ve yenilemesine ilişkin ücretler ile uyuşmazlık çözüm mekanizmasının işletilmesi ile ilgili işlemlere ilişkin ücretleri belirlemek ve gerektiğinde değişiklik yapmak,

4. Tahsise açılacak veya kullanımına son verilecek alt alan adlarını belirlemek,

5. Belgeli tahsis edilen alt alanların tahsisinde istenecek belgeleri belirlemek,

6. Bu Yönetmelikte belirtilen veya Kurul tarafından belirlenen hallerle sınırlı olmak kaydıyla kayıt kuruluşu niteliğinde faaliyet yürütmek,

7. Alan adı ihtilaflarına ilişkin kendisine iletilen mahkeme kararlarını, uyuşmazlık çözüm hizmet sağlayıcının kendisine ilettiği ihtilafa konu olan

[30] RG. 07.11.2010, 27752.

alan adları ile hakem veya hakem heyeti kararlarını internet sitesinde güncel olarak bulundurmak ve bu kararların gereğini yerine getirmek,

8. Kendisine iletilen talep ve şikayetleri değerlendirmek ve mevzuat çerçevesinde gerekli tedbirleri almak,

9. Her yıl Nisan ayı sonuna kadar bir önceki yıla ait faaliyet raporunu hazırlayarak Kurumun internet sitesinden ve gerekli olduğu hallerde diğer uygun araçlarla kamuoyuna duyurmak,

10. ICANN, RIPE NCC, CENTR gibi kuruluşlar nezdinde gerekli çalışmaları yürütmek.

C. Bilgi Toplumu İnşasında İnternet

Bilgi toplumu, sanayi toplumunun bir sonraki aşaması olarak yeni bir toplumu ifade etmektedir. Bu yeni toplumun temelini bilgi oluşturmaktadır. Bilgiyi üreten, iyi kullanan ve yöneten, kısacası bilgi üzerinde hakimiyet sahibi olan üretimde de söz sahibi olmaktadır. Gelişmiş ülkeler, genel olarak her alanda, özel olarak ise ekonomik alanda sahip oldukları üstünlüğü devam ettirebilmenin yolu olarak bilgi toplumunun sunduğu imkanları sonuna kadar kullanmakta; gelişmekte olan ülkeler ise bu imkanları gelişmiş ülkelerin seviyesini yakalayabilmenin bir fırsatı olarak değerlendirmekte ve bu alana ciddi yatırım yapmakta ve teşvikte bulunmaktadır.

Türkiye, sanayi devrimindeki gecikmeyi bilgi çağında tekrar yaşamamak için bu çağın gereklerinin yerine getirilmesinde güçlü bir siyasi ve bürokratik irade göstermektedir. 1998 yılından günümüze, uygulamaya konulan KAMU-NET Projesi, e-Dönüşüm Türkiye Projesi ve Bilgi Toplumu Stratejisi ve eki Eylem Planı ülkemizin bilgi toplumuna dönüşümünde önemli köşe taşları olmuştur. 2005 yılında Yüksek Planlama Kurulu kararıyla yürürlüğe konulan ve 2006-2010 yıllarını kapsayan Bilgi Toplumu Stratejisi[31], bilgi toplumuna dönüşüm yolunda 7 stratejik öncelik belirlemiştir. Sosyal dönüşüm, bilgi ve iletişim teknolojilerinin iş dünyasına nüfuzu, vatandaş

[31] 11.7.2006 tarihli ve 2006/38 sayılı Yüksek Planlama Kurulu Kararıyla onaylanan Bilgi Toplum Stratejisi ve eki Eylem Planı, 28.7.2006 tarihli ve 26242 sayılı Resmi Gazete'de yayımlanarak yürürlüğe girmiştir.

odaklı hizmet dönüşümü, kamu yönetiminde modernizasyon, küresel rekabetçi bilgi teknolojileri sektörü, rekabetçi, yaygın ve ucuz iletişim altyapı ve hizmetleri, ar-ge ve yenilikçiliğin geliştirilmesi, söz konusu 7 önceliği oluşturmaktadır. Eylem Planında ise öngörülen bu önceliklerin, 2006-2010 yılları arasında gerçekleştirilmesi için 111 tane eylem öngörülmüştür. Bilgi Toplumu Stratejisi Eylem Planı Gerçekleşme Durumu bir rapor ile kamuoyuna açıklanmış[32] ve 2012 yılında Kalkınma Bakanlığı bünyesinde yeni bir bilgi toplumu stratejisi çalışması başlatılmıştır[33].

Diğer taraftan, kamu hizmeti niteliğini haiz, ancak işletmeciler tarafından karşılanmasında mali güçlük bulunan evrensel hizmetin sağlanması, yürütülmesi ve elektronik haberleşme sektörü ile bu Kanun kapsamında belirlenen diğer alanlarda evrensel hizmet yükümlülüğünün yerine getirilmesine ilişkin usul ve esasları belirlemek amacıyla 5369 sayılı Evrensel Hizmet Kanunu yürürlüğe konulmuştur. Kanunda evrensel hizmet, *"Türkiye Cumhuriyeti sınırları içinde coğrafi konumlarından bağımsız olarak herkes tarafından erişilebilir, önceden belirlenmiş kalitede ve herkesin karşılayabileceği makul bir bedel karşılığında asgari standartlarda sunulacak olan, internet erişimi de dahil elektronik haberleşme hizmetleri ile bu Kanun kapsamında belirlenecek olan diğer hizmetler"* olarak tanımlanmıştır. Kanun ile evrensel hizmetin gelirleri de belirlenmiştir. Bu gelirler, Ulaştırma, Denizcilik ve Haberleşme Bakanlığının bütçesine "evrensel hizmet gelirleri" olarak kaydedilmektedir.

Ülkemizde 2011 yılı itibariyle toplam 14.1 milyon internet abone sayısı bulunmaktadır. 2009 yılında 3G hizmetlerinin uygulamaya konulmasıyla birlikte bu tarihten itibaren mobil internet abone sayısında ciddi bir artış olmuş ve 2011 yılı itibariyle mobil internet abone sayısı 6.4 milyona ulaşmıştır. Aynı yıl itibariyle ADSL kullanıcı sayısı 6.7 milyon, kablo internet kullanıcı sayısı

---

[32] Devlet Planlama Teşkilatı, **Bilgi Toplumu Stratejisi Eylem Planı (2006-2010) Değerlendirme Raporu Rapor No: 5**, http://www.bilgitoplumustratejisi.org/tr/doc/8a3247663bd29634013bdda974630002, 28.01.2012.

[33] http://www.bilgitoplumustratejisi.org/tr/node/hakkimizda, 28.01.2013.

460 bin olarak gerçekleşmiştir. 2011 yılında internet abone sayısındaki artış % 39 oranındadır[34].

İnternetin bilgi toplumuna dönüşüm açısından ortaya çıkardığı etkinin daha iyi alaşılabilmesi için internet ile ilgili bazı istatistiki bilgilere bakmak faydalı olacaktır.

Haziran 2012 tarihi itibariyle dünyada 2.405.518.378 internet kullanıcısı bulunmaktadır. İnternet kullanıcılarının nüfusa göre dünyadaki dağılımı sırasıyla şu şekilde gerçekleşmiştir[35]:

Tablo 1. İnternet kullanıcılarının nüfusa göre dünyadaki dağılımı

Sır	Ülke	%
a1	Asya	44.8
2	Avrupa	21.5
3	Kuzey Amerika	11.4
4	Latin Amerika	10.4
5	Afrika	7.0
6	Ortadoğu	3.7
7	Avustralya	1.0

Söz konusu verilere göre 2010-2012 yılları arasında dünyada internet kullanımı % 566.4 oranında artmıştır.

Haziran 2012 tarihi itibariyle en fazla internet kullanıcısının bulunduğu 20 ülke şu şekilde gerçekleşmiştir[36].

[34] Bu istatistiki veriler için bkz. Bilgi Teknolojileri ve İletişim Kurumu, **Faaliyet Raporu 2011**, http://www.tk.gov.tr/kutuphane_ve_veribankasi/raporlar/faaliyet_raporlari/index.php, 05.10.2012, s. 28.
[35] http://www.internetworldstats.com/stats.htm, 28.12.2012.
[36] http://www.internetworldstats.com/top20.htm, 28.12.2012.

Tablo 2. En fazla internet kullanıcısının bulunduğu 20 ülke

Sıra	Ülke	Kullanıcı Sayısı
1	Çin	538,000,000
2	ABD	245,203,319
3	Hindistan	137,000,000
4	Japonya	101,228,736
5	Brezilya	88,494,756
6	Rusya	67,982,547
7	Almanya	67,483,860
8	Endenozya	55,000,000
9	İngiltere	52,731,209
10	Fransa	52,228,905
11	Nijerya	48,366,179
12	Meksika	42,000,000
13	İran	42,000,000
14	Kore	40,329,660
15	**Türkiye**	**36,455,000**
16	İtalya	35,800,000
17	Filipinler	33,600,000
18	İspanya	31,606,233
19	Vietnam	31,034,900
20	Mısır	29,809,724

Dünya sıralamasında Türkiye, 36.455.000 internet kullanıcı sayısı ile 15. sırada yer almaktadır.

Dünyanın değişik bölgelerindeki nüfusa göre internet kullanım oranı ise sırasıyla şu şekildedir[37]:

Tablo 3. Dünyanın değişik bölgelerindeki nüfusa göre internet kullanım oranı

Sıra	Ülke	%
1	Kuzey Amerika	78.6
2	Avustralya	67.6
3	Avrupa	63.2
4	Latin Amerika	42.9
5	Ortadoğu	40.2
6	Asya	27.5
7	Afrika	15.6
	Dünya ortalaması	34.3

Aralık 2011 tarihi itibariyle nüfusa göre dünyada internet kullanım oranının en yüksek olduğu ilk 20 ülke ise şu şekilde gerçekleşmiştir[38].

[37] http://www.internetworldstats.com/stats.htm, 28.12.2012.
[38] http://www.internetworldstats.com/top25.htm, 28.12.2012.

Tablo 4. Nüfusa göre dünyada internet kullanım oranının en yüksek olduğu ilk 20 ülke

Sıra	Ülke	%
1	İzlanda	97.8
2	Norveç	97.2
3	İsveç	92.9
4	Falkland Islands	92.4
5	Luxembourg	91.4
6	Grönland	90.2
7	Avusturalya	89.8
8	Hollanda	89.5
9	Danimarka	89.0
10	Finlandiya	88.6
11	Saint Lucia	88.5
12	Yeni Zelenda	84.5
13	İsviçre	84.2
14	İngiltere	84.1
15	Niue	83.9
16	Almanya	82.7
17	Güney Kore	82.7
18	Liechtenstein	81.8
19	Kanada	81.6
20	Belçika	81.4

Bu listeye göre dünya sıralamasında Türkiye ilk 50 ülke içerisinde yer almamaktadır. Türkiye'de internet kullanıcı sayısı nüfusun % 45.7'sini oluşturmaktadır.

Mayıs 2011 tarihi itibariyle internette en fazla kullanılan ilk 10 dil şu şekilde gerçekleşmiştir[39]:

Tablo 5. İnternette en fazla kullanılan ilk 10 dil

Sıra	Dil	%
1	İngilizce	26.8
2	Çince	24.2
3	İspanyolca	7.8
4	Japonca	4.7
5	Portekizce	3.9
6	Almanca	3.6
7	Arapça	3.3
8	Fransızca	3.0
9	Rusça	3.0
10	Korece	2.0
	Diğer diller	17.8

[39] http://www.internetworldstats.com/stats7.htm, 28.12.2012.

Ç. İnternetin Hukuksal Açıdan Önem Taşıyan Fonksiyonları

İnternet kişiler, şirketler, örgütler veya devletler tarafından birçok amaç için kullanılabilir. Bu amaç, yararlı - zararlı, hukuksal - hukuk dışı veya meşru – gayrı meşru bir amaç olabilir. Bu ayrımlara burada hiç girilmeyecektir. Fakat, söz konusu amaçların gerçekleştirilebilmesi için internetin bazı fonksiyonlarının kullanılması gerekir. Bu fonksiyonlar belki sayısızdır ancak hukuksal açıdan önem taşıyan bazı fonksiyonların neler olduğunun belirlenmesi önem taşımaktadır. İnternetin hukuksal açıdan önem taşıyan fonksiyonları ortaya konulmadan bu alanda ortaya çıkan hukuksal sorunlara çözüm üretilmeye çalışılması faydasız olabilir.

1. e-Demokrasi

İnternet ile ilgili konular ele alındığında üzerinde en fazla durulan konulardan birisi de demokrasi konusudur (*internet demokrasisi*). Hatta günümüzde çoğu zaman demokrasi ve ifade özgürlüğü belli bir noktada internet ile açıklanmakta; internet, demokrasinin olmazsa olmazlarından birisi olarak görülmektedir. İnterneti demokrasinin vazgeçilmez bir aracı olarak gören bu görüşe göre, internet toplumların demokratikleşmesi açısından önemli etkiler ortaya çıkarabilmektedir[40]. İnternet ile insanların bilgiye erişim, düşüncelerini açıklama ve yayma özgürlük alanı oldukça genişlemiştir. Devletin internete müdahalesindeki sınırlı etki nedeniyle bu özgürlük, internette, diğer kitle iletişim araçlarından farklı olarak oldukça geniş bir şekilde kullanılabilmektedir. İnternet, "*temsili demokrasinin"* ortaya çıkardığı sorunları "*katılımcı demokratik araçlar"* sunarak aşmaktadır[41].

İnternetin demokrasiyi geliştireceğine yönelik bu görüşleri gerçekçi bulmayan bir görüş ise internetin "*gerçek demokrasiyi"* gerçekleştirmesinin imkansız olduğunu ileri sürmektedir. Bu görüşe göre ilk olarak internet, katılımcı bir demokrasi oluşturmaktan çok uzaktır. İnternete erişim açısından var olan "*dijital bölünme"*, demokrasinin gelişmesi açısından önemli bir

---

[40] Ronald Deibert, Rafal Rohozinski, "Liberation vs. Control: The Future of Cyberspace", **Journal of Democracy**, Volume 21, Number 4, 2010, s. 46.

[41] Özgür Uçkan, **e-Devlet, e-Demokrasi ve Türkiye**, Literatür Yayınları: 95, 1. Basım, İstanbul, Nisan 2003, s. 26-27.

sorundur[42]. Yeterli eğitim düzeyine veya yeterli maddi kaynaklara sahip olmayan insanların internet kullanamaması da katılımcılığı engellemektedir. İnternette enformasyon, belli grupların elindedir ve yine belli gruplara akmakta ve onlar tarafından kullanılmaktadır. İkinci olarak, teknolojiyi elinde bulunduran güçler, düşünceyi, siyaseti ve toplumsal yaşamı da kontrol etmektedir. İnternet, gücü elinde bulunduranların çıkarlarına hizmet etmekte, onların gözetim imkanlarını artırmakta ve toplumun daha sıkı bir şekilde denetimine neden olmaktadır[43].

Ayrıca "*sanal toplulukların" (online communities)*; terör, pornografi, ırkçılık ve şiddet gibi suç eğilimleri gösterme potansiyeli, ötekileştirme, grup kutuplaşması ve genellikle diyolağa kapalı yapılar oluşturması ve bunların sonucu olarak bu toplulukların devlet tarafından gözetimi, internetin çok sesli ve çoğulcu bir yapıdan ziyade tek tipleştirici, içe dönük ve dışlayıcı bir yapı olarak karşımıza çıkmasına neden olmaktadır. Bu durumda ise demokrasinin farklılıklara saygı unsuru anlamını yitirmektedir[44].

Nihayet, devletin internete pozitif veya negatif anlamda müdahalesi, internetin kişilere sunduğu demokratik katılım imkanlarını şekillendirmekte ve bu müdahale demokratik bir gelişime yönelebileceği gibi anti-demokratik bir gelişime de yönelebilmektedir. Toplumların siyasi, sosyal, kültürel ve inanç değerleri internette de yansımasını bulmakta ve bu değerler internetin gelişimini de kendi yönünde belirlemektedir[45]. Söz konusu değerlerin demokratik bir gelişmişlik düzeyini ortaya koyamaması durumunda bunun internete yansıması da aynı olmakta ve bu tür toplumlarda demokratik bir internet gelişiminden söz edilememektedir[46]. Bu görüşün ortaya koyduğu internet-demokrasi ilişkisi kısaca şu şekilde özetlenebilir: *"Enformasyon teknolojilerinin olumsuz yönleri göz ardı edilerek 'demokrasi havarisi' gibi*

---

[42] Uçkan, **a.g.e.**, s. 37.
[43] Uğur Dolgun, "İnternet ve Demokrasi", http://www.journals.istanbul.edu.tr/tr/index.php/iktisatsosyoloji/article/viewFile/11379/10639, 27.01.2013, s. 228.
[44] Dolgun, **a.g.m.**, s. 226-227.
[45] Akdeniz / Altıparmak, **a.g.e.**, s. 2.
[46] Dolgun, **a.g.m.**, s. 228.

lanse edilmeleri, ya çok iyimser bakış açısını ya da 'bazı niyetleri örtme' çabasını ifade eder"[47].

İnternet-demokrasi ilişkisine yönelik birbiri ile çatışan bu iki farklı görüşün her ikisinin de doğru olan tarafları bulunmaktadır. İnternet, elbette toplumlara geniş bir özgürlük alanı açmış ve demokrasinin gelişmesine ivme kazandırmıştır. Ancak, bununla birlikte internetin belli güçler, gruplar ve kimi devletler tarafından yönlendirildiği, enformasyonun bu güçlere aktığı ve bunlar tarafından kullanıldığı, toplumların bu güçler tarafından gözetildiği ve kontrol edildiği de yadsınamaz[48].

İnternetin demokrasi ile ilişkisine ilişkin bu genel açıklamalardan sonra doğrudan e-demokrasi kavramı üzerinde yoğunlaşmak faydalı olacaktır. İnternet, genel olarak demokratik gelişime katkısı yanında günümüzde elektronik katılım imkanlarını sunması yönüyle e-demokrasinin gerçekleştirilmesi fonksiyonunu da yüklenmektedir. e-Demokrasi, elektronik araçların kullanılarak devlet yönetiminin etkilenmesi, kamusal kararların alınmasına vatandaşların katılımının sağlanması, elektronik katılım araçları ile yönetimden hesap sorulabilmesi, devlet yönetiminde elektronik araçların kullanılarak vatandaşların yönetime katılmasının ve şeffaflığın sağlanması olarak tanımlanabilir[49]. Hak ve özgürlüklerin gerçekleştirilmesi için kamu kurumlarına yapılacak başvuruların elektronik ortamda da yapılabilmesi, siyasetçi ve bürokratlara alacakları kararlar üzerinde etki doğurmak amacıyla toplu e-postalar gönderilmesi, elektronik oylamalar (e-voting), sanal kampanya ve forumlar, elektronik müzakereler, vatandaşların ve sivil toplum kuruluşlarının da katılımının sağlandığı sanal toplantılar, kamusal bilgilerin internet ortamında kullanıma sunulması ve kişilerin kendileri hakkında devlet tarafından tutulan kayıtlara internet ortamından kişisel veriler korunarak ulaşabilmesi gibi imkanlar elektronik katılım araçları olarak kullanılabilir[50]. Örneğin, 4982 sayılı Bilgi Edinme Hakkı Kanununun 6. maddesine göre bilgi

[47] Dolgun, **a.g.m.**, s. 230.
[48] Uçkan, **a.g.e.**, s. 35-36.
[49] Ali Şahin, Handan Temizel, Metehan Temizel, "Türkiye'de Demokrasiden e-Demokrasiye Geçiş Süreci ve Karşılaşılan Sorunlar", www.siyasaliletişim.org/pdf/edemokrasiyegecis.pdf, 08.01.2013, s. 254.
[50] Uçkan, **a.g.e.**, s. 39-40.

edinme başvurusu ve 6328 sayılı Kamu Denetçiliği Kurumu Kanununun 17. maddesine göre idarenin eylem, işlem, tutum ve davranışlarına karşı yapılacak şikayetler elektronik ortamda da yapılabilir. Yine örneğin, vatandaşlar ve avukatların dava ve takiplerini cep telefonları üzerinden anında takip edebilmeleri için Adalet Bakanlığınca UYAP sms bilgi sistemi oluşturulmuştur[51]. e-Devlet Kapısı üzerinden farklı kamu kurum ve kuruluşlarına ait birçok elektronik hizmet tek bir elden sunulmaktadır[52].

Ülkemizde kanun ve düzenleyici işlemlerin hazırlanması sürecinde internet ortamında vatandaşların görüşlerinin alınmasına yönelik bir uygulama bulunmamaktadır. Başbakanlığın ve bakanlıkların internet sitelerinde açılacak forumlar ile kanun ve düzenleyici işlemlerin hazırlanması sürecinde vatandaşların görüşleri alınabilir. Böyle bir uygulamanın getirilmesi e-demokrasinin gerçekleştirilmesi açısından önemli bir aşama olacaktır.

Bazı kamu kurumlarının, okulların, özellikle küçük çaptaki yerel yönetimlerin internet siteleri oldukça yetersizdir. Çoğu internet sitesi kurumun bilgi verme işlevini dahi tam olarak yerine getirememektedir.

2. e-Devlet

Elektronik devlet (e-devlet), bilgi ve iletişim teknolojilerinin kamu hizmetlerinin sunumunda kullanılarak kamu hizmetlerinin daha etkin, verimli, şeffaf, hesap verebilir, kesintisiz, hızlı, basit, vatandaşa daha yakın ve bütünleşik bir şekilde sunulabilmesini amaçlayan kamu yönetimi anlayışı olarak tanımlanabilir[53]. E-devlet uygulamaları sadece fiziksel ortamda sunulan kamu hizmetlerinin elektronik ortama taşınması olarak karşımıza çıkmamakta; bunun yanında aynı zamanda kamusal ve hukuksal bir dönüşümü de beraberinde getirmektedir. E-devlet uygulamaları ile birlikte kamusal örgütlenme biçiminde ve idari usullerde değişiklikler ortaya

---

[51] http://www.sms.uyap.gov.tr/, 28.01.2013.
[52] https://www.turkiye.gov.tr/hizmetler, 28.01.2013.
[53] Demokaan Demirel, "e-Devlet ve Dünya Örnekleri", **Sayıştay Dergisi**, Sayı: 61, Nisan-Haziran 2006, s. 84. N. Murat İnce, **Elektronik Devlet Kamu Hizmetlerinin Sunulmasında Yeni İmkanlar**, Devlet Planlama Teşkilatı Yayınları, Ankara, Mayıs 2001, s. 21.

çıkmakta, siyasal katılımcılık etkinleşmekte, insan kaynakları yönetimi biçim değiştirmekte ve yeni hukuksal düzenlemelere ihtiyaç duyulmaktadır[54].

Gerek e-devlet uygulamalarının hayata geçirilebilmesi, gerekse ortaya çıkabilecek hukuksal sorunların ortadan kaldırılması amacıyla devletler, e-devletin hukuksal altyapısı konusunda hukuksal düzenlemeler yapmaktadır[55]. Bazı devletler diğer hukuksal düzenlemeler yanında doğrudan bu alanı düzenleyen kanunlar da yürürlüğe koyarken, bazı devletler müstakil bir kanun yerine, gerektiği durumlarda çeşitli kanunlarda değişiklikler veya e-devletin özel alanlarına yönelik spesifik düzenlemeler yaparak hukuksal değişimi sağlamaya çalışmaktadır. ABD, İtalya, Fransa, Avusturya ve İspanya gibi devletler e-devlete ilişkin diğer düzenlemeler yanında müstakil bir e-devlet kanunu yürürlüğe koyan devletlerdir. ABD'de e-Government Act of 2002[56], Avusturya'da e-Government Act 2004[57], İtalya'da e-Government Code 2006[58], Fransa'da Ordinance on Electronic Interactions Between Public Services Users and Public Authorities and Among Public Authorities[59], İspanya'da ise Law on Citizen's Electronic Access to Public Services 2007[60] yürürlüğe konulmuştur. Ülkemizde ise müstakil bir e-devlet kanunu bulunmamaktadır. Ancak, e-devlet uygulamalarının hukuksal altyapısını sağlamak amacıyla birçok kanunda değişiklik yapılmıştır. Örneğin UYAP, Hukuk Muhakemeleri Kanununda[61]; MERNİS, Nüfus Hizmetleri

---

[54] Demirel, **a.g.m.**, s. 99.
[55] İnce, **a.g.e.**, s. 41.
[56] Metin için bkz. http://www.cio.noaa.gov/itmanagement/egovact.pdf, 19.12.2012.
[57] Metin için bkz. http://www.epractice.eu/files/media/media_928.pdf, 19.12.2012.
[58] Bkz. http://www.epractice.eu/en/document/288279, 19.12.2012.
[59] Bkz. http://www.epractice.eu/files/eGovernmentFrance.pdf, 19.12.2012.
[60] Bkz. http://www.epractice.eu/files/eGovernmentSpain.pdf, 19.12.2012.
[61] İlgili hüküm şu şekildedir:
*"**Elektronik işlemler***
***MADDE 445-** (1) Ulusal Yargı Ağı Bilişim Sistemi (UYAP), adalet hizmetlerinin elektronik ortamda yürütülmesi amacıyla oluşturulan bilişim sistemidir. Dava ve diğer yargılama işlemlerinin elektronik ortamda gerçekleştirildiği hâllerde UYAP kullanılarak veriler kaydedilir ve saklanır.*
(2) Elektronik ortamda, güvenli elektronik imza kullanılarak dava açılabilir, harç ve avans ödenebilir, dava dosyaları incelenebilir. Bu Kanun kapsamında fizikî olarak hazırlanması öngörülen tutanak ve belgeler güvenli elektronik imzayla elektronik ortamda hazırlanabilir ve gönderilebilir. Güvenli elektronik imza ile oluşturulan tutanak ve belgeler ayrıca fizikî olarak gönderilmez, belge örneği aranmaz.
(3) Elektronik ortamdan fizikî örnek çıkartılması gereken hâllerde tutanak veya belgenin aslının aynı olduğu belirtilerek hâkim veya görevlendirdiği yazı işleri müdürü tarafından imzalanır ve mühürlenir.

Kanununda[62]; e-ihale projesi, Kamu İhale Kanununda[63]; elektronik tebligat, Tebligat Kanununda[64] yeni düzenlemeler gerektirmiştir. 29.06.2009 tarihli ve 2009/15169 sayılı Bakanlar Kurulu Kararıyla yayımlanan Kamu Hizmetlerinin Sunumunda Uyulacak Usul ve Esaslara İlişkin Yönetmelikte (md. 4), basılı ortamdaki bilgi ve belgelerin elektronik ortama taşınması ve veritabanlarının diğer idarelerle paylaşılmasının esas olduğu; idarece, başvuruların elektronik

---

(4) Elektronik ortamda yapılan işlemlerde süre gün sonunda biter.
(5) Mahkemelerde görülmekte olan dava, çekişmesiz yargı, geçici hukuki koruma ve diğer tüm işlemlerde UYAP'ın kullanılmasına dair usul ve esaslar yönetmelikle düzenlenir".

[62] Kanunda yer alan MERNİS ile ilgili hükümlerden birisi şu şekildedir:
"***Adres bilgilerinin kullanımı***
MADDE 52- *(1) Bakanlık, talepleri halinde kurumlara, usûl ve esasları Bakanlıkça tespit edilmek üzere adres bilgilerini elektronik ortamda Adres Paylaşımı Sistemi ve Kimlik Paylaşımı Sistemi çerçevesinde verebilir.*
(2) Teknik altyapısını tamamlamış olan muhtarlıklar sorumluluk alanlarındaki yerleşim yeri adres bilgilerinin güncelliğini takip etmek amacıyla Kimlik Paylaşımı Sistemine erişebilirler.
(3) Kurumlar, yürütecekleri iş ve işlemlerde Genel Müdürlükte tutulan adres bilgilerini esas alırlar.
(4) Adrese ilişkin bilgi ve belgeler nüfus müdürlüklerinden, Adres Paylaşımı Sisteminden veya Kimlik Paylaşımı Sistemine bağlanarak bu sistemdeki kayıtlara uygun belge üretebilen muhtarlıklardan temin edilebilir. Bu şekilde üretilen belgelerin güvenliği Bakanlığın tespit ettiği usûl ve esaslara göre sağlanır.
(5) Nüfus sayımında veya tespitinde, aile ve hayatî istatistiklerin oluşturulmasında ve bu bilgileri esas alan kanunların uygulanmasında MERNİS nüfus bilgileri kullanılır".

[63] Kanunda yer alan e-ihale projesi ile ilgili hükümlerden birisi şu şekildedir:
"***Elektronik Kamu Alımları Platformu***
Ek Madde 1- *Bu Kanun kapsamında yapılan ihalelerde; bu Kanunun 13 üncü maddesi hükümleri saklı kalmak üzere, ilan, ihale dokümanının hazırlanması ve verilmesi, katılım ve yeterliğe ilişkin belgelerin sunulması, tekliflerin hazırlanması, sunulması ve değerlendirilmesi, ihalenin karara bağlanması ve onaylanması, kesinleşen ihale kararlarının bildirilmesi ve sözleşmenin imzalanması gibi ihale süreciyle ilgili aşamalar ile her türlü bildirimler kısmen veya tamamen, Kurum tarafından oluşturulan Elektronik Kamu Alımları Platformu üzerinden gerçekleştirilebilir.*
Elektronik Kamu Alımları Platformunun kurulması ve işletilmesi ile ihale sürecinde elektronik araçların kullanımına ilişkin esas ve usuller Kurum tarafından belirlenir.
Bu Kanunun 13 üncü maddesi uyarınca yapılacak bütün ilanlar aynı zamanda Elektronik Kamu Alımları Platformunda da yayımlanır.
Bu Kanun kapsamındaki alımlarda aday veya isteklilerin yeterliğinin tespitine ilişkin olarak Elektronik Kamu Alımları Platformu üzerinden sistemler kurulabilir. Bu sistemlerin kurulması, kurdurulması, denetlenmesi, yetkilendirilen kuruluşların yetkilerinin iptal edilmesi veya tedbir niteliğinde kararlar alınması hususlarında Kurum yetkilidir".

[64] İlgili hüküm şu şekildedir:
*"**Elektronik tebligat:***
Madde 7/a - *Tebligata elverişli bir elektronik adres vererek bu adrese tebligat yapılmasını isteyen kişiye, elektronik yolla tebligat yapılabilir.*
Anonim, limited ve sermayesi paylara bölünmüş komandit şirketlere elektronik yolla tebligat yapılması zorunludur.
Birinci ve ikinci fıkra hükümlerine göre elektronik yolla tebligatın zorunlu bir sebeple yapılamaması hâlinde bu Kanunda belirtilen diğer usullerle tebligat yapılır.
Elektronik yolla tebligat, muhatabın elektronik adresine ulaştığı tarihi izleyen beşinci günün sonunda yapılmış sayılır.
Bu maddenin uygulanmasına ilişkin usûl ve esaslar yönetmelikle belirlenir".

ortamda da yapılmasına, sürecin başvuru sahibince izlenebilmesine ve sonucun ilgilisine elektronik ortamda iletilmesine yönelik tedbirler alınacağı ve hizmetin e-Devlet Kapısına entegrasyonunun sağlanacağı düzenlenmiştir.

Ülkemizde bilgi toplumu politika, hedef ve stratejileri çerçevesinde; ilgili kamu kurum ve kuruluşlarıyla gerekli işbirliği ve koordinasyonu sağlayarak e-devlet hizmetlerinin kapsamı ve yürütülmesine ilişkin usul ve esasları belirlemek, bu hizmetlere ilişkin eylem planları yapmak, koordinasyon ve izleme faaliyetlerini yürütmek, gerekli düzenlemeleri yapmak ve bu kapsamda ilgili faaliyetleri koordine etmek görevi Ulaştırma, Denizcilik ve Haberleşme Bakanlığına verilmiştir[65]. Kamu hizmetlerinin elektronik ortamda verilebilmesini sağlayan e-devlet kapısı hizmetlerinin yürütülmesi ise TÜRKSAT'a bırakılmıştır[66].

2012 BM e-devlet gelişmişlik indeksinde Türkiye 80. sırada yer almıştır[67]. İndekse göre ilk 20 ülke şu şekildedir[68].

[65] Bkz. 26.9.2011 tarihli ve 655 sayılı Ulaştırma, Denizcilik ve Haberleşme Bakanlığının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname, md. 2/1/f ve 13, RG. 1.11.2011, 28102 (Mükerrer). Bu düzenlemeden önce Başbakanlık tarafından kamoyu ile paylaşılan bir kanun taslağında bu görevlerin, taslak ile oluşturulacak Bilgi Toplumu Ajansı tarafından yürütülmesi öngörülmüştü. Bkz. http://www.gelisim.org/makaleler/e-devlet.doc, http://akgul.bilkent.edu.tr/e-devlet/taslak.pdf, 19.12.2012.

[66] Bkz. 406 sayılı Telgraf ve Telefon Kanunu, Ek md. 33, http://www.mevzuat.gov.tr/Kanunlar.aspx, 16.10.2012.

[67] United Nations, **e-Government Survey 2012**, New York, 2012, http://unpan1.un.org/intradoc/groups/public/documents/un/unpan048065.pdf, 19.12.2012, s. 28.

[68] United Nations, **e-Government Survey 2012**, New York, 2012, http://unpan1.un.org/intradoc/groups/public/documents/un/unpan048065.pdf, 19.12.2012, s. 11.

Tablo 6. 2012 BM e-devlet gelişmişlik indeksi

World e-Government Development Leaders 2012		
Sıra	**Ülke**	**e-Devlet Gelişmişlik İndeksi**
1	Kore Cumhuriyeti	0.9283
2	Hollanda	0.9125
3	Birleşik Krallık	0.8960
4	Danimarka	0.8889
5	ABD	0.8687
6	Fransa	0.8635
7	İsveç	0.8599
8	Norveç	0.8593
9	Finlandiya	0.8505
10	Singapur	0.8474
11	Kanada	0.8430
12	Avustralya	0.8390
13	Yeni Zelanda	0.8381
14	Liechtenstein	0.8264
15	İsviçre	0.8134
16	İsrail	0.8100
17	Almanya	0.8079
18	Japonya	0.8019
19	Lüksemburg	0.8014
20	Estonya	0.7987

Alexa Aralık 2012 verilerine göre Türkiye'de en çok ziyaret edilen ilk 500 internet sitesi arasında yer alan kamu kurum ve kuruluşlarına ait internet siteleri şunlardır: meb.gov.tr (23. sırada), osym.gov.tr (62. sırada), mgm.gov.tr (117. sırada), icisleri.gov.tr (139. sırada), anadolu.edu.tr (141. sırada), millipiyango.gov.tr (153. sırada), sgk.gov.tr (196. sırada), ibb.gov.tr (213. sırada), ptt.gov.tr (215. sırada), ziraatbank.com.tr (219. sırada), aa.com.tr (224. sırada), trt.net.tr (299. sırada), gib.gov.tr (310. sırada), dmi.gov.tr (320. sırada), diyanet.gov.tr (339. sırada), iskur.gov.tr (407. sırada), hastanerandevu.gov.tr (417. sırada), saglik.gov.tr (436. sırada), istanbul.edu.tr (447. sırada), iett.gov.tr (475. sırada)[69].

[69] http://www.alexa.com/topsites/countries/TR, 21.12.2012.

3. İletişim

İletişim, kişilerin çeşitli semboller aracılığı ile karşılıklı bilgi, düşünce ve duygu paylaşımı olarak tanımlanabilir[70]. İletişim kişisel bir boyut içerebileceği gibi kitlesel bir boyut da içerebilir[71]. Kişisel iletişim özel bir alan oluşturmakta ve bu özel alan içerisinde yer alan kişilerin iletişimini; kitle iletişimi ise kamusal alana yönelen ve geniş halk kitlelerine ulaşan iletişimi ifade etmektedir[72]. İki kişinin yüz yüze veya telefon ile görüşmesi veya birbirine posta göndermesi kişisel iletişime; gazete, radyo veya televizyon yayıncılığı ise kitle iletişimine örnek oluşturabilir[73]. Gerek kişisel gerekse kitle iletişiminde bazı araçlar kullanılabilir. Bu araçlar, iletişim araçlarıdır. Örneğin, klasik anlamda telefon veya posta kişisel iletişim aracı; basın, radyo, televizyon veya sinema ise kitle iletişim araçlarındandır. Konuyu internet açısından ele aldığımız zaman ise bu sınıflandırmalar nispeten anlamını yitirmektedir. İnternet kişisel iletişime olanak tanıdığı gibi kitle iletişimine de olanak tanımaktadır[74]. Bu nedenle internetin bir kişisel iletişim aracı olma özelliği bulunduğu gibi kitle iletişim aracı olma özelliği de bulunmaktadır. Bu çerçevede internet, hem kişisel hem kitle iletişimine olanak tanıyan yeni nesil bir iletişim aracı olarak tanımlanabilir. Bir kişinin arkadaşına e-mail göndermesi, msn'de, Skype'de veya bir sohbet odasında (chat room) sohbet etmesi kişisel bir iletişim olarak değerlendirilebilecekken, bir elektronik kitap (e-book) veya gazetenin veya herhangi bir düşüncenin internette yayınlanması veya bir forum sitesine yorum yazılması kitle iletişimi olarak değerlendirilebilir[75]. İnternette imkan bulan bazı iletişim türlerinin ise hem kişisel hem de kitle iletişim yönü bulunabilir. Örneğin, sosyal paylaşım

---

[70] Kayıhan İçel, Yener Ünver, **Kitle İletişim Hukuku**, Yeniden İncelenmiş 9. Bası, Beta Yayınları, İstanbul, 2012, s. 4.

[71] Barış Günaydın, **İnternet Yayıncılığı ve İfade Özgürlüğü**, Adalet Yayınevi, Ankara 2010, s. 19.

[72] İçel ve Ünver, interneti bir kitle iletişim aracı olarak değerlendirdikten sonra kitle iletişimini, "*kitle iletişim araçlarından yararlanılarak, bilgi, düşünce ve tutumların insan topluluklarına tek veya çok yanlı olarak ulaştırılması"* olarak tanımlamaktadır. İçel / Ünver, **a.g.e.**, s. 10-11.

[73] Muammer Ketizmen, **Türk Ceza Hukukunda Bilişim Suçları**, Adalet Yayınevi, Ankara, 2008, s. 22.

[74] B. Zakir Avşar, Gürsel Öngören, **İnternet Hukuku**, Türkiye Odalar ve Borsalar Birliği, Mart 2009, s. 1.

[75] Ömer Gedik, **Türk Yargı Kararları Çerçevesinde Türkiye'de Kitle İletişim Özgürlüğü**, Seçkin Yayınları, Ankara, 2008, s. 36-37.

sitesilerinde paylaşımda bulunulması kişisel bir iletişim sağlayabileceği gibi kitle iletişimi de sağlayabilir. Bugün sosyal paylaşım sitelerinde paylaşılan bilgilerin yüzbinlere ulaşması kitle iletişiminin yeni bir şekli olarak değerlendirilebilir.

İletişim araçları elektronik iletişim aracı olup olmamasına göre de bir tasnife tabi tutulabilir. Örneğin basın, elektronik olmayan bir iletişim aracı iken radyo, televizyon ve sinema elektronik iletişim araçlarıdır. internet de bir elektronik iletişim aracıdır.

İnternet; iletişiminin kapsamının net bir şekilde belirlenmesi, bu iletişimin hak ve özgürlükler bağlamında değerlendirilmesi ve sınırlarının çizilmesi aşamasında önem taşımaktadır. Bu konu çalışmanın ilerleyen bölümlerinde ilgili yerlerde ayrıca incelenmiştir.

Yeni nesil kitle iletişim aracı olarak internet diğer kitle iletişim araçlarından birçok açıdan farklılık göstermektedir. Bu farklılıklar ana hatları ile şu şekilde ele alınabilir:

1. İnternette kitle iletişimi tek yönlü bir boyut içermemekte aynı zamanda interaktif bir özelliğe de sahip bulunmaktadır. İnternetin interaktif özelliği nedeniyle kişilerin içeriğe aktif katılımı yoğun bir şekilde sağlanabilmektedir. Örneğin, Alexa Aralık 2012 verilerine göre dünyada en çok ziyaretçi alan ilk 20 internet sitesi şunlardır: google.com, facebook.com, youtube.com, yahoo.com, baidu.com, wikipedia.org, live.com, amazon.com, qq.com, twitter.com, taobao.com, blogspot.com, linkedin.com, google.co.in, yahoo.co.jp, sina.com.cn, ebay.com, google.co.jp, msn.com ve yandex.ru[76]. Alexa Aralık 2012 verilerine göre Türkiye'de en çok ziyaretçi alan ilk 20 internet sitesi ise şunlardır: facebook.com, google.com.tr, youtube.com, google.com, live.com, twitter.com, hurriyet.com.tr, milliyet.com.tr, sahibinden.com, blogspot.com, mynet.com, haberturk.com, wikipedia.org, r10.net, donanimhaber.com, gittigidiyor.com, sporx.com, yandex.com.tr, garanti.com.tr ve hepsiburada.com[77]. Görüldüğü üzere dünyada ve ülkemizde arama motorları, sosyal paylaşım siteleri, online ansiklopediler, e-

[76] http://www.alexa.com/topsites, 21.12.2012.
[77] http://www.alexa.com/topsites/countries;0/TR, 21.12.2012.

ticaret siteleri, blog siteleri, haber siteleri, sohbet ve chat siteleri en çok ziyaret edilen siteler arasında yer almakta ve yoğun bir interaktif katılım gerçekleşmektedir.

Diğer kitle iletişim araçları büyük ölçüde bu özellikten yoksundur[78].

2. Bir kitle iletişim aracı olarak internet, "*internet gazeteciliği" (Internet journalism)* veya "*internet medyası"* kavramının ortaya çıkmasına neden olmuştur[79]. İnternet gazeteciliğini, geleneksel gazeteciliğin internetteki izdüşümü olarak görenler bulunduğu gibi özgün ve yeni bir iletişim aracı olarak görenler de vardır. İlk görüşü ileri sürenler internet gazeteciliğinin sadece bir taklitten ibaret olduğunu ifade etmektedir. İnternette yer alan haberler geleneksel gazetelerde yer alan haber içeriklerinden farksızdır. İnternet gazeteciliğinde yapılan tek değişiklik geleneksel gazetelerde yer alan haberlerin içeriğinden ziyade tasarımına yöneliktir. İkinci görüşü ileri sürenlere göre ise internet gazeteciliği, gazetecilik açısından kendine özgü ve yepyeni bir alan ortaya çıkarmıştır. Bu alan, geleneksel gazetelerde yazılamayanların kolayca yazılabileceği derecede özgür ve bağımsız bir alandır. Ayrıca, internet gazeteciliği, sadece geleneksel gazetelerin internet versiyonundan oluşmamaktadır. Geleneksel gazetelerden bağımsız internet gazetelerinin sayısı her geçen gün artmaktadır.

Yeni bir medya aracı olarak ortaya çıkan internet gazeteciliği bazı hukuksal sorunları da beraberinde getirmektedir. Örneğin, internet gazeteciliğinin kamu kurumlarınca akredite edilmediği ve hukuksal bir statüye kavuşturulmadığı için ülkemizde kurumsallaşamadığı ve bu ihtiyacın acilen karşılanması gerektiği ileri sürülmektedir[80]. 20 tane gazete, 2012 yılında internet medyasına karşı ortak bir bildiri yayınlamıştır[81]. Bu bildiride, gazetelerde yer alan haberlerin internet medyasında kullanılmasının haksızlık oluşturduğu belirtilmiş ve bu tür kullanıma karşı çıkılmıştır. Kaynak gösterilerek dahi gazete haberlerine internet medyasında yer verilemeyeceği

---

[78] Günaydın, **a.g.e.**, s. 7.
[79] Günaydın, **a.g.e.**, s. 31.
[80] Medya Derneği, **Türkiye'nin İnternet Sansürü Sorunu**, Redaksiyon ve Güncelleme: Aslı Telli Aydemir, Temmuz 2010, s. 3.
[81] http://www.memurlar.net/haber/290958/, 03.10.2012.

vurgulanmıştır. Gazetelerde yer alan haberlerin kaynak gösterilmeden, kaynak gösterilerek tamamen veya kaynak gösterilerek özet şeklinde ya da hiçbir şekilde internet medyasında yer alıp alamayacağına dair açık düzenlemelere ihtiyaç bulunduğu belirtilmektedir.

3. İnternet, "*sanal topluluklar" (online communities)* ortaya çıkarmıştır[82]. Sanal topluluklar, ortak bir sorun veya ilgi alanına yönelik olarak kişilerin veya kuruluşların geçici veya sürekli elektronik iletişim araçlarını kullanarak interaktif bir şekilde bir araya geldikleri kollektif gruplar olarak tanımlanmaktadır[83]. e-Mail grupları, sohbet odaları, Second Life gibi sanal ortamlar, sosyal paylaşım siteleri, bloglar, e-ticaret siteleri, online ansiklopediler gibi sanal toplulukların etkinliği her geçen gün artmaktadır. Sanal toplulukların tanımlanması, sınıflandırılması ve takibi, kişi, kuruluş ve devletler açısından mevcut veya geleceğe yönelik olarak ortaya çıkması muhtemel sanal toplulukların gerek oluşturulması veya bunlara iştirak edilmesi ve gerekse bu toplulukların etkilenmesi açısından önem taşımaktadır[84].

Ülkemiz, sosyal paylaşım sitelerinin kullanılması açısından oldukça iyi bir konumdadır. Örneğin, Socialbakers Aralık 2012 istatistiklerine göre son altı aylık dönem içerisinde Facebook'un bugün dünyada en çok kullanıcısının bulunduğu ülkeler ABD (169.271.480 kullanıcı), Brezilya (64.048.700 kullanıcı), Hindistan (61.900.760 kullanıcı), Endonezya (51.392.040 kullanıcı), Meksika (39.961.000 kullanıcı), İngiltere (33.323.600 kullanıcı), Türkiye (31.947.120 kullanıcı), Filipinler (29.963.980 kullanıcı), Fransa (25.606.180 kullanıcı), Almanya (25.406.380 kullanıcı)'dır. Socialbakers Aralık 2012 istatistiklerine göre Türkiye, 31.947.120 kullanıcı ile Facebook'u en çok takip eden 7. ülke konumundadır[85].

Sanal topluluklar, kendi kurallarını oluşturmaya çalışmakta ve topluluk içerisinde çıkan uyuşmazlıkların kendileri tarafından çözümüne yönelik

---

[82] Uçkan, **a.g.e.**, s. 28.
[83] Robert Plant, "Online Communities", **Technology in Society**, 26, 2004, s. 54.
[84] Plant, **a.g.m.**, s. 55.
[85] http://www.socialbakers.com/facebook-statistics/?interval=last-6-months#chart-intervals, 21.12.2012.

tercihler sunabilmektedir. Örneğin, e-ticaret siteleri topluluk içerisinde ortaya çıkan uyuşmazlıkların çözümünde kişilere alternatif uyuşmazlık çözüm yöntemleri sunabilmektedir[86]. Diğer taraftan, sanal topluluklar devletin her geçen gün daha fazla ilgili alanına girmektedir.

4. İnternetin bir kitle iletişim aracı olarak geliştirdiği kavramlardan birisi "*vatandaş gazeteciliği"* (*citizen journalism)* kavramıdır. Vatandaş gazeteciliği, mesleği gazetecilik olmayan kişilerin internet üzerinden sosyal medya araçlarını da kullanarak interaktif bir şekilde internet içeriğine ve kamuoyunun oluşturulmasına katkı sağlaması olarak tanımlanabilir. Örneğin, ulusal bir gazetede güncelliğini yitirmiş ama sansasyonel bir amaç için tekrar yer verilen bir haberin daha önce yayımlanmış şekline internetten ulaşıp, bu haberin gerek yayını yapan gazete ve gerekse diğer ulusal gazetelere e-mail ile gönderilerek yayından kaldırılmasını istemek ve olumlu bir sonuca ulaşmak artık mesleği gazetecilik olmayan kişiler açısından hiç de zor değildir.

İnternet, geleneksel kitle iletişim araçlarının sahipliği ve içeriği belirlemedeki tekelcilik üzerinde adem-i merkeziyetçi bir etki doğurmaktadır[87]. Bugün internet üzerinde bir web sitesi sahibi olmak oldukça kolaydır ve ciddi bir maliyet gerektirmemektedir. İçerik üretimi konusuda da kişiler birçok şekilde düşüncelerini internet üzerinden açıklama ve elektronik faaliyette bulunma imkanına kavuşmuştur. Bu yönüyle internet, medya tekellerinin hegemonyasına meydan okuyan bir kitle iletişim aracı olma özelliği taşımaktadır[88].

5. İnternette yayınlanan bir içerik ulusal sınırları aşarak anında uluslararası bir nitelik kazanmaktadır. Bu yönüyle internet diğer kitle iletişim araşlarına nazaran daha evrenseldir. Ayrıca, internetin ortaya çıkardığı bilgi miktarı muazzam bir seviyeye gelmiştir. Bu husus, doğru bilgiye ulaşılması,

---

[86] Thomas Schultz, "Carving up the Internet: Jurisdiction, Legal Orders, and the Private/Public International Law Interface", **EJIL**, Vol. 19, No. 4, 2008, s. 833, 835.
[87] Andrew Chadwick, **Internet Politics States, Citizens, and New Communication Technologies**, Oxford University Press, New York, Oxford, 2006, s. 6.
[88] Günaydın, **a.g.e.**, s. 22.

bilginin yönetimi, analizi ve kullanılması gibi alanların önem kazanmasını sağlamıştır.

6. Anından farklı dilleri de içerebilecek şekilde birçok haber içeriğine ulaşılabilmektedir.

7. İçeriğin değiştirilmesi, ek yapılması, çıkarılması, güncellenmesi ve arşiv taraması çok daha hızlı ve kolay yapılabilmektedir[89].

8. Okuyucu, izleyici ya da dinleyici olmanın ötesinde günlük yaşama ilişkin birçok işlem internet üzerinden gerçekleştirilebilmektedir. Arama motorlarından yapılan aramalar genelde kişilerin ilgi alanlarını ve interneti kullanma amaçlarını göstermesi açısından önemlidir. Bu çerçevede aşağıda yer alan 2012 Google aramaları internetin ne derece geniş bir kullanım alanına sahip olduğunu ortaya koymaktadır.

2012 yılı içerisinde Google'da trend olan aramalar (Türkiye) şunlardır[90]:

Tablo 7. Google'da trend olan aramalar (Türkiye)

1	Facebook
2	Youtube
3	e-Okul
4	Ösym
5	Ekşi Sözlük
6	Araba
7	Milliyet
8	İşkur
9	Hürriyet
10	Habertürk

[89] Günaydın, **a.g.e.**, s. 40.
[90] http://www.google.com/zeitgeist/2012/#turkey/searches, 24.12.2012.

2012 yılında Dünyada tren olan aramalar ise şunlardır[91]:

Tablo 8. Dünyada trend olan aramalar

1	Whitney Houston
2	Gangnam Style
3	Hurricane Sandy
4	iPad3
5	Diablo 3
6	Kate Middleton
7	Olympics 2012
8	Amanda Todd
9	Michael Clarke Duncan
10	BBB12

İnternette bilgi edinebilmek için kullanılan en önemli yöntem arama motorlarına müracaat edilmesidir. Arama motorları, bazı aritmetik yöntem ve kriterlere göre aranan kelimeleri internet sitelerinde tarayıp, aranan kelimeye en uygun internet sitelerini kullanıcının önüne belli bir liste dahilinde getirmektedir. Böylece arama motorları ile kullanıcı, internette istediği bilgiye kısa sürede ulaşabilmektedir.

Arama motorları, fonksiyonlarını yerine getirirken amaçları doğrultusunda bazı internet sitelerine tarama sonucunda hiç yer vermeyebilecekleri gibi, istemedikleri internet sitelerini de listenin gerisinde bırakabilir veya gerilerde yer alan internet sitelerini haksız bir şekilde öne çıkarabilir. Bu yöndeki uygulamalar ifade özgürlüğü açısından ciddi sorunlar ortaya çıkardığı gibi arama motorlarının toplumsal, kültürel, ekonomik ve siyasi güç ve etki açısından ne derece önemli olduğunu da göstermektedir.

9. Herkes kolayca yayıncı (içerik sağlayıcı) olarak internete katılabilmekte; içerik sağlayıcı konumuna gelmek, diğer kitle iletişim araçlarına göre çok daha kolay ve herkese açık bir özellik göstermektedir. Siyasetçiler de interneti çeşitli amaçlar için kullanmaktadır. Örneğin, Socialbakers Aralık 2012 istatistiklerine göre Dünya genelinde Twitter'da en

[91] http://www.google.com/zeitgeist/2012/#the-world/searches, 24.12.2012.

çok takipçisi bulunan ilk 10 siyasetçi, Barack Obama (@BarackObama) (24.760.589 takipçi), Hugo Chávez Frías (@chavezcandanga) (3.813.259 takipçi), Arnold (@Schwarzenegger) (2.673.436 takipçi), Abdullah Gül (@cbabdullahgul) (2.587.044 takipçi), Recep Tayyip Erdoğan (@RT_Erdogan) (2.110.544 takipçi), Enrique Peña Nieto (@EPN) (1.377.029 takipçi), Mohd Najib Tun Razak (@NajibRazak) (1.089.209 takipçi), Kemal Kılıçdaroğlu (@kilicdarogluk) (1.002.277 takipçi), Sarah Palin (@SarahPalinUSA) (875.591 takipçi), عبـــدالعزيز بـــن فهـــد (@afaaa73) (820.174 takipçi)'dır[92].

10. Suiistimale açık çok daha fazla alan ortaya çıkmaktadır.

İnternet, gerek kişisel gerekse kitle iletişim aracı olarak kişilere yeni imkan ve fırsatlar sunmakla birlikte bazı hukuksal sorunların da ortaya çıkmasına neden olmaktadır. Genel olarak kişisel hak ihlalleri ve suç oluşturan eylemlerin gerçekleştirilmesi internet iletişiminin düzenlenmesi ihtiyacını ortaya çıkarmaktadır. İnternet iletişiminin ortaya çıkardığı çoğu alan birçok hukuk sisteminde yürürlükte olan mevzuat kapsamında değerlendirilmekte ve var olan hukuk kuralları ile çözüm üretilmeye çalışılmaktadır. Ancak bazı alanlar özel düzenleme gerektiren alanlar olarak düşünülmekte ve bu alanlara yönelik özel düzenlemeler öngörülmektedir. Bunun dışında genel olarak internet iletişimine yönelik düzenlemeler de yapılabilmektedir.

Ülkemizde internetin genel olarak düzenlenmesine ilişkin iki yaklaşım ortaya çıkmıştır. Birinci yaklaşım, örneğin nasıl bir kitle iletişim aracı olarak basın veya radyo-televizyon yayıncılığını genel olarak düzenleyen kanunlar varsa internet iletişiminin de benzer bir şekilde ayrı bir kanunla düzenlenmesi gerektiğini savunmaktadır[93]. Diğer yaklaşım ise internet iletişimini, basın veya radyo-televizyon yayıncılığı kapsamında değerlendirmiş ve buna yönelik düzenleme yapılmasını savunmuştur.

---

[92] http://www.socialbakers.com/twitter/group/politics/, 21.12.2012.

[93] Medya Derneği, **Türkiye'nin İnternet Sansürü Sorunu**, Redaksiyon ve Güncelleme: Aslı Telli Aydemir, Temmuz 2010, s. 6.

İnternet iletişimini basın kapsamında değerlendiren yaklaşım uygulamada karşılığını mülga 5680 sayılı Basın Kanununda 2002 yılında yapılan değişiklik ile bulmuştur[94]. Bu düzenleme ile Basın Kanununda yer alan yalan haber, hakaret ve benzeri fiillerden doğacak maddi ve manevi zararlarla ilgili hükümlerin, bilişim teknolojileri ve internet ortamında sayfa açılması veya elektronik gazete, elektronik bülten vb. suretiyle yayınlanan her türlü yazı, resim, işaret, sesli veya sessiz görüntü ve benzerleri hakkında da uygulanacağı öngörülmüştür[95].

İnternet iletişimini radyo-televizyon yayıncılığı kapsamında değerlendiren yaklaşım ise uygulamada karşılığını mülga 3984 sayılı Radyo ve Televizyonların Kuruluş ve Yayınları Hakkında Kanunun 31. maddesinde bulmuştur[96]. Yapılan değişiklik ile, her türlü teknoloji ile ve her tür iletişim ortamında yapılacak yayın ve hizmetlerin usul ve esaslarının, Haberleşme Yüksek Kurulunun belirleyeceği strateji çerçevesinde Üst Kurulca tespit edilip Haberleşme Yüksek Kurulunun onayına sunulacağı ve bu yayın ve hizmetlerin mevzuata uygunluğunun Üst Kurulca denetleneceği öngörülmüştür. Ancak, anılan Kanunun kapsam başlıklı 2. maddesinde yer alan *"Bu Kanun, her türlü teknik, usul ve araçlarla ve her ne isim altında olursa olsun elektromanyetik dalga ve diğer yollarla yurt içine ve dışına yapılan radyo ve televizyon yayınları ile ilgili hususları kapsar"* hükmü gereği 31. maddenin internet ortamında yapılan yayınlar açısından uygulanması mümkün değildir[97].

---

[94] 4756 sayılı Radyo ve Televizyonların Kuruluş ve Yayınları Hakkında Kanun, Basın Kanunu, Gelir Vergisi Kanunu ile Kurumlar Vergisi Kanununda Değişiklik Yapılmasına Dair Kanun (md. 26), RG. 21.5.2002, 24761.

[95] Söz konusu düzenlemenin yerinde bir düzenleme olduğunu savunan görüş için bkz. İçel / Ünver, **a.g.e.**, s. 457.

[96] Fikret İlkiz, "İnternet Ortamında Yayınlar", **İnternet ve Hukuk**, Derleyen: Yeşim M. Atamer, İstanbul Bilgi Üniversitesi Yayınları, İstanbul, 2004, s. 464. 31. madde metni için bkz. http://www.mevzuat.adalet.gov.tr/html/844.html, 22.02.2013.

[97] Tamer Soysal, "İnternet Servis Sağlayıcılarının Hukuki Sorumlulukları", **TBB Dergisi**, Sayı. 61, 2005, s. 330-331.

Bu düzenlemelere karşı yükselen eleştiriler[98] ile söz konusu yaklaşımlardan vazgeçilmiş ve internet iletişimi genel olarak 2007 yılında yürürlüğe konulan 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun ile özel bir düzenlemeye tabi tutulmuştur. Doktrinde 5651 sayılı Kanun, erişimin engellenmesi, içeriğin yayından çıkarılması ve cevap hakkı kurumlarının düzenlenmiş olması nedeniyle 5187 sayılı Basın Kanunu ve 6112 sayılı Radyo ve Televizyonların Kuruluş ve Yayın Hizmetleri Hakkında Kanun gibi özel bir kitle haberleşme kanunu olarak değerlendirilmektedir[99].

Ayrıca, 5809 sayılı Elektronik Haberleşme Kanununda elektronik haberleşme, interneti de kapsamına alacak şekilde *"Elektriksel işaretlere dönüştürülebilen her türlü işaret, sembol, ses, görüntü ve verinin kablo, telsiz, optik, elektrik, manyetik, elektromanyetik, elektrokimyasal, elektromekanik ve diğer iletim sistemleri vasıtasıyla iletilmesi(ni), gönderilmesi(ni) ve alınması(nı)"* olarak tanımlanmıştır. Ancak, Kanunun kapsam maddesinde 5651 sayılı Kanun hükümleri istisna tutulduğundan dolayı internete ilişkin olarak bu Kanun hükümleri, ancak 5651 sayılı Kanunda bir hüküm bulunmaması halinde uygulanabilecektir.

Bizce, yukarıda ifade edilen özellikleri internetin mutlaka diğer kitle iletişim araçlarından bağımsız olarak ele alınmasını gerektirmektedir. Bu nedenle 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun düzenlemesi yerinde bir yaklaşım olmuştur.

4. Propaganda ve Aktivizm

İnternette propaganda kişiler, sivil toplum örgütleri, siyasi partiler, terör örgütleri veya devletler tarafından yapılabilir. Propaganda birçok amaç için

---

[98] Akdeniz / Altıparmak, **a.g.e.**, s. 13. Okan Tanşu, "Bilişim Çağı, Yeni Tanımlamalar ve Hukuki Düzenlemeler", **İnternet ve Hukuk**, Derleyen: Yeşim M. Atamer, İstanbul Bilgi Üniversitesi Yayınları, İstanbul, 2004, s. 149.

[99] Kayıhan İçel, "Türkiye'de İnternet Ortamında İşlenen Suçlardan ve Kabahatlerden Sorumluluğun Genel Esasları – Erişimin Engellenmesi – İçeriğin Yayından Çıkarılması ve Cevap Hakkı", **İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi,** Yıl: 8, Sayı: 16, Güz 2009, s. 19.

yapılabilir ve bu amaç yasal bir çerçeveye dayanabileceği gibi yasa dışı bir faaliyete de bürünebilir. Devletler ulusal güvenliğin sağlanması, terör örgütlerine karşı propaganda, ulusal kimliğin güçlendirilmesi, psikolojik savaş, uluslararası alanda saygınlığın artırılması gibi amaçlarla internet üzerinden propaganda yapabilmektedir. Diğer taraftan, internet üzerinden propagandaya en fazla başvuran yapılar, terör örgütleridir. PKK ve El-Kaide gibi terör örgütleri internet üzerinden etkili bir şekilde propaganda faliyeti yürütmeyi amaçlamaktadır[100]. Sivil toplum örgütleri de interneti aktif bir şekilde kullanmakta; bilgi toplama ve dezenformasyon dahil içerik yayınlama, diyalog, devlet sırlarını ifşa[101], organize olma ve karar vericiler üzerinde lobicilik faaliyetleri gibi aktiviteler ile amaçlarını gerçekleştirmeye çalışmaktadır[102]. İnternet bu açıdan sivil toplum örgütlerine muazzam imkanlar sunmaktadır. Örneğin, internette basit bir tarama yapıldığında birçok bakan, milletvekili, belediye başkanı ve üst düzey bürokratın e-mail adresi, telefon numarası, memleketi ve eğitimi gibi bilgilere kolayca ulaşılabilmektedir.

İnternet ortamında propaganda ve aktivizm, politik amaçların gerçekleştirilmesi açısından günümüzde çok etkin bir araç haline gelmiştir. Bu etkinlik, siyasi rejimlerin değişimi sonucunu bile doğurabilmektedir. Tunus, Libya ve Mısır devrimleri internet ortamında yürütülen propaganda ve aktivizm faaliyetlerinin sonucunda gerçekleştirilebilmiştir. Bu devrimlerde sosyal medyanın çok büyük rolü olmuştur. BBC'nin yayınladığı "*How Facebook Changed The World The Arab Spring"* belgeseli[103], sosyal paylaşım sitelerinin ülkeler açısından ne kadar etkin bir şekilde kullanılabileceğini gösteren güzel bir örnek olarak ele alınabilir. Benzer

---

[100] Deibert / Rohozinski, **a.g.m.**, s. 48.

[101] Aktivist grupların internet ortamı sayesinde devlete ait sırlara erişmesi ve bunları ifşa etmesine yönelik imkan ve fırsatların gelişmesi, devletin sır olan bilgilerin gizliliğini muhafaza etmesini her geçen gün zorlaştırmaktadır. Ronald J. Deibert, "Deep Probe: The Evolution of Network Intelligence", **Intelligence and National Security**, Vol. 18, No. 4, 2003, s. 187.

[102] Dorothy E. Denning, "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy", **Networks and Netwars: The Future of Terror, Crime, and Militancy**, http://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1382/MR1382.ch8.pdf, 04.12.2012, s. 243.

[103] http://www.youtube.com/watch?v=8EnUzdkL_WU, 19.07.2012.

şekilde ülkemizde "*Gezi Parkı Eylemleri*", büyük ölçüde sosyal medya üzerinden yürütülmüş ve etkin bir hal almıştır.

Propaganda ve aktivizm, bazen bu yöntemlere başvuranların hackerlar ile işbirliği içerisinde hareket etmeleri sonucunu doğurmaktadır. Hackerların geçmişe göre günümüzde daha politik bir konuma geldikleri göz önüne alındığında aktivistlerin, hackerlar ile işbirliği içerisinde amaçlarını gerçekleştirmek açısından daha etkin bir konuma geldikleri söylenebilir[104].

5. Suç

İnternet suçta bir araç olarak kullanılabilir[105]. Dolandırıcılık, özel hayatın gizliliğinin ihlal edilmesi, kimlik hırsızlığı, hakaret, siber saldırı (kişisel veya ulusal tehdit içerikli), nefret söylemi, ırkçılık, pornografi, çocukların cinsel istismarı, kumar, uyuşturucu madde satışı, fikri mülkiyet haklarının ihlali gibi suçlar internette en çok işlenen suçlardan bazılarıdır[106].

Bilişim suçları, aşağıda ayrı bir bölüm altında incelenmiştir.

6. İstihbarat

İnternet, içerdiği muaazzam bilgi düzeyi ile önemli bir istihbarat kaynağı haline gelmiş durumdadır. İnternetin olmadığı yıllarda istihbarat faaliyetleri açısından ulaşılmak istenen bilgilere artık internet ile birlikte saniyeler içerisinde ulaşabilmek mümkündür. Otuz yıl önce devletler açısından gizli olduğu kabul edilen ve korunan bilgiler, şimdi internette herkesin ulaşabileceği şekilde yer almaktadır. Devletler, istihbarat açısından internetin sunduğu bu fırsatı kullanabilmekte ve internet ortamında önemli bilgilere ulaşabilmektedir[107].

---

[104] Deibert, **a.g.m.**, s. 179. Yazar, bu durumu *hacktivism* olarak kabul etmektedir.
[105] Muharrem Özen, İhsan Baştürk, **Temel Hak ve Özgürlükler Bağlamında Bilişim – İnternet ve Ceza Hukuku**, Adalet Yayınevi, Ankara, 2011, s. 4. Veli Özer Özbek, "İnternet Kullanımında Ortaya Çıkabilecek Bazı Ceza Hukuku Sorunları", **DEÜHFD**, C. 4, S. 1, 2002, s. 102.
[106] Özbek, **a.g.m.**, s. 107.
[107] Deibert / Rohozinski, **a.g.m.**, s. 54. Kanada istihbarat servisinin internetin dikkatli bir şekilde izlenmesi gerektiğine ilişkin raporu hakkında bkz. Deibert, **a.g.m.**, s. 188.

a. Echelon Sistemi

Echelon Sistemi, 1971 yılında ABD, İngiltere, Kanada, Avustralya ve Yeni Zelenda arasında bir elektronik izleme sistemi olarak kurulmuştur. Echelon, dünyanın herhangi bir yerinden yapılan cep telefonu, e-mail ve fax iletişimini uydular üzerinden izleyebilmektedir[108]. İnternet üzerinden yapılan her türlü iletişim de Sistemin takibi altındadır.

Soğuk savaş döneminde kurulan sistemin amacı, Sovyet emperyalizmine karşı elektronik izleme ve istihbarat toplama faaliyeti yürütmekti. Soğuk savaşın sona ermesi ile birlikte Echelon'un faaliyeti sona ermedi. Echelon, günümüzde de istihbarat toplama faaliyetine devam etmektedir. ABD, İngiltere, Kanada, Avusturalya ve Yeni Zelanda'da kurulmuş olan istasyonlar, sisteme yüklenmiş anahtar kelimeler veya ses tarama sistemi ile dünyanın herhangi bir yerinden telefon ile veya internet ortamında yapılan iletişimi tespit etmekte, dinlemekte ve kayıt altına almaktadır.

Echelon'un ekonomik casusluk ve siyasi çıkarlar için kullanıldığı da ileri sürülmektedir[109]. Sistem, ABD ve commonwealth ülkelerinin şirketlerinin uluslararası ihaleleri almalarını sağlamak için bir araç olarak kullanılmakta ve böylece söz konusu şirketlerinin küresel ekonomik düzende rekabet gücü bizzat söz konusu devletler tarafından garanti altına alınmaya çalışılmaktadır. Sistemin böyle bir amaç için kullanılması diğer ülke şirketlerinin ticari haklarını ihlal etmekte ve ülkelerin ulusal ekonomik menfaatlerine tehdit oluşturmaktadır. Ayrıca Sistem, özel hayatın gizliliği ve haberleşme özgürlüğü açısından ciddi hukuksal sorunlar ortaya çıkarmaktadır. Özel hayatın gizliliği ve haberleşme özgürlüğü açısından internet iletişiminin önleme amaçlı denetimi aşağıda ayrı bir bölüm altında incelenmiştir.

---

[108] Clay Wilson, **Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress**, CRS Report for Congress, January 2008, s. 13.

[109] Ali Çimen, **Echelon İstihbarat Dünyasının Perde Arkası**, Timaş Yayınları, 5. Baskı, İstanbul, 2006, s. 248, 255. Özgür Uçkan, Yasin Beceni, "Bilişim-İletişim Teknolojileri ve Ceza Hukuku", **İnternet ve Hukuk**, Derleyen: Yeşim M. Atamer, İstanbul Bilgi Üniversitesi Yayınları, İstanbul, 2004, s. 426.

b. Siber Casusluk

Yabancı istihbarat servisleri siber casusluk faaliyetleri yürütebilmektedir. Üretilen casus programlar sayesinde devletlerin ya da ticari kuruluşların siber ortamda yürüttükleri faaliyetler takip edilebilmekte ve önemli bilgiler ele geçirilebilmektedir. Bu yöntem, günümüz dünyasında istihbarat servislerinin gizli istihbarat elde etme yöntemlerinden birisi haline gelmiştir[110].

İstihbarat açısından günümüz dünyasında teknolojik ve ticari sırların ele geçirilmesi önem kazanmıştır[111]. "*Endüstriyel siber casusluk" (industrial cyber espionage)* kavramı, bu gelişimi ifade etmektedir. Günümüzde endüstri casusluğunu devlet politikası halinde getiren devletler bulunmaktadır. 21. yüzyılın istihbarat servisleri, uluslararası bankacılık işlemlerini takip ederek küresel ekonomideki boşlukları yakalamaya ve ulusal ekonomik çıkarları için kullanmaya çalışan bir vizyonda karşımıza çıkmaktadır[112].

II. İNTERNETİN FARKLI HUKUK DİSİPLİNLERİ İLE İLİŞKİSİ

İnternetin birçok farklı hukuk disiplini ile ilişkisi bulunmaktadır. Bu ilişkiler internet alanına özgü bir hukuk disiplinin var olup olmayacağı tartışmalarını da beraberinde getirmiştir. Doktrinde bir görüş, ayrı bir hukuk disiplini olarak internet hukukunun geliştiğini savunurken diğer bir görüş ise internet hukukunun ilgi alanına giren konuları klasik hukuk disiplinlerinin konuları arasında görmekte ve ayrı bir internet hukukunun var olamayacağını ileri sürmektedir.

Bu tartışmaların ötesinde, bir diğer tartışma konusu da internet hukukunun inceleme alanında olan konuların kamu hukuku – özel hukuk ayrımında nerede yer aldığına ilişkin yapılan tartışmalardır. Bu tartışmalar ayrı bir başlık altında incelenmiştir.

---

[110] ABD yetkililerinin, *"Sırlarımızı koruma ve diğer devletlerin sırlarını ele geçirme konusunda daha aktif olmalıyız"* şeklindeki yaklaşımı hakkında bkz. Deibert / Rohozinski, **a.g.m.**, s. 55.
[111] Çimen, **a.g.e.**, s. 236.
[112] Çimen, **a.g.e.**, s. 241.

A. Bağımsız Bir Hukuk Disiplini Olarak İnternet Hukuku

İnternetin bulunduğu bir yerde ortaya çıkan hukuksal sorunlar hukukun birçok farklı disiplinini ilgilendirebilir. İnternet kullanılarak bir suç işlendiğinde ceza hukuku, devlet tarafından bir internet sitesine erişim engellendiğinde veya örneğin şirketler tarafından kişilerin bilgileri haksız bir şekilde kaydedildiğinde ya da kullanıldığında anayasa, medeni, idare[113] ve ceza hukuku, bir sanatçının eseri internet kullanılarak haksız bir şekilde elde edildiğinde fikri mülkiyet hukuku, tüketiciyi yanıltan ürünler satışa sunulduğunda tüketicinin korunması hukuku, bir devletin internet sitelerine ülke dışından bir siber saldırı veya uluslararası bir internet şirketinin sitesinde bir ülke hukukuna aykırı yayın yapıldığında uluslararası kamu hukuku, farklı ülkelerde bulunan iki özel hukuk kişisi arasında ortaya çıkan hukuksal bir uyuşmazlıkta hangi ülke hukukunun uygulanacağının belirlenmesi açısından uluslararası özel hukuk, internet üzerinden yapılan işlemlere ilişkin elektronik kayıt ve delillerin mahkemelere sunulması gerektiğinde usul hukuku disiplinlerinin ilke ve kuralları devreye girmekte ve internet söz konusu her bir farklı disiplin açısından bir inceleme alanı oluşturmaktadır. Bunun yanında, internete özgü hukuk kurallarının gelişmesi "*bilişim hukuku*", "*siber hukuk" (cyber law)* ve *"internet hukuku" (Internet law)* gibi farklı terimlerle adlandırılan bir hukuk disiplininin gelişmesini sağlamıştır.

Siber hukuk, internet hukukundan daha geniş bir anlama sahiptir. Siber hukuk, internet hukukunu kapsamına aldığı gibi bilgisayar ile ilgili ortaya çıkan diğer hukuksal sorunlar da bu alan içerisinde incelenmektedir[114]. Bilişim hukuku kavramı da aynı anlamı ifade etmektedir. İnternet hukuku ise özel bir iletişim ağı olarak internet ortamının kullanılmasından kaynaklanan hukuksal sorunların inceleme alanını oluşturduğu bir hukuk disiplinidir.

İnternet ortamında düzenleme öngörülen alanların çoğu aslında devlet tarafından ilk defa düzenlenen alanlar değildir. İnternet var olmadan önce de devletlerin ifade özgürlüğünü güvence altına almaya, kişisel verileri

---

[113] Tekin Akıllıoğlu, "İdari Usul ve Kişisel Verilerin Korunması", http://www.idare.gen.tr/akillioglu-idariusul.htm, 05.09.2012.

[114] Viktor Mayer-Schönberger, "The Shape of Governance: Analyzing the World of Internet Regulation", **Virginia Journal of International Law**, Vol. 43, 2003, s. 607.

korumaya, ticaretin hukuksal güvence içerisinde yürütülmesine ya da müstehcenliğin cezalandırılmasına yönelik düzenlemeler yürürlüğe koydukları görülmektedir. İnternetin gelişimi ile değişen şey ya bu kuralların geliştirilmesi ya da internete özgü spesifik kuralların yürürlüğe konulması olmuştur[115]. Bu yönüyle, gelişen bu kurallar, alanında bulundukları hukuk disiplininin inceleme alanından çıkmamış ama aynı zamanda internet hukukunun inceleme alanına girmiştir. Bu nedenle internet ile ilgili konular incelenirken, aslında incelenen çoğu alanın bir geçmişi bulunduğunu unutmamak gerekir. Örneğin elektronik imza, teknolojik bir gelişmenin ürünü olarak ortaya çıkmıştır ama sözleşme hukukunun kurallarından bağımsız bir gelişim göstermemiştir. Bu nedenle, her ne kadar teknoloji yeni olsa da internet ile ilgili çoğu konuyu internet hukuku kapsamında ilk defa düzenlenmesi gereken bir alan veya sadece internet hukukunun konusu olarak görmemek gerekir.

Bununla birlikte, internet her geçen gün yeni hukuksal sorunların ortaya çıkmasına neden olmaktadır ve bu sorunlar mevcut hukuk kurallarının uygulanması ile bir çözüme kavuşturulamamaktadır. Bu sorunların çözümüne yönelik yeni hukuk kuralları yürürlüğe konulmaktadır. Bu gelişim internetin kendisine özgü bir hukukunun oluşmasına ve bunun dinamik bir yapı kazanmasına neden olmaktadır. Bazı yazarlar, internet hukukunu ayrı bir hukuk dalı olarak değerlendirmektedir[116].

Hukuka aykırı olarak bilişim sistemine zarar verme suçunda olduğu gibi bazı kurallar ise bilgisayarın ve internetin gelişimi ile ilk defa ortaya çıkmış ve internet hukuku alanındaki yerini almıştır. Hatta bilişim alanında suçlarla mücadele, siber suçlar veya bilişim suçları şeklinde adlandırılan ayrı bir ceza hukuku disiplinin ortaya çıkmasına neden olmuştur. Bu disiplin içerisinde bazı alt disiplinler de oluşmuştur. Örneğin, bilişim suçlarının tespitini sağlamak amacıyla geliştirilen teknik ve hukuksal yöntemler başlı

[115] Mayer, **a.g.m.**, s. 151.
[116] Mayer-Schönberger, **a.g.m.**, s. 607.

başına bir hukuk disiplini olarak "*adli bilişim" (computer forensic)* disiplininin ortaya çıkmasını sağlamıştır[117].

B. Kamu Hukuku Açısından İnternet

İnternet ile ilgili konuların bir kısmının kamu hukuku içerisinde değerlendirilmesinde herhangi bir tereddüt oluşmamaktadır[118]. İnternet çeşitli yönleri ile anayasa, idare, ceza, genel kamu ve uluslararası kamu hukuku disiplinlerinin ilgi alanına girmektedir.

İnternetin düzenlenmesi temel hak ve özgürlüklere, bu bağlamda özellikle ifade özgürlüğü, haberleşme özgürlüğü ve özel hayatın gizliliği hakkına müdahale oluşturduğundan bu konu Anayasa hukukunun inceleme alanlarından birisini oluşturmuştur.

İnternetin düzenlenmesinde rol alan idari kuruluşlar ve bunların görevleri, e-devlet uygulamaları, idari işlemin internet üzerinden yapılması ve ilan edilmesi[119], internet üzerinden idari başvuru, idarenin kişisel verileri işlemesi ve veri paylaşımı, internet içeriğine idare tarafından erişimin engellenmesi, filtreleme, bu alanda idarenin regülasyon[120] ve yaptırım uygulama yetkisi ve bu çerçevede idarenin düzenleyici işlemlerine ilişkin konular doğrudan idare hukukunun inceleme konuları arasına girmektedir. Siber suçlar ve bunlarla mücadele yöntemleri ise ceza hukukunun konuları arasındadır.

Devletin internetin düzenlenmesi konusunda sahip olduğu egemenlik yetkisi (jurisdiction) ile internetin bazı alanlarına ilişkin yapılan uluslararası sözleşmeler ve yetki sahibi bazı uluslararası kuruluşlar, genel kamu hukuku ile uluslararası kamu hukukunun inceleme konuları arasındadır.

İnternet ile ilgili bazı konular ise kamu hukuku – özel hukuk ayrımında herhangi bir tarafa net bir şekilde yerleştirilememektedir. Örneğin, kişisel verilerin korunması konusu bir yönüyle kamu hukuku içerisinde

---

[117] Özen / Baştürk, **a.g.e.**, s. 140 vd.
[118] İçel / Ünver, **a.g.e.**, s. 20.
[119] Münci Çakmak, "İdare Hukuku ve İnternet", **GÜHFD**, Cilt, IX, Sayı. I-II, Haziran-Aralık 2005, http://webftp.gazi.edu.tr/hukuk/dergi/9_12.pdf, 02.10.2012.
[120] Burak Öztürk, **Fransız ve Türk Hukukunda İdarenin Düzenleme Yetkisinin Kapsamı**, Yetkin Yayınları, Ankara, 2009, s. 136.

değerlendirilebilirken bir yönüyle de özel hukuk içerisinde değerlendirilmektedir[121]. Kişisel verilerin korunması konusunda yetkili kamu kuruluşlarının oluşturulması ve bunların verdiği kararların kamu hukuku kuralları[122], kişisel verilerin ihlalinden dolayı ortaya çıkan zararın tazminine yönelik düzenlemelerin ise özel hukuk kuralları olduğu düşünüldüğünde bu ayrımdaki belirsizlik internet alanı açısından daha iyi anlaşılmaktadır[123]. Bununla birlikte her ne kadar kamu hukuku – özel hukuk ayrımı internet alanında bir muğlaklaşma oluştursa da bu örnekte de görüldüğü üzere gibi kişisel verilerin korunmasını sağlayan kamu kurumlarının oluşturulması ve bunların kararlarının kamu hukuku içerisinde değerlendirilmesi gerekliliği tartışmasızdır. Bunun da ötesinde kişisel verilerin korunması konusu, insan hakları ile ilgili bir boyut taşıdığı gibi kamu düzeninin sağlanması ve serbest piyasa ekonomisinin düzenlenmesi gibi kamusal bir boyut da taşımaktadır. Yine örneğin, 5651 sayılı Kanunun 9. maddesinde yer alan içeriğin yayından çıkarılması ve cevap hakkına ilişkin düzenleme bir özel hukuk konusu gibi gözükmekle birlikte bu konuda görevli mahkemenin sulh ceza mahkemesi olarak belirlenmesi ve anılan mahkemenin kararlarının yerine getirilmemesi durumunda hapis cezasının öngörülmesi, bu müessesenin aynı zamanda bir ceza hukuku, dolayısıyla kamu hukuku konusu olduğunu da göstermektedir.

---

[121] Dilek Yüksel Civelek, **Kişisel Verilerin Korunması ve Bir Kurumsal Yapılanma Önerisi (Uzmanlık Tezi)**, Devlet Planlama Teşkilatı Müsteşarlığı, Yayın No: 2821, Ankara, Nisan 2011, s. 3. Doğan Kılınç, "Anayasal Bir Hak Olarak Kişisel Verilerin Korunması", **AÜHFD**, 61 (3), 2012, s. 1103.

[122] Kişisel verileri işleyen özel hukuk kişilerinin yetkili kamu kurumlarınca denetlenmesi, idare hukukunda yeni bir alanın ortaya çıkmasını sağlamıştır. Akıllıoğlu, **a.g.m.**, s. 2.

[123] Christopher Kuner, "Data Protection Law and International Jurisdiction on the Internet (Part 1)", **International Journal of Law and Information Technology**, Oxford University Press, Vol. 18, No. 2, 2010, s. 183.

İKİNCİ BÖLÜM
İNTERNET VE DÜZENLEME

İnternetin düzenlenmesi (Internet regulation), internet yönetişimi (Internet governance), internet hukuku (Internet law) veya bilişim hukuku (cyber law), internet sansürü (Internet cencorship), filtreleme (filtering), erişimi engelleme veya bloklama (blocking) internetin düzenlenmesi söz konusu olduğunda başvurulan kavramlardan bazılarıdır. Hukuk disiplini açısından kavramlar oldukça önemlidir. Devletin internete müdahalesinin bu şekilde farklı kavramlarla ifade edilmesi aslında hukuk ve internetin farklı yönlerine işaret etmesi açısından önem taşımaktadır.

İnternet hukuku, internet ile ilgili her türlü konuya hukuksal bir çerçeve çizmeye çalışan bir hukuk disiplinidir. Bilişim hukuku ise internet ağını kapsamına alan; ancak internet dışındaki diğer bilgi ve iletişim teknolojilerinin kullanılmasının ortaya çıkardığı hukuksal sorunlara da çözüm arayan bir disiplindir. Bu nedenle bilişim hukuku, internet hukukundan daha geniş bir çerçeveyi ifade eder.

İnternet yönetişimi, hukuk dışında internet ile ilgili yönetim konularını da kapsamına aldığından aslında çok farklı bir alanı ifade etmektedir. Ancak bununla birlikte internet yönetişiminin hukuktan bağımsız bir nitelik taşıması söz konusu olamaz.

İnternet bahsinde en olumsuz içeriğe sahip olan kavram, sansür kavramıdır. Erişimin engellenmesi, filtreleme ve bloklama ise çoğu zaman sansürün hukuksal argümanı olarak değerlendirilmektedir. İnternet sansürü, internet içeriğine erişimin devlet tarafından temel hak ve özgürlükler ihlal edilerek engellenmesi olarak tanımlanabilir; ancak erişimin engellenmesi, filtreleme veya bloklama her durumda sansür oluşturmayabilir.

Erişimin engellenmesi, filtreleme veya bloklama, özünde kişilerin hukuka aykırı bulunan içeriğe erişiminin engellenmesine yönelik hukuksal araçlardır. Ancak bu kavramlar arasında bazı farklılıklar da bulunmaktadır. Erişimin engellenmesi, daha geniş çerçevede filtreleme veya bloklama da dahil internet içeriğine erişimin her türlü engellenmesi olarak ele alınabileceği

gibi olay bazlı içeriğe erişimi engellemeyi tanımlamak için de kullanılabilir. Benzer şekilde filtreleme, geniş anlamda internet içeriğine erişimin engellenmesini sağlayan her türlü faaliyet olarak ele alınabilir. Engelleme ister otomatik şekilde (dynamic filtering) ister olay bazlı (blacklist filtering) olsun nihayetinde bu faaliyet bir filtreleme faaliyetidir[124]. Dar anlamda filtreleme otomatik olarak önceden belirlenen anahtar kelimeler ile içeriğe erişimin engellenmesini sağlayan teknik bir yöntemdir. Bloklama ise belli IP adreslerine erişimin engellenmesi anlamında kullanılmaktadır[125].

Nihayet düzenleme kavramı, apayrı bir içeriğe sahiptir. Bir konunun düzenlenmesi, olması gerekeni ortaya koyması yönüyle ayrı ve özel bir bakış açısını gerektirir. Düzenlemenin kamu hukuku açısından ele alınması ise devletin o konuya genel olarak yaklaşımını gösterir.

İnternetin devlet tarafından düzenlenmesi, oldukça tartışmalı bir konudur. Bununla birlikte devlet, interneti düzenleme konusunda oldukça isteklidir.

I. ULUSLARARASI YETKİ

"Uluslararası yetki" (international jurisdiction) sorunu, birden fazla devletin hukuksal bir konu hakkında yetki iddiasında bulunması ile ortaya çıkmaktadır. Aşağıda bu konu, internet alanında ortaya çıkan uluslararası yetki iddiaları açısından incelenmiştir.

A. Genel Olarak

Uluslararası yetki konusu kişinin hangi ülkenin hukuk kurallarına tabi olacağının belirlenmesi ile ilgilidir[126]. Yetki konusu, uluslararası hukukta yasama yetkisi (legislative jurisdiction), yargısal yetki (judicial jurisdiction) ve uygulama yetkisi (enforcement jurisdiction) olmak üzere üç farklı şekilde ele

---

[124] Peter A. Craddock, **Legal Implications of Internet Filtering**, http://www.arpia.be/public/PACraddock%20-%20Legal%20Implications%20of%20internet%20Filtering.pdf, 19.03.2013, s. 4.

[125] TJ McIntyre, Colin Scott, "Internet Filtering: Rhetoric, Legitimacy, Accountability and Responsibility", http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1103030, 18.03.2013, s. 5.

[126] Hüseyin Pazarcı, **Uluslararası Hukuk**, 10. Bası, Turhan Kitabevi, Ankara, 2011, s. 152.

alınmaktadır[127]. Yasama yetkisi, devletin düzenleme açısından sahip olduğu yetki alanını; yargısal yetki yargı mercilerinin yargılama açısından yetki alanını; uygulama yetkisi ise gerek düzenlemelerde yer alan kuralların ve gerekse mahkeme kararlarının uygulanmasındaki yetki alanını ifade etmektedir. Devletin sahip olduğu söz konusu üç tür yetki birbiri ile içiçe olmasına rağmen bazı durumlarda farklılık da gösterebilmektedir[128]. Örneğin, yargılama yetkisini haiz bir devletin yasama yetkisine sahip olmaması mümkündür. Bir devletin mahkemeleri başka bir devletin hukuk kurallarını uygulamak zorunda kalabilir. Ancak, kamu hukuku açısından bu durumun gerçekleşmesi mümkün değildir[129]. Kamu hukuku kuralları yönünden devletin egemenlik yetkisi ön plana çıkmaktadır.

B. İnternet Alanında Uluslararası Yetki

İnternet, uluslararası yetkinin kullanılması açısından klasik uluslararası hukuk konularından farklı bir çerçevede değerlendirilmektedir. İnternet yapısı itibariyle evrenseldir ve internetin ulaştığı her yerde etki doğurmaktadır. Dolayısıyla ortaya çıkardığı uluslararası sorunlar da diğer sorunlardan farklılık göstermektedir.

"İnternet alanında uluslararası yetki" (international jurisdiction on the Internet) sorunu, internette sınır ötesinden yapılan bir yayın ile suç işlenmesi[130], suç oluşturan içeriğin internet sitesinden çıkarılması veya bu siteye erişimin engellenmesi kararının verilmesi, internet iletişiminin izlenmesi, hakaretten dolayı tazminat sorumluluğu[131], sınır ötesi e-ticaretten

---

[127] Kuner, **a.g.m.**, s. 184.

[128] Kurt Wimmer, Eve Pogoriler, Stephen Satterfield, "International Jurisdiction and the Internet in the Age of Cloud Computing", http://www.cov.com, 05.03.2013, s. 5.

[129] Stephan Wilske, Teresa Schiller, "International Jurisdiction in Cyberspace: Which States May Regulate the Internet?", **Federal Communications Law Journal**, Vol. 50, Iss. 1, 1997, s. 145.

[130] Özbek, **a.g.m.**, s. 114.

[131] 5718 sayılı Milletlerarası Özel Hukuk ve Usul Hukuku Hakkında Kanunda şu hüküm yer almaktadır (md. 35):

*"**Kişilik haklarının ihlalinde sorumluluk***

***MADDE 35 –** (1) Kişilik haklarının, basın, radyo, televizyon gibi medya yoluyla, internet veya diğer kitle iletişim araçları ile ihlâlinden doğan taleplere, zarar görenin seçimine göre;*

a) Zarar veren, zararın bu ülkede meydana geleceğini bilecek durumda ise zarar görenin mutad meskeni hukuku,

b) Zarar verenin işyeri veya mutad meskeninin bulunduğu ülke hukuku veya

kaynaklanan hukuksal uyuşmazlıklarda ve kişisel verilerin korunması bakımından uygulanacak hukuk ve çözüm yerinin belirlenmesi gibi konularla ilgili olarak ortaya çıkmaktadır. Görüldüğü gibi internet alanında uluslararası yetki sorunu, hem kamu hem de özel hukuk konularını ilgilendirmektedir. Burada konu, kamu hukuku konuları açısından incelenmiştir.

1. Uluslararası Yetki Sorununun Ortaya Çıkması

İnternet ile ilgili her konuda bir uluslararası yetki sorunu ortaya çıkmamaktadır. Böyle bir sorunun ortaya çıkması için sorunun uluslararası bir boyut kazanması gerekir. İnternetin süjelerinin bulunduğu ülkelerin aynı ya da farklı olması durumuna göre sorun uluslararası bir boyut kazanabilmektedir. İnternet üzerinde düzenleme öngörülebilecek üç süje bulunmaktadır. Bu süjelerin ülkesel olarak bulundukları yer farklı sonuçların ortaya çıkmasına neden olmaktadır. Şöyle ki bu üç süjenin de ülke sınırları içerisinde bulunması durumunda bir uluslararası yetki sorunu ortaya çıkmaz ve devlet bu üç suje üzerinde de tartışmasız egemenlik yetkisini haizdir. Bunun tam aksine, bu üç sujenin ülke sınırları dışında bulunması durumunda ise devletin egemenlik yetkisini sujeler üzerinde kullanması mümkün olmadığından dolayı, devletlerin bu durumda bir düzenlemeye gitmesinin anlamı da bulunmamaktadır[132].

Bu tartışmasız iki husus dışında uluslararası yetki sorununun ortaya çıktığı alan, bu üç sujeden içeriği üretenin ülke sınırları dışında ve diğer iki sujenin ülke sınırları içerisinde bulunması durumudur. Bu durumda da eğer devlet, ülke dışından yapılan yayın üzerinde ülkesinde faaliyet gösteren aracılar aracılığıyla bir düzenleme veya yaptırım öngördüyse, bu halde de bir

---

c) Zarar veren, zararın bu ülkede meydana geleceğini bilecek durumda ise zararın meydana geldiği ülke hukuku,
uygulanır.

(2) Kişilik haklarının ihlâlinde cevap hakkı, süreli yayınlarda, münhasıran baskının yapıldığı ya da programın yayınlandığı ülke hukukuna tâbidir.

(3) Maddenin birinci fıkrası, kişisel verilerin işlenmesi veya kişisel veriler hakkında bilgi alma hakkının sınırlandırılması yolu ile kişiliğin ihlâl edilmesinden doğan taleplere de uygulanır". RG. 12.12.2007, 26728.

[132] Jack Goldsmith, Tim Wu; **Who Controls the Internet? Illusions of a Borderless World**, Oxford University Press, 2006, s. 68.

uluslararası yetki sorunu ortaya çıkmamaktadır. O halde yetki sorununun ortaya çıktığı alan, ülke dışından yapılan bir yayın hakkında, o yayını yapan içerik sağlayıcı üzerinde bir düzenleme veya yaptırım öngörülmesi durumudur.

Örneğin, Türkiye'de Facebook üzerinden iletişime geçen iki kişinin iletişim bilgilerinin Facebook tarafından tespit edilmesi ve bu bilgilerin Amerikan makamlarına aktarılması durumunda internet iletişiminin tespitinde uygulanacak hukuk kuralları açısından bir yetki sorunu bulunmaktadır. Yine örneğin, "*bulut bilişim" (cloud computing)* hizmetlerinden yararlanılması durumunda verinin tutulduğu sunucunun, veri işlem sorumlusunun, veri sahibinin ve verileri işlenen kişilerin farklı ülkelerde bulunması durumunda uluslararası yetki sorunu ortaya çıkmaktadır[133].

2. Yetki Konusuna İlişkin Uluslararası Hukuk Kuralları

Devleti uluslararası yetki konusunda sınırlandıran uluslararası kamu hukuku kurallarının bulunup bulunmadığı tartışmalıdır. Eğer devleti sınırlandıran uluslararası kamu hukuku kurallarının bulunduğu kabul edilirse devlet, her konuda uluslararası yetki iddiasında bulunamayacaktır. Bazı uluslararası sözleşmelerde devletin uluslararası yetkisinin sınırı çizilmiştir. Birleşmiş Milletler Sözleşmesinin 2. maddesinde yer alan devletlerin egemen eşitliği ilkesi bu anlamda devleti sınırlandıran uluslararası hukuk kurallarından en önemlisidir[134]. Uluslararası yetkisine saygı gösterilmeyen bir devletin misilleme ile karşılık verebileceği de genel olarak kabul edilmektedir[135]. Uluslararası Adalet Divanın da devletin uluslararası yetkisine saygı gösterilmesi gerektiği yönünde kararları bulunmaktadır[136].

Buna karşılık, özellikle ceza hukuku gibi alanlarda devletin uluslararası yetkisinin oldukça geniş olduğu ve devletin cezalandırma yetkisini uygularken

---

[133] Wimmer / Pogoriler / Satterfield, **a.g.m.**, s. 1.
[134] Schultz, **a.g.m.**, s. 808.
[135] Wilske / Schiller, **a.g.m.**, s. 126.
[136] Pazarcı, **a.g.e.**, s. 155-156.

diğer devletlerin ceza hukuku düzenlemeleri ile bağlı olmadığı görüşü de etkin bir görüş olarak ileri sürülmektedir[137].

3. Uluslararası Yetki Konusunda İleri Sürülen Teoriler

Bir devletin uluslararası bir konu hakkında yetki iddiasında bulunabilmesi için söz konusu olayla kendi arasında hukuksal bir bağ kurması gerekmektedir (bağlantı noktası)[138]. Doktrinde bu bağın çeşitli şekillerde kurulduğu bazı ilkeler geliştirilmiştir. Bunlar; "*mülkilik ilkesi" (territoriality principle), "şahsilik ilkesi" (personality principle), "koruma ilkesi" (protective principle), "hedef ilkesi" (targeting principle)*, "*etki ilkesi" (effect principle)* ve *"evrensellik ilkesi" (universality principle)* olarak ele alınabilir[139]. Bu ilkelerin uluslararası yetki sorununun ortaya çıktığı diğer kamu hukuku konularından farklı olarak internet alanındaki etkinliği ayrı bir önem taşımaktadır.

İnternet ile ilgili konularda yetkinin kullanılması açısından uluslararası bir standart bulunmamaktadır. Uygulamada, devletlerin çoğunluğu etki ilkesini uygulamakta ve yabancı bir ülke kaynaklı olsa bile ülkelerinde yayınlanan içerik hakkında yargı yetkisini doğrudan kullanmaktadır[140]. ABD gibi bazı devletler, uluslararası yetki konusunda oldukça geniş bir uygulama takip etmektedir[141].

a. Mülkilik İlkesi

Mülkilik ilkesi, kural olarak bir devletin ülkesel sınırları içerisinde düzenleme, yargılama ve uygulama yetkisinin bulunduğunu kabul eder. Bu ilke, bir devlet hukukunun diğer ülkelerde uygulanmasını da engeller. İnternet ile ilgili bazı alanlarda mülkilik ilkesine göre devletin uluslararası yetki sorunu ortaya çıkmamaktadır. Örneğin, internet ortamında yapılan yayınlar açısından veri girişinin yapıldığı yer mülkilik ilkesine göre ilgili ülke

---

[137] Durmuş Tezcan, Mustafa Ruhan Erdem, R. Murat Önok, **Uluslararası Ceza Hukuku**, Seçkin Yayınları, Ankara, 2009, s. 77-78.
[138] Tezcan / Erdem / Önok, **a.g.e.**, s. 79.
[139] Henn, **a.g.m.**, s. 160. Kuner, **a.g.m.**, s. 188-191.
[140] Mayer-Schönberger, **a.g.m.**, s. 666, 667.
[141] Wilske / Schiller, **a.g.m.**, s. 120. Uçkan / Beceni, **a.g.m.**, s. 406-407.

hukukunun uygulanmasını gerektirir[142]. Yine, erişimin engellenmesi ve filtreleme konusunda devletin yetkisini ülkesinde faaliyet gösteren servis sağlayıcılar üzerinde kullanmasında uluslararası yetki sorunu bulunmamaktadır[143]. Bu çerçevede 5651 sayılı Kanun kapsamında erişim sağlayıcı ve yer sağlayıcı açısından getirilen yükümlülükler sadece Türkiye' de bulunan erişim ve yer sağlayıcılar açısından uygulanabilir niteliktedir ve bu konuda uluslararası bir yetki sorunu da bulunmamaktadır. Benzer bir yaklaşım e-Ticaret Direktifinde de kendisini göstermiştir. Direktifin (22) numaralı gerekçesine göre, servis sağlayıcılar kural olarak kuruldukları ülke hukukuna tabi olmalıdır.

Bu ilkeye göre, ülke sınırları dışında gerçekleşse bile etkisini ülke sınırları içerisinde gösteren bir olay hakkında da söz konusu devletin uluslararası yetkisi bulunmaktadır[144]. Örneğin, devlete karşı ülke dışından bir siber saldırı gerçekleştirildiğinde bu saldırının etkisini gösterdiği ülke devletinin uluslararası yargılama yetkisi bulunmaktadır[145]. Bu çerçevede dar anlamda bilişim suçlarının ülke dışından işlenmesi durumunda siber saldırının etkisini gösterdiği ülke devleti her zaman yargılama yetkisini haizdir. TCK'nın yer bakımından uygulanması açısından Türkiye'de işlenen suçlar hakkında Türk kanunları uygulanır. Fiilin kısmen veya tamamen Türkiye'de işlenmesi veya neticenin Türkiye'de gerçekleşmesi halinde suç, Türkiye'de işlenmiş sayılır (md. 8)[146].

b. Şahsilik İlkesi

Şahsilik ilkesi, devletin kendisine özellikle vatandaşlık bağı ile bağlı olan kişiler üzerinde düzenleme ve yaptırım uygulama yetkisinin bulunduğunu kabul eden bir ilkedir[147]. Bu ilke özellikle ceza hukuku,

---

[142] Özbek, **a.g.m.**, s. 127.
[143] Wilske / Schiller, **a.g.m.**, s. 129. Schultz, **a.g.m.**, s. 824.
[144] Ceza hukuku açısından harekete üstünlük tanıyan görüş, neticeye üstünlük tanıyan görüş ve karma görüş tartışmaları için bkz. Tezcan / Erdem / Önok, **a.g.e.**, s. 87-93.
[145] Segura-Serrano, **a.g.m.**, s. 223.
[146] İçel ve Ünver'e göre, *"İnternet suçlarının internete bağlı her ülkede ve bu meyanda Türkiye'de de işlendiğini kabul etmek gerekir"*. İçel / Ünver, **a.g.e.**, s. 445. Aksi yönde bkz. Tezcan / Erdem / Önok, **a.g.e.**, s. 92-93.
[147] Pazarcı, **a.g.e.**, s. 165.

vergilendirme, diplomatik koruma gibi alanlarda uygulama alanı bulmaktadır[148]. Çocuk pornografisinin dağıtımı konusunda şahsilik ilkesine göre ülke topraklarında bulunmayan vatandaşlara yükümlülükler yüklenebilir[149]. Böylece, çocuk pornografisi ile daha etkin bir şekilde mücadele edilebilir.

c. Koruma İlkesi

Koruma ilkesine göre, bir devletin güvenliğini tehdit eden suçlara karşı bu suçlar kim tarafından veya nerede işlenirse işlensin farketmeksizin devlet uluslararası yetkiyi haizdir[150]. Bu ilke TCK'nın 13. maddesinin birinci fıkrasının (b) bendinde düzenlenmiştir. (b) bendine göre TCK'nın İkinci Kitap, Dördüncü Kısım altındaki Üçüncü, Dördüncü, Beşinci, Altıncı, Yedinci ve Sekizinci Bölümlerde yer alan suçların vatandaş veya yabancı tarafından, yabancı ülkede işlenmesi halinde, Türk kanunları uygulanacaktır. Bu çerçevede devletin bölünmez bütünlüğüne karşı internet ortamında yürütülen propaganda, dünyanın neresinden yürütülürse yürütülsün koruma ilkesi gereği Türk ceza hukuku kurallarına göre cezalandırılabilmelidir[151].

ç. Hedef İlkesi

Bu ilke, internet sitelerinin özel olarak yabancı devlet vatandaşlarını hedefleyip hedeflemedikleri hususunu esas almakta ve eğer bir internet sitesi spesifik olarak yabancı bir ülke vatandaşını hedef almışsa, ortaya çıkan hukuksal sorunlar açısından hedef alınan ülke devletinin uluslararası yetkisinin bulunduğu ileri sürülmektedir[152]. Başka bir ülke vatandaşının hedef alınıp alınmadığının belirlenmesi açısından internet sitesinin yazıldığı dil ve sunucuların konumlandırıldığı yer gibi kriterlerin değerlendirilebileceği belirtilmektedir[153]. İnternet sitesinin interaktif veya pasif bir site olup olmaması, hedef ilkesinin uygulanması açısından önemli olabilir. Belli ülke

[148] Kuner, **a.g.m.**, s. 188.
[149] Wilske / Schiller, **a.g.m.**, s. 131-132.
[150] Tezcan / Erdem / Önok, **a.g.e.**, s. 144-145.
[151] Özbek, **a.g.m.**, s. 115.
[152] Henn, **a.g.m.**, s. 163. Schultz, **a.g.m.**, s. 817-818.
[153] Henn, **a.g.m.**, s. 163. Özbek, **a.g.m.**, s. 125, 127.

vatandaşlarına yönelik interaktif bir internet sitesi yayına sunulmuşsa hedef alınan ülke devletinin uluslararası yetkisinin bulunduğu daha kolay kabul edilebilir[154]. İçerik sağlayıcının belli bir ülkeye yönelik internet yayını yapması durumunda da aynı şey söylenebilir.

d. Etki İlkesi

Etki ilkesi, uluslararası bir olay hakkında bu olayın etkisini gösterdiği devletin egemenlik yetkisinin bulunduğunu savunan anlayıştır[155]. İnternet alanında en yaygın uygulama alanı bulan ilke, etki ilkesidir.

Etki ilkesinin kabul edilmesi durumunda içerik sağlayıcının, her devletin hukukuna uygun yayın yapması gerekecektir[156]. Aksi takdirde, herhangi bir devlet kendi ulusal hukukuna aykırı bulduğu söz konusu yayın hakkında yaptırım uygulayabilme yetkisini haiz olacaktır[157]. Bu yaklaşım, içerik sağlayıcılara oldukça ağır yük getireceği ve öngörülebilirliği ortadan kaldıracağı gerekçesiyle eleştirilmektedir[158].

Mahkemelerce etki ilkesinin uygulandığı birçok karar verilmiştir. Alman federal soruşturma makamı, ABD'de faaliyet gösteren *Compuserve*'e ait ikiyüz civarında tartışma grubu hakkında Alman çocuk pornografisi ile mücadeleye ilişkin hukuk kuralları gereğince erişimi engelleme kararı vermiş ve firma bu karara uymak zorunda kalmıştır[159]. Ayrıca, Almanya'daki şirket genel müdürü hakkında hapis cezası verilmiştir[160].

Doktrinde, internet alanına ilişkin uluslararası yetki konusu ele alındığında ilk atıf yapılan davalardan birisi "*LICRA v. Yahoo"* davasıdır *(La Ligue Contre Le Racisme et L' Antisemitisme (LICRA) v. Yahoo! Inc.)*[161]. Yahoo'nun Fransa'daki web sitesinde Nazi içerikli ürünlerin satılmasının

---

[154] Wimmer / Pogoriler / Satterfield, **a.g.m.**, s. 12.
[155] Schultz, **a.g.m.**, s. 812.
[156] Henn, **a.g.m.**, s. 173.
[157] Schultz, **a.g.m.**, s. 812.
[158] Özbek, **a.g.m.**, s. 124.
[159] Wilske / Schiller, **a.g.m.**, s. 122-123.
[160] Özbek, **a.g.m.**, s. 119.
[161] Bernhard Maier, "How Has The Law Attempted to Tackle The Borderless Nature of The Internet?", **International Journal of Law and Information Technology**, Vol. 18, No. 2, Oxford University Press, 2010, s. 144.

Fransız ceza hukukuna aykırılık oluşturduğu gerekçesiyle söz konusu hukuka aykırı içeriğin internet sitesinden çıkarılması için 2000 yılında Fransız mahkemesinde Yahoo'ya karşı iki Fransız grup tarafından dava açılmıştır[162]. Söz konusu ürünlerin Yahoo'nun web sitesinde yer alması ABD hukukuna aykırılık oluşturmamaktadır[163].

Knobel, ırkçılığın Fransız hukukunda yasak olduğunu; her ne kadar Yahoo, bir Amerikan şirketi olsa ve sunucuları bu ülkede bulunsa da Yahoo'nun Fransa'daki web sayfalarında yer alan hukuka aykırı içeriğe karşı Fransız hukukunun uygulanacağını iddia etmiştir. Yahoo yetkilileri ise internetin kontrolünün imkansız olduğunu, Yahoo'nun birçok ülkede faaliyet gösterdiğini ve bu ülkelerin her birinin hukukunu ayrı ayrı göz önünde bulundurmanın mümkün olmadığını ileri sürmüştür[164]. Onlara göre, Yahoo'nun Amerika'da olan sunucularına konulan içerik Fransa'nın egemenlik alanı dışında kalmaktadır[165].

2000 yılında Fransız Mahkemesi kararını vermiş; Yahoo'nun Fransa'dan erişilebilen sayfaları üzerinde Fransız yargısının egemenlik yetkisinin bulunduğu, söz konusu web sayfalarında satış için Nazi ürünlerinin bulunmasının Fransız hukukuna aykırı olduğu, coğrafik olarak Yahoo'nun Fransa'daki kullanıcıları tanımlayabilmesi ile bu kullanıcıların ilgili sayfalara erişiminin engellenebilmesinin teknik olarak çok büyük oranda mümkün olduğu ve bu teknik kabiliyet çerçevesinde Yahoo tarafından filtrelemenin yapılması gerektiğine hükmedilmiştir[166]. Yahoo, bu kararın ABD'de faaliyet gösteren bir şirket olarak kendileri hakkında uygulanamayacağını ileri sürmüş ve bunu sağlamak için Kaliforniya bölge mahkemesinde dava açmıştır *(Yahoo! Inc. v. La Ligue Contre Le Racisme et L' Antisemitisme (LICRA))*[167]. Mahkeme, Fransız mahkemesinin kararının Yahoo hakkında uygulanmasını Birinci Değişiklik hükümlerine (First Amendment) aykırı

[162] Goldsmith / Wu, **a.g.e.**, s. 1-2. Henn, **a.g.m.**, s. 168.
[163] Maier, **a.g.m.**, s. 145.
[164] Schultz, **a.g.m.**, s. 810.
[165] Segura-Serrano, **a.g.m.**, s. 203.
[166] Goldsmith / Wu, **a.g.e.**, s. 7-8.
[167] Maier, **a.g.m.**, s. 147.

bulmuştur[168]. Bu dava doktrinde, hukuka aykırı internet içeriğine bir ülke sınırları içerisinden erişilmekle birlikte içerik sağlayıcının ülke dışında bulunması durumunda, anılan içerikle ilgili olarak içerik sağlayıcının bulunduğu ülke devleti yanında içeriğin ulaştığı ülke devletinin uluslararası yetkisinin de bulunduğunu gösteren bir dava olarak kabul edilmekte ve örnek gösterilmektedir[169].

Etki ilkesinin bu derece geniş bir çerçevede ele alınması ve yorumlanması, internet ortamında yapılan bir yayından dolayı her devletin uluslararası yetkiye sahip olması gibi bir tablo karşımıza çıkarmaktadır. Uluslararası yetkinin bu derece geniş bir çerçevede ele alınmasının ortaya çıkarabileceği sakıncaları gidermek amacıyla internet ortamında yapılan yayın ile ilgili ülke devleti ve vatandaşları arasında bir bağ kurularak etki ilkesinin aranması gerektiği ileri sürülmektedir[170]. Bu yaklaşım uygulamada da kendisini göstermektedir. Örneğin, Alman Federal Veri Koruma Kanununa (the German Federal Data Protection Act) göre bu Kanun, Avrupa Birliği dışında bulunan bir veri işleme sorumlusunun Almanya'daki kişisel verileri toplaması, işlemesi veya kullanması durumunda da uygulanır (md. 1/5)[171]. Çocukların Online Ortamda Mahremiyetinin Korunması Hakkında Kanun (The US Children's Online Privacy Protection Act (COPPA)'a göre, Amerika'daki çocuklar hakkında bilgi toplayan herhangi bir site hakkında, bu sitenin içerik sağlayıcısı Amerika dışında dünyanın herhangi bir yerinde bulunsa bile bu Kanun hükümleri uygulanır[172]. Avustralya İstenmeyen e-Mail Kanunu (The Australian Spam Act 2003)'na göre istenmeyen ticari e-mailler ülke dışından gelse bile bu Kanun hükümleri uygulanır. Benzer şekilde, Avustralya Mahremiyet Kanunu (Australian Privacy Act 1998)'na göre Avustralya dışından gerçekleştirilse bile kişisel verilerin işlenmesine ilişkin

[168] Henn, **a.g.m.**, s. 169.
[169] Segura-Serrano, **a.g.m.**, s. 204.
[170] Tezcan / Erdem / Önok, **a.g.e.**, s. 92-93.
[171] Kuner, **a.g.m.**, s. 191.
[172] Kuner, **a.g.m.**, s. 192.

hususlar Avusturalya vatandaşlarını veya bu ülkede ikamet edenleri ilgilendiriyorsa bu Kanun hükümleri uygulanır[173].

TCK'da bilişim suçlarına ilişkin Türk devletinin sahip olduğu uluslararası yetki açısından uygulanabilecek hükümler bulunmaktadır. Kanunun 12. maddesine göre bir yabancı, Kanunun 13. maddesinde yazılı suçlar dışında, Türk kanunlarına göre aşağı sınırı en az bir yıl hapis cezasını gerektiren bir suçu yabancı ülkede Türkiye'nin zararına işlediği ve kendisi Türkiye'de bulunduğu takdirde, Türk kanunlarına göre cezalandırılır. Yargılama yapılması Adalet Bakanının istemine bağlıdır. Bu suçun bir Türk vatandaşının veya Türk kanunlarına göre kurulmuş özel hukuk tüzel kişisinin zararına işlenmesi ve failin Türkiye'de bulunması halinde, bu suçtan dolayı yabancı ülkede hüküm verilmemiş olması koşulu ile suçtan zarar görenin şikayeti üzerine fail, Türk kanunlarına göre cezalandırılır.

İnternet alanında yürürlüğe konulan düzenlemelerin ve mahkeme kararlarının uygulanabilmesi *(enforcement jurisdiction)* ise konuyu farklı bir noktaya taşımaktadır. Uygulanabilirlik için, hakkında düzenleme yapılan veya karar verilen kişiler veya bunların malvarlığının ilgili ülke egemenlik alanında bulunması veya konunun ilgili devletlerce uluslararası bir anlaşma ile çözüme kavuşturulması gerekmektedir[174]. Bu çerçevede örneğin, devletlerin etkinliğine göre, kimi devletler almış oldukları kararları uluslararası internet şirketlerine kolayca uygulatabilirken kimi devletler ise bu konuda başarısız kalmaktadır. Bu şirketler, güçlü devletlerin veya malvarlıklarının bulunduğu ülkelerin taleplerini göz önünde bulundurmakta, diğer devletlerin taleplerini ise söz konusu devletlerin egemenlik alanında bulunmadıkları gerekçesiyle reddetmektedir[175].

---

[173] Kuner, **a.g.m.**, s. 193.
[174] OpenNet Initiative, **A Starting Point: Legal Implications of Internet Filtering**, 2004, http://www.opennetinitiative.org, 09.10.2012, s. 11. Schultz, **a.g.m.**, s. 813.
[175] Goldsmith / Wu, **a.g.e.**, s. 81-82.

e. Evrensellik İlkesi

Bu ilkeye göre soykırım, köle ticareti ve terör suçları gibi bazı suçların yargılanmasında, anılan suçlar ile devlet arasında herhangi bir bağ aranmaksızın her devletin uluslararası yargılama yetkisinin bulunduğu kabul edilmektedir[176]. Söz konusu suçların internet ortamında işlenmesi durumunda da evrensellik ilkesine göre her devletin yargılama yetkisi söz konusu olabilir. TCK'nın 13. maddesinde yer alan suçların[177] vatandaş veya yabancı tarafından internet ortamında işlenmesi halinde Türk kanunları uygulanır.

Çocuk pornografisinin her ne şekilde olursan olsun üretimi, dağıtımı, indirilmesi veya bulundurulmasına yönelik suçlar, evrensellik ilkesine göre her devlet tarafından cezalandırılabilmelidir.

II. İNTERNETİN DÜZENLENMESİ KONUSUNDA İLERİ SÜRÜLEN TEORİLER

İnternetin düzenlenmesi konusunda karşımıza, düzenlemeyi savunan ve buna karşı olan iki anlayış çıkmaktadır. Günümüzde belli bir noktaya kadar anlamını yitirmiş olan bu ayrım, tarihsel gelişimin ortaya konulabilmesi

---

[176] Tezcan / Erdem / Önok, **a.g.e.**, s. 148-149.

[177] TCK'nın 13. maddesi aşağıdaki şekildedir:

*"**Diğer suçlar***

***Madde 13** - (1) Aşağıdaki suçların, vatandaş veya yabancı tarafından, yabancı ülkede işlenmesi halinde, Türk kanunları uygulanır:*

a) İkinci Kitap, Birinci Kısım altında yer alan suçlar.

b) İkinci Kitap, Dördüncü Kısım altındaki Üçüncü, Dördüncü, Beşinci, Altıncı, Yedinci ve Sekizinci Bölümlerde yer alan suçlar.

c) İşkence (madde 94, 95).

d) Çevrenin kasten kirletilmesi (madde 181).

e) Uyuşturucu veya uyarıcı madde imal ve ticareti (madde 188), uyuşturucu veya uyarıcı madde kullanılmasını kolaylaştırma (madde 190).

f) Parada sahtecilik (madde 197), para ve kıymetli damgaları imale yarayan araçların üretimi ve ticareti (madde 200), mühürde sahtecilik (madde 202).

g) Fuhuş (madde 227).

h) (Mülga : 26/6/2009 – 5918/1 md.)

i) Deniz, demiryolu veya havayolu ulaşım araçlarının kaçırılması veya alıkonulması (madde 223, fıkra 2, 3) ya da bu araçlara karşı işlenen zarar verme (madde 152) suçları.

(2) (Ek ikinci fıkra: 29/6/2005 – 5377/3 md.) İkinci Kitap, Dördüncü Kısım altındaki Üçüncü, Dördüncü, Beşinci, Altıncı ve Yedinci Bölümlerde yer alanlar hariç; birinci fıkra kapsamına giren suçlardan dolayı Türkiye'de yargılama yapılması, Adalet Bakanının talebine bağlıdır

(3) Birinci fıkranın (a) ve (b) bentlerinde yazılı suçlar dolayısıyla yabancı bir ülkede mahkûmiyet veya beraat kararı verilmiş olsa bile, Adalet Bakanının talebi üzerine Türkiye'de yargılama yapılır".

açısından önem taşımaktadır. Bu iki anlayış dışında ayrıca, karma yönetişim modelini savunan yazarlar da bulunmaktadır.

A. İnternetin Düzenlenmesi Anlayışına Karşı Olan Teoriler

İnternetin düzenlenmesine karşı olan teoriler; özgürlükçü ve self-regülasyon teorisi olarak karşımıza çıkmaktadır.

1. Özgürlükçü Teori

Özgürlükçü teori, internetin devletlerin egemenlik alanından tamamen bağımsız olmasını savunan anlayıştır. Bu teorinin özünü, internetin gerçek dünyadan apayrı, sanal bir dünya oluşturduğu görüşü oluşturmaktadır[178]. Özellikle ABD'de 90'lı yıllarda taraftar bulmuştur[179]. Doktrinde internetin özgür olması konusu ele alındığında genelde hemen bu düşüncenin bir öncüsü olarak "*A Declaration of Independence of Cyberspace"* deklarasyonu ile John Perry Barlow'a atıf yapılmaktadır[180].

Teorinin savunucuları, internetin doğası gereği hiçbir sınıra tabi olmadığını ileri sürmektedir[181]. Devletler tarafından öngörülen her sınırlandırma sonuçsuz kalacaktır. İnternet evrensel ve sınır tanımaz bir yapıya sahiptir. Ayrıca, devletlerin interneti düzenlemeye çalışmaları çözülmesi mümkün olmayan hukuksal sorunlar ortaya çıkarır. Bir devletin internet üzerinde düzenleme yapmaya çalışması diğer devletlerin egemenlik alanına müdahale anlamına gelir ve bu düzenlemelerin diğer devletlerin egemenlik alanlarında uygulanması mümkün değildir. Bu görüş, internet düzenlenmesinin teknik olarak mümkün olmadığını da ileri sürmektedir. Özellikle internette yer alan hukuka aykırı içeriğin engellenmesi teknik olarak mümkün değildir. Yapılan her türlü engelleme, bir şekilde internet kullanıcıları tarafından aşılacak ve engellenen içeriğe erişilebilecektir.

Bu teoriye karşı ileri sürülen eleştirilerden en önemlisi bu anlayışın "*siber anarşi" (cyber anarchy)* doğurabilecek bir içeriğe sahip olduğu

---

[178] Mayer-Schönberger, **a.g.m.**, s. 618.
[179] Segura-Serrano, **a.g.m.**, s. 194.
[180] Mayer-Schönberger, **a.g.m.**, s. 618. Schultz, **a.g.m.**, s. 802.
[181] Uçkan / Beceni, **a.g.m.**, s. 420.

yönündedir. Ayrıca, internet gerçek dünyadan apayrı, sanal bir dünya değil; aksine gerçek dünyanın bir parçasını oluşturmaktadır. İnternetin düzenlenmesi konusunda bazı teknik sıkıntılar bulunsa da, devletin internet üzerinde öngördüğü düzenleme ve sınırlandırmaların, tamamen işlevsiz olduğu da ileri sürülemez.

2. Self-Regülasyon Teorisi

Bu teoriye göre, internet kullanıcıları tarafından informel olarak zaten "*netiquette*"[182] *(internet görgü kuralları)* olarak isimlendirilen bir internet kurallar bütünü kendiliğinden oluşturulmuştur[183]. Sistem, bu kurallar bütünü dahilinde hiçbir devlet müdahalesi olmaksızın kendiliğinden işlemekte ve teknolojik ilerlemelere karşı kendisini otomatik olarak yenilemektedir. İnternetin yönetimi, merkezi kontrolü elinde bulunduran devletler tarafından değil, bizzat internetin kullanıcısı olan kişiler ve bu kişiler tarafından oluşturulan gruplar *(online communities)* tarafından sağlanmalıdır. Bu görüş, *citizen* kavramının yerine kişileri milliyetlerinden bağımsız olarak "*netizen" (internet kullanıcısı)* kavramı altında toplamakta ve internet yönetiminin kişiler tarafından sağlanması gerektiğini savunmaktadır.

Self-regülasyon teorisi, özgürlükçü teori gibi ABD orijinlidir. Bu teori, özgürlükçü teoriden düzenlemeyi tamamen reddetmemesi yönü ile ayrılmaktadır. İnternetin doğduğu Amerika'da self-regülasyon düşüncesi özellikle 1990'lı yıllarda oldukça taraftar bulmuş, interneti devletin egemenlik alanından ayırmak ve ulusal hukuk kuralları dışında internete özgü hukuk kuralları oluşturmanın özgürlükler açısından kaçınılmaz olduğu savunulmuş, özellikle 2000'li yıllardan sonra ise devletin interneti düzenleme yetkisini kullanmaya başlaması ile birlikte bu görüş etkinliğini kaybetmeye başlamıştır[184].

Bu teori, internetin kendi kendisini yönetmesinin mümkün olmadığı gerekçesiyle eleştirilmiştir. Eleştirilere göre, internetin kendi geliştirdiği

---

[182] "*Netiquette"*, görgü kuralları anlamına gelen ingilizce *etiquette* kavramının internete uyarlanmış şekli olarak kullanılmaktadır. Mayer-Schönberger, **a.g.m.**, s. 620.
[183] Segura-Serrano, **a.g.m.**, s. 196.
[184] Goldsmith / Wu, **a.g.e.**, s. 14.

kuralların devletlerin müdahalesi olmaksızın uygulanması mümkün değildir[185]. Ayrıca, self-regülasyon teorisi belli güçlerin internet üzerinde egemen duruma gelmeleri ve interneti kendi çıkarlarına yöneltmeleri sonucunu doğurabilir.

B. İnternetin Düzenlenmesi Anlayışını Savunan Teoriler

İnternetin düzenlenmesi anlayışını savunan teoriler, ulusal ve uluslararası düzenleme anlayışını savunan teoriler olarak ikiye ayrılabilir.

1. Ulusal Düzenleme Anlayışını Savunan Teoriler

Ulusal düzenleme anlayışını savunan teorilerin dayanağını oluşturan gerekçeler farklılık göstermektedir. Ulusal egemenliğin sağlanması, e-ticaretin güvenliği, kültürel farklılığın korunması ve kişisel hakların güvence altına alınması gerekçelerine dayanan teoriler, ulusal düzenleme anlayışını savunmaktadır.

a. Ulus-Devlet Egemenlik Teorisi

Ulus-devlet egemenlik teorisine göre hiçbir devlet, ülke sınırları dışında gerçekleştirilmiş bir faaliyetin zararlı sonuçlarının kendi ülke sınırları içerisinde etki göstermesine müsaade etmez. Bu husus aynı zamanda uluslararası hukukun genel ilkelerinden birisi olarak kabul edilmiştir. Devletler egemenlik yetkisine saygı duyulmasını talep etme hakkına sahiptir. Her devlet, devlet olmanın gereği olarak ülke sınırları içerisinde gerçekleşen zararlı etkiden dolayı, zararlı etkiye neden olan kişilerin milliyetleri ve faaliyetin ülke sınırları dışında gerçekleştirilmiş olması önem arz etmeksizin zararlı faaliyetin sahibi olan kişileri hukuksal ve cezai yargılamaya tabi tutar. Ülke dışından gerçekleştirilen internet faaliyetleri bunun tipik bir örneğini oluşturmaktadır.

Bu teori, şirketlerin tabi olduğu kurallar boyutundan yola çıkarak uluslararası internet şirketlerinin diğer uluslararası şirketlerden, faaliyette

---

[185] Segura-Serrano, **a.g.m.**, s. 197.

bulundukları ülkelerin ulusal hukuklarına uymaları bakımından hiçbir farkları olmadığını ileri sürmektedir[186]. Nasıl uluslararası internet şirketleri, ilgili ülke kurallarına uymadan bu ülkelerde iş yapamıyorlarsa aynı şekilde söz konusu şirketlerin de bu ülkelerde iş yapamaması gerekir. Bu değerlendirme esas alındığı zaman örneğin, Youtube'a yüklenen ve Türk hukukuna aykırılık oluşturan videoların aykırılığının Türk yetkili makamlarınca tespiti ve youtube yetkililerine ulaştırılması halinde videolara Türkiye'den erişimin engellenmesi gerekir. Youtube, Türkiye'de faaliyette bulunmak istiyorsa Türk hukuk kurallarına uygun hareket etmek zorundadır. Goldsmith'in örneğinden yola çıkarak örneğin, nasıl bugün Mercedes Benz Türkiye'de faaliyet gösterirken Türk hukuk kurallarına uygun olarak faaliyet gösterebiliyorsa, aynı durum youtube açısından da her yönüyle geçerlidir[187].

İnternetin düzenlenmesi konusunda ulus-devletin etkinliğinin ortadan kaldırılmasının, Amerikan hukukunun ve Batı değerlerinin dünyaya hakim kılınması gibi bir amaç taşıdığı da ileri sürülmektedir[188]. İnternet Amerika tarafından keşfedilmiş ve bugün internetin sunduğu imkanlardan en fazla yararlanan ve internet içeriğini şekillendiren güçler Batı kaynaklıdır. Bu teoriye göre, internetin devletler tarafından düzenlenmesi demokrasi ve hukuk devleti ilkelerinin de bir gereğidir ve bu ilkelerin uygulanması açısından düzenleme, devletsel bir zorunluluktur. Demokrasi içerisinde meşruiyetini halktan alan bir devletin internet konusunda düzenleme yapamaması, sahip olduğu meşruiyetin sorgulanması sonucunu doğurabilir.

Bu teori özellikle, internet üzerinde devletlere düzenleme yetkisi tanınması durumunda içerik sağlayıcıların her devletin hukuksal düzenlemelerine uygun hareket etmek zorunda kalacağı; bunun ise hem demokratik ve adil bir yaklaşım olmayacağı hem de teknik olarak mümkün olmayacağı gerekçesiyle eleştirilmektedir[189].

---

[186] Goldsmith / Wu, **a.g.e.**, s. 160.
[187] Goldsmith / Wu, **a.g.e.**, s. 160.
[188] Schultz, **a.g.m.**, s. 804.
[189] Mayer-Schönberger, **a.g.m.**, s. 612.

b. e-Ticaretin Güvenliği İçin Düzenleme Teorisi

e-Ticaretin güvenliği için düzenleme teorisine göre, bir ülkede e-ticaretin yürütülebilmesi için hukuki düzenleme kaçınılmaz görünmektedir. Nasıl her hukuk devletinde sanal olmayan ticari ilişkiler ticaret kanunları ile düzenlenmişse ve düzenleme, hukuk devleti açısından bir gereklilik ise aynı durum e-ticaret açısından da söz konusudur. Aksi halde, elektronik ortamda ticari ilişkilerin yürütülmesi mümkün olamaz. Örneğin, Amerikan hukukuna göre eBay kullanıcısı, bu site üzerinden yapmış olduğu bir ticari ilişkiden dolayı eBay'i sorumlu tutamamaktadır. Bu çerçevede, Amerika'da eBay'e sağlanmış bu hukuksal güvenlik olmasaydı bugün bu firmanın bu haliyle başarılı bir şekilde var olamayacağı ileri sürülmüştür[190].

İnternet üzerinden kişilerin e-imzalarını kullanarak veya e-sözleşme yaparak ticari faaliyetlerini yürütmeleri ticari hayatın bir gerekliliği olarak ortaya çıkmıştır. E-imza ve e-sözleşme müesseseleri hukuk düzenince tanınmadan ve düzenlenmeden, o ülkede e-ticaretin gelişmesi mümkün gözükmemektedir. Artık günümüzde devletin interneti düzenlemesi ve hukuksal güvence sağlaması gerekliliği hususunda en aktivist olanlar, e-ticaret şirketleridir.

e-Ticaretin güvenliği için düzenleme teorisi uygulama alanında da fazlasıyla kendisini göstermektedir. Örneğin, AB'nin internetin düzenlenmesindeki yaklaşımlarından birisi de Avrupa entegrasyonunun güçlendirilmesi amacıyla ekonomik nitelikli ve internetin spesifik alanlarına yönelik düzenlemeler yapmak şeklindedir[191].

c. Kültürel Farklılık Teorisi

Kültürel farklılık teorisine göre, her toplum farklı bir toplumsal yapıya ve değerlere sahiptir. Bu değerler doğrudan hukuku etkilemekte ve hukuksal düzenlemeler bu değerler ekseninde şekillenmektedir. İnternet söz konusu olduğunda da her toplum açısından doğru kabul edilebilecek bir kurallar

---

[190] Goldsmith / Wu, **a.g.e.**, s. 139.
[191] Mayer, **a.g.m.**, s. 156.

bütünü ortaya konulamaz[192]. Kimi ülkelerin değerleri pornografiyi olumlu karşılayabilirken kimi ülkelerin değerleri bunu kabul etmez[193]. Bu kültürel farklılıklara saygı duymak dışında hukukun yapabileceği başka birşey yoktur. Bu nedenle internetin her devlet açısından kendi kuralları çerçevesinde düzenlenmesi ve herkesin buna saygı duyması gerekir. Örneğin, internette yayınlanan "*Innocence of Muslims"* isimli film[194] içeriğinin Müslümanların dini inançlarına açık bir saldırı ve nefret suçu (hate crime) oluşturduğu konusunda genel olarak Müslümanlar görüş birliği içerisinde iken Batılılar söz konusu filmin ifade özgürlüğü kapsamında değerlendirilebileceğini ileri sürmüştür[195]. Bu durumda hangi toplumun değerlerine göre internet düzenlenecektir? Kültürel farklılık teorisine göre her toplum kendi değerlerine göre interneti düzenleme hakkına sahiptir.

Uygulamaya bakıldığında da gerçekten devletlerin interneti düzenleme yaklaşımları kültürel farklılıklarına göre oldukça değişiklik göstermektedir. Örneğin, genel olarak Batı ülkelerinde ırkçılığın önlenmesi, İslam ülkelerinde ise pornografik içerik önemli bir internet düzenleme nedenidir.

ç. Kişisel Hakların Korunması İçin Düzenleme Teorisi

Toplumsal bir konunun devlet tarafından düzenlenmesi, kişilerin sahip oldukları hak ve sorumlulukları belirlediği için aslında bir taraftan da kişi haklarına güvence getiren bir yapıya sahiptir. Örneğin, internette dolandırıcılığın önlenmesi için kamu gücünün devreye girmesi gerekir. Aynı şekilde, kişinin bir fotoğrafının, video görüntüsünün veya isminin kişilik haklarını zedeleyecek bir şekilde internette yer alması veya internette kişiye hakaret içeren yayınların yapılması durumunda, kişilik haklarına yapılan tecavüzün önlenmesi ve hakkın kişiye teslim edilmesi için yine kamu

---

[192] Henn, **a.g.m.**, s. 172.
[193] Özbek, **a.g.m.**, s. 114.
[194] http://www.youtube.com/watch?v=DqdtEyLQKf4, 03.10.2012.
[195] Çoğu islam ülkesinde internet ortamında yapılan İslam karşıtı görüşler yasaklanmaktadır. İnternet ortamında, Batı ile İslam dünyası arasında Müslümanların Hıristiyanlaştırılması ve buna karşı konulmasına yönelik ciddi bir mücadele kendisini göstermektedir. Bkz. Helmi Noman, **In The Name of God: Faith-Based Internet Censorship In Majority Muslim Countries**, Opennet Initiative, August 2011, s. 7, 9.

gücünün, bir diğer deyişle devletin düzenleme ve yaptırım uygulama yetkisinin varlığına ihtiyaç duyulacaktır[196].

İnternet ile ilgili belki en çok yazılan, fikir üretilen ve gündemde tutulan konu, fikri mülkiyet haklarının korunması konusudur. Bu konuda, devletlerin gereken önlemleri alması gerektiğine ilişkin ciddi bir çaba vardır. Bu çerçevede, fikri mülkiyet haklarının korunmasının, ancak Devletlerin öngöreceği düzenlemeler ile gerçekleştirilebileceği söylenebilir.

2. Uluslararası Düzenleme Anlayışını Savunan Teori

Uluslararası düzenleme anlayışını savunan teori, internetin sınırları aşan bir nitelik taşıması ve evrensel bir yapıya sahip olması nedeniyle bu alanın ancak uluslararası düzeyde düzenlenebileceğini ileri sürmektedir[197]. İnternet ile ilgili bazı alanlar özellikle uluslararası bir işbirliği gerektirmektedir[198]. Fikri mülkiyet haklarının korunması, siber suçlarla mücadele ve kişisel verilerin korunması gibi alanların uluslararası düzenleme gerektirdiği ifade edilmiştir[199]. Bu teori, uygulamada da karşılığını bulmuş ve söz konusu alanlara ilişkin olarak bazı uluslararası sözleşmeler yapılmıştır.

İnternet ile ilgili bazı sorunlar uluslararası bir içeriğe sahiptir ve bu sorunların çözümü birden fazla devletin egemenlik alanı ile ilgilidir. Bu durum ise kaçınılmaz olarak uluslararası hukuk kurallarının devreye girmesini gerektirmektedir.

Uluslararası düzenleme teorisi, özellikle toplumların kültürel farklılıklarının uluslararası düzenlemelere yansıtılamayacağı gerekçesiyle eleştirilmektedir.

C. Karma Yönetişim Teorisi

Karma yönetişim teorisi (mixed governance), diğer teorilerin internetin düzenlenmesi konusunda uç noktaları oluşturduklarını, aslında düzenleme

---

[196] John Weckert, "What Is So Bad About Internet Content Regulation", **Ethics and Information Technology** 2, Kluwer Academic Publishers, 2000, s. 107.
[197] Mayer-Schönberger, **a.g.m.**, s. 626.
[198] Weckert, **a.g.m.**, s. 108.
[199] Segura-Serrano, **a.g.m.**, s. 201.

konusunda devletlerin, uluslararası kuruluşların, kişi ve toplulukların birlikte etkin olduğu bir yönetişim anlayışının gerçekleştirilebileceğini savunmaktadır[200]. Örneğin, bu teoriye göre ICANN'ın yapısı, ulusal, uluslararası ve self-regülasyon teorilerini; internet alanına ilişkin AB direktiflerinin öngördüğü yapı ise ulusal ve uluslararası düzenleme teorilerini birlikte bünyesinde barındıran bir yönetişim anlayışını oluşturmaktadır[201].

Ç. Değerlendirme

İnternetin devlet tarafından düzenlenmesine karşı olan fikirler *"don't regulate the Internet"* veya *"hands off the Internet (internete dokunma)"* sloganları ile özellikle 90'lı yıllarda doktrinde bazı yazarlarca ileri sürülmüş ve artık günümüzde bu görüşler etkinliğini kaybetmiştir[202]. Devletin her yönüyle interneti düzenleme konusunda yetkisinin bulunduğu artık tartışmasızdır[203]; devletin ve uluslararası kuruluşların uygulaması da bu yöndedir[204]. Tartışılan konular ise yapılan düzenlemelerin içeriğine ilişkin hususlardır[205].

İnternetin düzenlenmesine karşı olan anlayışları çok da sağlam temelleri ve felsefi anlayışları olan fikirler olarak görmemek gerekir. İnternet birçok hukuksal sorunu beraberinde getirmiştir ve bu süreç devam etmektedir. Hukuksal sorunların olduğu yerde düzenleme olmak zorundadır[206]. Önemli olan bu düzenlemenin kim tarafından yapılacağı ve içeriğine ilişkin hususlardır. Ulusal egemenlik anlayışı ve ulus-devlet yapılanmalarının geçerli olduğu bir dünyada, internet her ne kadar evrensel bir yapıya sahip olsa da her devlet egemenlik yetkisini kullanmak istemektedir.

---

[200] Mayer-Schönberger, **a.g.m.**, s. 631.
[201] Mayer-Schönberger, **a.g.m.**, s. 646, 656.
[202] Philip J. Weiser, "Internet Governance, Standard Setting and Self-Regulation", **Northern Kentucky Law Review**, Vol. 28: 4, s. 823-825. Schultz, **a.g.m.**, s. 802. Deibert / Rohozinski, **a.g.m.**, s. 49.
[203] Tekin Memiş, "Erişimin Engellenmesi, Hukuki Sorunlar ve Çözüm Önerileri", **EÜHFD**, C. XIII, S. 3-4, 2009, s. 163.
[204] Wilske / Schiller, **a.g.m.**, s. 121.
[205] Deibert / Rohozinski, **a.g.m.**, s. 56.
[206] İçel / Ünver, **a.g.e.**, s. 18. Mayer-Schönberger, **a.g.m.**, s. 619.

Diğer taraftan, özgürlükçü ve self-regülasyon teorisi, aslında göründüğü kadar da özgürlükçü bir içeriğe sahip değildir. Örneğin devletlerin müdahalesinin olmadığı bir internet düşündüğümüz zaman nihayetinde internet bir şekilde birileri tarafından yönetilecektir[207]. İnternetin kim tarafından yönetileceği sorusunu sorduğumuzda ise her olasılığın yolunun uluslararası internet şirketlerine ve ABD'ye çıktığı görülmektedir. Öte yandan, eğer internet birileri tarafından yönetilemeyecekse o zaman bir siber anarşizmin ortaya çıkması kaçınılmaz gözükmektedir.

Özgürlükçü ve self-regülasyon teorileri, piyasa çıkarlarını temsil eden piyasa temelli teorilerdir. Bu teorilerin genel kamu yararını veya temel hak ve özgürlükleri gerçek anlamda temsil edebildiğini söylemek oldukça güçtür.

Uygulamaya baktığımız zaman devletlerin 90'lı yıllardan itibaren ve özellikle 2000'lerden sonra artan bir trend içerisinde interneti çeşitli yönleriyle düzenlemeye tabi tuttukları görülmektedir[208]. Örneğin AB, internetin düzenlenmesi konusunda pasif bir yaklaşım sergilememiş, aksine aktif bir şekilde internetin değişik alanlarına ilişkin olarak çeşitli direktifler yürürlüğe koymuştur. E-ticaret, kişisel verilerin korunması ve siber suçlarla mücadele gibi alanlarda birçok AB direktifi bulunmaktadır. AB, söz konusu direktif yaklaşımı ile üye ülkeler arasında bir uygulama birliği ve standardizasyon sağlamayı amaçlamıştır[209].

Nihayet, burada yapılan değerlendirmeler devletin internet ile ilgili her konuda mutlaka düzenleme yapması gerektiği gibi bir sonuç ortaya çıkarmamaktadır. Devlet gerekli gördüğü alanlarda düzenleme yapabileceği gibi gerekli görmediği alanlarda yönetimi, internetin kendi sistemine bırakabilir. Nihayetinde buna karar verecek olan devletin kendisidir. Bu noktada diğer önemli bir konu düzenlemenin içeriğidir ve tartışılması gereken esas husus düzenlemenin içeriğine ilişkin konulardır.

---

[207] Mayer, **a.g.m.**, s. 161.

[208] 2000'li yıllara kadar Almanya, Fransa ve AB'nin interneti düzenleme çaba ve girişimleri için bkz. Mayer, **a.g.m.**, s. 151-161. Chadwick, **a.g.e.**, s. 2.

[209] İnternetin düzenlenmesi konusunda ABD'nin üstünlüğüne karşı Avrupa cephesinden ciddi bir direniş vardır. Bu alanda Avrupa etkin bir duruma gelmeye çalışmakta ve interneti birçok açıdan düzenlemektedir. Mayer, **a.g.m.**, s. 150.

III. İNSAN HAKLARI AÇISINDAN İNTERNETİN DÜZENLENMESİ

Bu bölümde insan hakları açısından internetin düzenlenmesi genel olarak ele alınmış, internet düzenlemesinin spesifik alanlarına yönelik değerlendirmeler ise ilgili olduğu yerlerde ayrıca yapılmıştır.

A. İnternet Düzenlemesinin İnsan Hakları Üzerindeki Etkisi

İnsan hakları, kişilerin sırf insan olmasından dolayı doğuştan sahip oldukları kişiliğe bağlı, dokunulamaz ve devredilemez temel hak ve özgürlükler olarak tanımlanmaktadır[210]. Kaynağını doğal hukuk felsefesinden alan bu tanımlama[211] pozitif hukuk belgeleri ile daha somut bir şekle büründürülmüştür[212]. İnsan haklarının özellikle 2. Dünya Savaşından sonra uluslararası insan hakları sözleşmelerinde yer almaya başlamasıyla birlikte bu alanda önemli gelişmeler kaydedilmiştir. Günümüzde insan hakları, anayasaların da güvence altına aldığı çağdaş demokratik hukuk devletlerinin olmazsa olmaz önemli bir değeri haline gelmiştir[213]. İnsan haklarının güvence altına alınması özgürlükçü demokratik hukuk devletinin vazgeçilmez önceliğidir.

İnsan hakları, negatif-pozitif-aktif statü hakları, birinci-ikinci-üçüncü kuşak haklar, kişi-siyasi-sosyal haklar, insan-vatandaşlık hakları, bireysel-kollektif haklar gibi sınıflandırmalar yapılarak açıklanmaya çalışılmaktadır[214]. Bu tür sınıflandırmalar oldukça anlamlıdır ve her sınıflandırma insan haklarının farklı açılardan önemine işaret etmektedir. Ancak, biz burada sadece Anayasamızda öngörülen yaklaşım üzerinde durmayı yeterli gördük. İnsan hakları, Anayasamızın İkinci Kısmında "*Temel Haklar ve Ödevler*" başlığı ile düzenlenmiş; bu kısım içerisinde "*Kişinin Hakları ve Ödevleri*", "*Sosyal ve Ekonomik Haklar ve Ödevler*", "*Siyasi Haklar ve Ödevler*"

---

[210] Mustafa Erdoğan, **İnsan Hakları Teorisi ve Hukuku**, Genişletilmiş 2. Baskı, Orion Kitabevi, Ankara, 2011, s. 38.
[211] Anıl Çeçen, **İnsan Hakları**, Savaş Yayınevi, Genişletilmiş 3. Basım, Ankara, 2000, s. 26.
[212] Ergun Özbudun, **Türk Anayasa Hukuku**, Gözden Geçirilmiş 12. Baskı, Yetkin Yayınları, Ankara, 2011, s. 108.
[213] Çeçen, **a.g.e.**, s. 53.
[214] Durmuş Tezcan ve Diğerleri, **İnsan Hakları El Kitabı**, Seçkin Yayınları, Genişletilmiş 3. Baskı, Ankara, 2010, s. 72-77. Erdoğan, **a.g.e.**, s. 180-181.

bölümlerine yer verilmiştir. Böylece, Anayasa ile öngörülen insan hakları yaklaşımı kaynağını G. Jellinek'in teorisini ouşturduğu negatif-pozitif-aktif statü hakları ayrımından almıştır[215]. Negatif statü hakları, yaşam hakkı, kişi hürriyeti, özel hayatın gizliliği, konut dokunulmazlığı gibi devletin müdahalesinin istenmediği haklardır. Pozitif statü hakları, çalışma hakkı, sağlık, çevre ve konut hakkı ve sosyal güvenlik hakkı gibi devlete aktif bir yükümlülük yükleyen haklardır. Aktif statü hakları ise kişilerin seçme ve seçilme, kamu hizmetine girme ve dilekçe hakkı gibi yönetime katılımını sağlayan haklardır.

İnternete yönelik düzenlemeler birçok hak ve özgürlük üzerinde etki doğurabilmektedir. İfade özgürlüğü, haberleşme özgürlüğü, bilim ve sanat özgürlüğü, özel hayatın gizliliği, kişinin maddi ve manevi varlığını koruma ve geliştirme hakkı, düzeltme ve cevap hakkı, ailenin korunması ve çocuk hakları ve gençliğin korunması internet düzenlemesinden en çok etkilenen hak ve özgürlüklerdir. Özgürlükler birbirini tamamlayıcı nitelikte olabilir. Örneğin, internette ifade özgürlüğüne getirilecek bir sınırlandırma aynı zamanda bilim ve sanat özgürlüğünü de sınırlandırabilir. Böyle bir durumda ifade özgürlüğü ile bilim ve sanat özgürlüğü birbirini tamamlamaktadır. Özel düzenlemenin (lex specialis) genel düzenlemeden (lex generalis) önce uygulanması gerektiğinden dolayı bu durumda bilim ve sanat özgürlüğüne ilişkin özel düzenlemelerin öncelikle uygulanması söz konusu olacaktır[216]. Özgürlükler birbiriyle çatışır bir nitelik de arz edebilir[217]. Örneğin, ifade özgürlüğünün özel hayatın gizliliği veya kişinin maddi ve manevi varlığını koruma ve geliştirme hakkı ile çatışması oldukça muhtemeldir. Özgürlüklerin çatışması durumunda tatmin edici bir sonuca varmak her zaman mümkün olamamaktadır. Ancak, böyle bir durumda özgürlüklerden birinin diğerine

---

[215] Hasan Tunç, Faruk Bilir, Bülent Yavuz, **Türk Anayasa Hukuku**, 3. Baskı, Berikan Yayınevi, Ankara, 2011, s. 119.
[216] Tezcan ve Diğerleri, **a.g.e.**, s. 273.
[217] Günaydın, **a.g.e.**, s. 76. Tezcan ve Diğerleri, **a.g.e.**, s. 245.

feda edilmemesi, somut olayın özelliklerine göre bir değerlendirilmeye varılması gerektiği belirtilmektedir[218].

İnternet konusunda yapılan herhangi bir düzenlemenin hangi hak ve özgürlüğü doğrudan etkilediği hususunun belirlenmesi önem arz etmektedir. Yapılan düzenlemelerin tamamını sadece bir hak veya özgürlük çerçevesinde ele almak doğru bir sonuç ortaya çıkarmamaktadır. Örneğin, internet düzenlemelerini bir bütün olarak kişisel haberleşme özgürlüğü çerçevesinde ele almak mümkün değildir. Benzer şekilde, internet iletişiminin tamamı doğrudan kişisel haberleşme veya ifade özgürlüğü ile ilgili olmadığından, internet düzenlemeleri bir bütün olarak ifade özgürlüğü çerçevesinde de ele alınamaz[219]. İnternet ortamında yer alan kişisel haberleşmeye ilişkin iletişimin kişisel haberleşme özgürlüğü çerçevesinde ele alınması mümkündür. İçeriğine belirsiz sayıda kişinin ulaşabildiği bir internet sitesine yönelik düzenleme ise ifade özgürlüğü ile ilgili bir konudur. Bu ayrımın yapılması oldukça önemlidir. Yoksa, internette yer alan kişisel haberleşmeye ilişkin bir konunun ifade özgürlüğü için öngörülen sınırlamalar ve güvenceler ile açıklanması söz konusu olacaktır. Aynı şey bunun tersi açısından da söz konusu olabilir. İfade özgürlüğüne ilişkin hususlar da kişisel haberleşme özgürlüğüne ilişkin sınırlandırma ve güvenceler ile açıklanamaz.

Aslında, hak ve özgürlükler açısından ortaya çıkan sorunların çoğu sırf internete özgü sorunlar değildir. İnternet ortamında karşılaşılan sorunlar, fiziksel dünyada karşılaşılan sorunların sadece internete yansımış halidir. Hakaretin önlenmesi ve bunun ifade özgürlüğü ile çatışması olgusu fiziksel dünyada nasıl karşımıza çıkıyorsa aynı şekilde internet ortamında da karşımıza çıkmaktadır. Bununla birlikte bazı sorunlar ise sadece internete özgüdür. Örneğin, ifade özgürlüğü açısından bir internet sitesine erişimin engellenmesi internet ortamına özgü bir hak ve özgürlük sorunudur.

---

[218] Murat Volkan Dülger, Yasin Beceni, **Türkiye'de İnternet Sitelerinin Erişiminin Engellenmesi Konusunda Farklı Hukuk Disiplinleri Açısından Değerlendirmeler**, Yayın No: TÜSİAD-T/2011, 03; 512, Mart 2011, s. 14.

[219] Ketizmen, **a.g.e.**, s. 23-24.

B. İfade Özgürlüğü ve İnternetin Düzenlenmesi

İnternet üzerinde yapılan düzenlemeler doğrudan ifade özgürlüğü ile bağlantılı konulardır. Örneğin, zararlı bir içeriğe erişimin engellenmesine yönelik bir karar ifade özgürlüğünü tamamen ortadan kaldırabilir. Zararlı içeriğe erişimin engellenmesi ile ifade özgürlüğünün sağlanması arasındaki hassas dengenin hassasiyetle gözetilmesi gerekir.

Hak ve özgürlükler, anayasalar yanında uluslararası sözleşmeler ile de güvence altına alınmaktadır. İnsan Hakları Evrensel Bildirgesi[220], Kişisel ve Siyasi Haklar Uluslararası Sözleşmesi[221] ve Avrupa İnsan Hakları Sözleşmesi[222] bu çalışma kapsamında ele alınan uluslararası insan hakları sözleşmeleridir. İnsan Hakları Evrensel Bildirgesinin 19. maddesine göre herkes düşünce ve ifade özgürlüğüne sahiptir. Bu özgürlük, müdahale olmaksızın kanaat taşıma ve herhangi bir yoldan ve ülke sınırlarını gözetmeksizin bilgi ve fikirlere ulaşmaya çalışma, onları edinme ve yayma serbestliğini de kapsar. Benzer bir hüküm Kişisel ve Siyasi Haklar Uluslararası Sözleşmesi ve Avrupa İnsan Hakları Sözleşmesinde de yer almıştır. Kişisel ve Siyasi Haklar Uluslararası Sözleşmesinin 19. maddesine göre herkesin, bir müdahale ile karşılaşmaksızın fikirlere sahip olma hakkı vardır. Herkes, ifade özgürlüğü hakkına sahiptir; bu hak bir kimsenin ülke hudutlarıyla sınırlanmaksızın sözlü, yazılı veya basılı veya sanatsal ürün şeklinde veya kendi tercih ettiği başka bir iletişim vasıtasıyla her türlü bilgi ve düşünceyi arama, edinme ve ulaştırma özgürlüğünü de içerir. Avrupa İnsan Hakları Sözleşmesinin ifade özgürlüğü başlıklı 10. maddesine göre ise, herkes görüşlerini açıklama ve anlatım özgürlüğüne sahiptir. Bu hak, kanaat özgürlüğü ile kamu otoritelerinin müdahalesi ve ülke sınırları söz konusu olmaksızın haber veya fikir almak ve vermek özgürlüğünü de içerir.

---

[220] The Universal Declaration of Human Rights 1948. Türkçe versiyon için bkz. http://www.meb.gov.tr/belirligunler/insan_haklari/bildirge.htm, 2.1.2013. İngilizce versiyon için bkz. http://www.un.org/en/documents/udhr/, 2.1.2013.

[221] International Covenant on Civil and Political Rights 1966. Türkçe versiyon için bkz. http://www.tbmm.gov.tr/komisyon/insanhaklari/pdf01/53-73.pdf, 2.1.2013. İngilizce versiyon için bkz. http://www2.ohchr.org/english/law/ccpr.htm, 2.1.2013.

[222] Convention for the Protection of Human Rights and Fundamental Freedoms 1950. Türkçe versiyon için bkz. http://www.anayasa.gov.tr/files/bireysel_basvuru/AIHS_tr.pdf, 2.1.2013. İngilizce versiyon için bkz. http://www.conventions.coe.int/Treaty/en/Treaties/Html/005.htm, 2.1.2013.

İfade özgürlüğüne ilişkin söz konusu uluslararası sözleşmelerde yer alan hükümler Anayasamızda da karşılığını bulmuştur. Anayasamızın 26. maddesine göre, herkes, düşünce ve kanaatlerini söz, yazı, resim veya başka yollarla tek başına veya toplu olarak açıklama ve yayma hakkına sahiptir. Bu hürriyet resmi makamların müdahalesi olmaksızın haber veya fikir almak ya da vermek serbestliğini de kapsar. Anayasamızda ifade özgürlüğünün bazı özel görünüm şekilleri ayrıca düzenlenmiştir. Bilim ve sanat özgürlüğü (md. 27) ve basın özgürlüğüne (md. 28. vd.) ilişkin hükümler bu çerçevede ayrıca düzenlenen özgürlüklerdir. AİHS'de bu özgürlükler ayrıca düzenlenmemiş; ifade özgürlüğü kapsamında öngörülmüştür[223].

Doktrinde ifade özgürlüğünün üç unsurunun bulunduğu belirtilmektedir: Bilgi edinme özgürlüğü, düşünce özgürlüğü ve düşünceyi açıklama özgürlüğü[224]. Bilgi edinme özgürlüğü, kişinin istediği bir konuda bilgi kaynaklarına ulaşmasını, araştırabilmesini, haber alabilmesini ve öğrenebilmesini ifade etmektedir. Bilgi edinme özgürlüğü, düşünce ve düşünceyi açıklama özgürlüğünden önce gelir. Bilgi edinilemeyen bir ortamda düşüncenin oluşması söz konusu olamaz. Bu nedenle bilgi edinme özgürlüğü, ifade özgürlüğünün en temel yapı taşıdır.

Bilgi edinme özgürlüğünün, yeni bir hak olarak "*internete erişim hakkını"* da içerdiği ileri sürülmektedir. İnternete erişim hakkının ise, devletler açısından negatif bir yükümlülük yanında aynı zamanda pozitif bir yükümlülük de içerip içermediği tartışmalıdır. Bir kısım yazar bilgi edinme özgürlüğünün, devletler açısından bazı pozitif ve negatif yükümlülükler gerektirdiği kanaatindedir. Onlara göre internete erişim bağlamında devlet, pozitif bir yükümlülük olarak kişilerin internete erişiminin sağlanması için gerekli olan ortamı oluşturmak; negatif bir yükümlülük olarak ise kişilerin internete erişimine müdahale etmemek yükümü altındadır. Aksi görüşte olan yazarlar

[223] Erdoğan, **a.g.e.**, s. 221.
[224] Çeçen, **a.g.e.**, s. 253.

ise bilgi edinme özgürlüğünün devletler açısından sadece negatif bir yükümlülük içerdiği kanaatindedir[225].

Düşünce özgürlüğü, kişinin herhangi bir konu hakkında sınırsız bir şekilde düşünce sahibi olabilmesini, düşüncesini açıklamaya zorlanamamasını, düşüncelerinden dolayı kınanamaması ve suçlanamamasını ifade eder. Düşünce özgürlüğü mutlak ve sınırsız bir özgürlük olarak kabul edilmiştir. Düşünceyi açıklama özgürlüğü ise, kişinin sahip olduğu düşünceyi kendini ifade edebilecek herhangi bir şekilde özgürce açıklayabilmesi ve bundan dolayı kınanmaması ve suçlanamamasını ifade etmektedir. Ancak, düşünceyi açıklama özgürlüğü mutlak ve sınırsız kabul edilmemiş, bazı sınırlardırmalara tabi tutulmuştur.

Açıklanamayan bir düşüncenin özgürlüğünden bahsetmek olanaksız olduğundan, düşünce özgürlüğü ile düşünceyi açıklama özgürlüğü arasında bu şekilde bir ayrım yapılması aslında çok anlamlı değildir. Bir düşünce, ancak açıklandığı zaman gerçek özgürlüğe ulaşır. Bu nedenle düşünce ve düşünceyi açıklama özgürlüğünü bir bütün olarak değerlendirmek gerekir.

Kitle iletişim araçları, ifade özgürlüğünün gerçekleştirilmesini sağlayan araçlardır. Basın, radyo ve televizyon, sinema ve internet gibi kitle iletişim araçları bu çerçevede ifade özgürlüğünün gerçekleştirilmesinin olmazsa olmazlarındandır[226]. Kitle iletişim araçları ile yapılan yayınlara getirilecek sınırlandırmalar bu çerçevede ifade özgürlüğünün sınırlandırılması sonucunu doğurabilir. Bir kitle iletişim aracı olarak internetin düzenlenmesine ilişkin hususların da ifade özgürlüğünü sınırlandırması mümkündür. Ancak, internetin düzenlenmesine yönelik her düzenlemenin doğrudan ilgili olduğu özgürlük ifade özgürlüğü değildir. İnternet ortamında yapılan kişisel haberleşme niteliğindeki iletişim, ifade özgürlüğü çerçevesinde değil, kişisel haberleşme özgürlüğü çerçevesinde ele alınabilir. Yine, özel hükmün önceliği ilkesi gereği internet ortamında yer alan bilimsel ve sanatsal eserlere ilişkin düzenlemeler öncelikle Anayasamızın bilim ve sanat özgürlüğünü

---

[225] Bkz. Alisdair A. Gillespie, "Restricting Access To The Internet By Sex Offenders**", International Journal of Law and Information Technology**, Oxford University Press, Vol. 19, No. 3, 2011, s. 169.

[226] Tezcan ve diğerleri, **a.g.e.**, s. 274.

düzenleyen 27. maddesi hükümleri çerçevesinde ele alınmalıdır. İnternette yer alan içerikten dolayı kişilerin cezai yaptırıma tabi tutulması, içeriğe erişimin engellenmesi, filtreleme, içeriğin yayından çıkarılması ve cevap hakkı gibi konular internette en fazla ifade özgürlüğünü ilgilendirebilecek konular olarak karşımıza çıkmaktadır. Bu konular aşağıda ilgili yerlerde incelenmiş ve gerektiği yerlerde ifade özgürlüğü açısından değerlendirmeler ayrıca yapılmıştır.

İnternetin düzenlenmesine ilişkin hususların basın özgürlüğü çeçevesinde ele alınması ise mümkün gözükmemektedir. Basın özgürlüğünün çerçevesini yazılı basın oluşturmaktadır[227]. Nitekim 5187 sayılı Basın Kanununda, Kanunun amaç ve kapsamı *"Bu Kanunun amacı, basın özgürlüğünü ve bu özgürlüğün kullanımını düzenlemektir. Bu Kanun basılmış eserlerin basımı ve yayımını kapsar"* olarak belirlenmiş ve 2. maddede basılmış eser, *"Yayımlanmak üzere her türlü basım araçları ile basılan veya diğer araçlarla çoğaltılan yazı, resim ve benzeri eserler ile haber ajansı yayınlarını,"* olarak tanımlanmıştır. Bu çerçevede internet ortamında yapılan yayınların basılmış eser olarak kabul edilmesi mümkün gözükmemektedir[228].

C. Özel Hayatın Gizliliği ve İnternetin Düzenlenmesi

Avrupa İnsan Hakları Sözleşmesinin "*Özel ve Aile Hayatına Saygı Hakkı"* başlıklı 8. maddesine göre, herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir. Özel hayatın gizliliği ve korunması hakkı Anayasamızda ise 3 farklı hükümde yer almıştır. Anayasamızın 20. maddesinde "*özel hayatın gizliliği"*, 21. maddesinde "*konut dokunulmazlığı"*, 22. maddesinde ise "*haberleşme özgürlüğü"* düzenlenmiştir. İnternet düzenlemesinin konut dokunulmazlığı ile bir ilgisi bulunmamaktadır. İnternet düzenlemesi, özel hayatın gizliliğini düzenleyen 20. madde ve haberleşme özgürlüğünü düzenleyen 22. madde ile ilgilidir.

20. maddeye göre herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. İnternet düzenlemesine ilişkin

---

[227] Günaydın, **a.g.e.**, s. 98-99.
[228] Özbek, **a.g.m.**, s. 105. İlkiz, **a.g.m.**, s. 453.

hususların kişilerin özel hayatı ve aile hayatını etkilemesi her zaman mümkündür. Örneğin, kişinin özel hayatına ilişkin resimlerin kişinin rızası dışında internet ortamında yer almamasına yönelik düzenlemeler bu özgürlüğü güvence altına almaktadır. Söz konusu maddeye 2010 yılında eklenen bir hükümle[229] kişisel verilerin korunması da anayasal güvence altına alınmıştır. Bu düzenlemeye göre herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel verilerin özel hukuk kişileri ve devlet tarafından işlenmesi, erişim ve yer sağlayıcılar tarafından kullanıcıların internet trafik bilgisinin tutulması gibi konular kişisel verilerin korunması hakkı ile ilgili konulardır.

Anayasamızın 22. maddesine göre ise herkes, haberleşme özgürlüğüne sahiptir ve haberleşmenin gizliliği esastır. 22. maddede düzenlenen özgürlük kişisel haberleşme özgürlüğüdür. Bu özgürlüğün kitle iletişim özgürlüğü ile ilgili bir yönü bulunmamaktadır. Maddede yer alan, haberleşmenin gizliliğinin esas olmasına ilişkin düzenleme de bunu göstermektedir. Kitle iletişimine ilişkin bir haberleşmenin gizliliğinden bahsedilemez. İnternet ortamında yapılan kişisel haberleşmeye ilişkin düzenlemelerin Anayasamızın 22. maddesi çerçevesinde ele alınması gerekir. E-posta, msn, Skype ve sohbet odaları gibi ortamlarda yapılan iletişim bu çerçevede 22. madde ile güvence altına alınmıştır. Bu tür ortamlarda yapılan iletişimin izlenmesi veya engellenmesi 22. madde çerçevesinde değerlendirilecektir.

Ç. İnternet Özgürlüğü

İnternetin diğer kitle iletişim araçlarından farklı özelliklere sahip olması ve ifade özgürlüğü açısından ortaya çıkardığı muazzam gelişim, "*internet özgürlüğü"* isminde yeni nesil bir özgürlüğün ortaya çıkmasına neden

[229] 5982 sayılı Türkiye Cumhuriyeti Anayasasının Bazı Maddelerinde Değişiklik Yapılması Hakkında Kanun, RG. 13.5.2010, 27580.

olmuştur[230]. Gerçi, insan haklarını düzenleyen mevcut uluslararası sözleşme ve anayasalarda doğrudan internet özgürlüğüne ilişkin bir hak yer almamaktadır; ancak her geçen gün internet özgürlüğünün söz konusu belgelerde yer alması gerektiğine ilişkin yaklaşımlar güç kazanmaktadır.

İnternet özgürlüğü, basın veya radyo-televizyon özgürlüğü gibi düşüncenin internet aracılığıyla ifade edilmesine yönelik bir özgürlük olarak tanımlanabilir[231].

D. Özgürlüğün Sınırları

İfade özgürlüğü ve özel hayatın gizliliği hakkının kullanılması her hukuk sisteminde bazı sınırlandırmalara tabi tutulmuştur.

1. İfade Özgürlüğünün Sınırları

Genel olarak ifade özgürlüğü, sınırsız bir özgürlük değildir. Gerek Avrupa İnsan Hakları Sözleşmesinde gerekse Anayasamızda bazı sınırlandırmalar öngörülmüştür. Avrupa İnsan Hakları Sözleşmesine göre kullanılması görev ve sorumluluk yükleyen ifade özgürlüğü, ulusal güvenliğin, toprak bütünlüğünün veya kamu emniyetinin korunması, kamu düzeninin sağlanması ve suç işlenmesinin önlenmesi, sağlığın veya ahlakın, başkalarının şöhret ve haklarının korunması veya yargı gücünün otorite ve tarafsızlığının sağlanması için bazı biçim koşullarına, sınırlamalara ve yaptırımlara bağlanabilir[232]. Benzer şekilde Anayasamıza göre, bu özgürlüklerin kullanılması milli güvenlik, kamu düzeni, kamu güvenliği, Cumhuriyetin temel nitelikleri ve Devletin ülkesi ve milleti ile bölünmez bütünlüğünün korunması, suçların önlenmesi, suçluların cezalandırılması, Devlet sırrı olarak usulünce belirtilmiş bilgilerin açıklanmaması, başkalarının şöhret veya haklarının, özel ve aile hayatlarının yahut kanunun öngördüğü meslek sırlarının korunması veya yargılama görevinin gereğine uygun olarak yerine getirilmesi amaçlarıyla sınırlanabilir. Diğer hak ve özgürlükler

---

[230] Gedik, **a.g.e.**, s. 36.
[231] Özbek, **a.g.m.**, s. 104.
[232] Olağanüstü hallerde hak ve özgürlüklerin askıya alınması Avrupa İnsan Hakları Sözleşmesinin 15. maddesinde, hakların kötüye kullanımının yasaklanması ise 17. maddesinde ayrıca düzenlenmiştir.

açısından olduğu gibi ifade özgürlüğü açısından da asıl olan özgürlük, istisna olan ise özgürlüğün sınırlandırılmasıdır[233]. Bu nedenle, ifade özgürlüğü açısından getirilen sınırlandırmalarda yapılacak yorumlarda özgürlüğün asıl, sınırlandırmanın istisna olduğu devamlı göz önünde bulundurulmak zorundadır.

İfade özgürlüğünün özel bir görünümü olarak bilim ve sanat özgürlüğünün sınırları ise ayrıca düzenlenmiştir. Anayasamızın 27. maddesine göre bilim ve sanatı yayma hakkı, Anayasanın 1, 2 ve 3. maddeleri hükümlerinin değiştirilmesini sağlamak amacıyla kullanılamaz.

Şu halde internet ortamında ifade özgürlüğü, Anayasanın ilgili maddelerinde öngörülen nedenlere bağlı olarak sınırlandırılabilir.

İfade özgürlüğünün sınırlandırılmasında *"açık ve mevcut tehlike"* kriterinin uygulanması gerektiği ileri sürülmektedir[234]. Bu kritere göre bir ifade açıklaması "açık ve mevcut bir tehlike" oluşturduğu noktada artık sınırlandırılmalıdır.

2. Özel Hayatın Gizliliğinin Sınırları

Avrupa İnsan Hakları Sözleşmesinin 8. maddesine göre özel ve aile hayatına saygı hakkının kullanılmasına bir kamu makamının müdahalesi, ancak ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için yapılabilir. Benzer şekilde Anayasamızın 20. maddesinin ikinci fıkrasına göre özel hayatın gizliliği; milli güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlakın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak sınırlandırılabilir. Maddede özel hayatın gizliliğinin sınırlandırılmasına ilişkin hususlar kişilerin üstünün, özel kağıtlarının ve eşyasının aranması ve bunlara el konulması olarak belirlenmiştir[235]. Bunun internet düzenlemesi ile ilgili bir boyutu

---

[233] Tunç / Bilir / Yavuz, **a.g.e.**, s. 112. Erdoğan, **a.g.e.**, s. 156.
[234] Erdoğan, **a.g.e.**, s. 222-223.
[235] Ketizmen, **a.g.e.**, s. 211.

bulunmamaktadır. İnternette, kişinin özel hayatının gizliliğinin sınırını diğer kişilerin bilgi edinme özgürlüğü ile kitle iletişim özgürlüğü oluşturmaktadır. Bu noktada özel hayatın gizliliği, bilgi edinme ve kitle iletişim özgürlüğü ile çatışmaktadır. Çatışmanın ortadan kaldırılması için yapılacak dengelemede bilgi edinme ve kitle iletişim özgürlüğünün ağır basması durumunda özel hayatın gizliliğinin ihal edildiğinden söz edilemeyecektir.

İnternette kişilerin özel hayatının gizliliğinin bir diğer sınırını kişisel verilerin işlenmesi oluşturmaktadır. Anayasamızın 20. maddesinin üçüncü fıkrasına göre kanunda öngörülen hallerde kişisel veriler işlenebilir. Şu halde, kanunun öngürmesi koşulu ile kişisel veriler işlenerek özel hayatın gizliliğine müdahale edilebilir.

Haberleşme özgürlüğü açısından konuyu ele aldığımızda ise Anayasamızın 22. maddesine göre milli güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlakın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya bir kaçına bağlı olarak haberleşme engellenebilir ve gizliliğine dokunulabilir.

E. Sınırlandırmanın Sınırları

İfade özgürlüğü ve özel hayatın gizliliğinin bazı durumlarda sınırlandırılabilmesi mümkün olmakla birlikte bu sınırlandırmaların bazı sıkı şartlar altında yapılması gerekir. Bu şartlar söz konusu özgürlükleri kişiler açısından güvence altına alan şartlardır.

1. İfade Özgürlüğünün Sınırlandırılmasının Sınırları

Avrupa İnsan Hakları Sözleşmesine göre ifade özgürlüğüne getirilecek sınırlandırmalar demokratik bir toplumda, zorunlu tedbirler niteliğinde, sözleşmede sayılan nedenlerden en az birine dayanarak ve yasayla öngörülen çerçevede olmak zorundadır. Benzer şekilde Anayasamızın "*Temel Hak ve Hürriyetlerin Sınırlanması"* başlıklı 13. maddesine göre, temel hak ve özgürlükler, özlerine dokunulmaksızın yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabilir. Bu sınırlamalar, Anayasanın sözüne ve ruhuna, demokratik toplum düzeninin

ve laik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamaz. Anayasanın 13. maddesinde yer alan söz konusu hüküm, hak ve özgürlüklerin tamamına şamildir[236]. Burada 13. madde, sadece ve kısaca ifade özgürlüğü açısından ele alınmıştır.

İfade özgürlüğü yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak sınırlandırılabilir. Milli güvenlik, kamu düzeni, kamu güvenliği, Cumhuriyetin temel nitelikleri ve Devletin ülkesi ve milleti ile bölünmez bütünlüğünün korunması, suçların önlenmesi, suçluların cezalandırılması, Devlet sırrı olarak usulünce belirtilmiş bilgilerin açıklanmaması, başkalarının şöhret veya haklarının, özel ve aile hayatlarının yahut kanunun öngördüğü meslek sırlarının korunması veya yargılama görevinin gereğine uygun olarak yerine getirilmesi Anayasanın 26. maddesinde sayılan sınırlandırma nedenleridir. Bu nedenler dışında kalan başka bir nedenden dolayı ifade özgürlüğünün sınırlandırılması mümkün değildir.

Hakkın özüne dokunulmazlık ilkesi gereği, ifade özgürlüğünün kullanılmasının tamamen ortadan kaldırılması mümkün değildir. Bu ilke, diğer özgürlüklerde olduğu gibi ifade özgürlüğünde de dokunulması insan onuru gereği mümkün olmayan çekirdek bir alan bulunduğunu kabul eder[237]. Her somut olayda, getirilen sınırlandırmanın hakkın özüne dokunup dokunmadığı araştırılacaktır.

Kanunilik ilkesi, Anayasamıza göre ifade özgürlüğüne getirilecek herhangi bir sınırlandırmanın mutlaka ilk elden kanun ile yapılmasını zorunlu kılar[238]. Buradaki kanun ibaresinin şekli anlamda kanun olduğu kabul edilmektedir. Bu durumda yasama organı tarafından yürürlüğe konulmuş bir kanun ile çerçevesi çizilmemiş bir konuda idarenin yürürlüğe koyacağı düzenleyici işlemlerle ifade özgürlüğüne müdahalede bulunması mümkün değildir. Bu durum idarenin yapacağı bireysel idari işlemler açısından da geçerlidir. AİHS'de yer alan kanunilik ilkesi ise maddi anlamda kanunilik

---

[236] Tunç / Bilir / Yavuz, **a.g.e.**, s. 113.
[237] Erdoğan, **a.g.e.**, s. 164.
[238] Özbudun, **a.g.e.**, s. 113.

olarak yorumlanmaktadır. AİHM, sadece yasama organı tarafından yürürlüğe konulan şekli anlamdaki kanunların değil, yürütme organı tarafından yürürlüğe konulan düzenleyici işlemlerin de maddi anlamda kanunilik koşulunu yerine getirebileceğini kabul etmektedir[239]. Hatta, AİHM'e göre yazılı hukuk kuralı niteliğinde olmayan içtihat hukuku, örf ve adet hukuku da maddi anlamda kanun koşulunu yerine getirebilir. AİHM'nin aradığı tek ölçüt yapılan düzenlemenin anlaşılabilir ve ulaşılabilir olmasıdır[240]. Anlaşılabilirlik, düzenlemenin yeteri derecede açıklık içermesini, ulaşılabilirlik ise düzenlemeye ilgili kişilerin kolayca erişebilmesini ifade etmektedir.

Demokratik toplum düzeninin gereklerine uygunluk, ifade özgürlüğüne getirilecek sınırlandırmaların demokratik bir toplumun gereklerine uygunluğunu ifade eder. Elbette demokratik toplum gerekleri her somut olayın özelliğine ve içerisinde bulunulan toplumun değerlerine göre şekillenecektir[241]. Ancak, demokratik bir toplumda bulunması zorunlu olan unsurlara aykırı bir sınırlandırmaya da gidilemeyecektir[242].

Ölçülülük ilkesi, ifade özgürlüğüne getirilecek herhangi bir sınırlandırmanın ulaşılmak istenen amacı gerçekleştirmeye uygun olmasını ifade eder. Bu ilke elverişlilik, oranlılık ve gereklilik unsurlarını içerir[243]. Elverişlilik ilkesi, hak ve özgürlüklerin sınırlandırılmasında getirilen aracın amacı gerçekleştirmeye elverişli olması anlamında kullanılmaktadır. Elverişliliğin bulunmaması durumunda getirilen sınırlandırmanın bu ilkeye aykırılık oluşturduğu kabul edilir. Oranlılık ilkesi, ulaşılmak istenen amaç ile araç arasında bir dengenin bulunmasını ifade eden ilkedir. Gereklilik ilkesi ise yapılan sınırlandırmanın gerekli olup olmadığını belirler. Daha az sınırlayıcı bir tedbir uygulanabilecekken daha ağır olan bir tedbirin uygulanması gereklilik ilkesine aykırı düşer[244].

---

[239] Erdoğan, **a.g.e.**, s. 158-159.
[240] Tezcan ve Diğerleri, **a.g.e.**, s. 287.
[241] Tezcan ve Diğerleri, **a.g.e.**, s. 450.
[242] Özbudun, **a.g.e.**, s. 115-116.
[243] Yücel Oğurlu, **Karşılaştırmalı İdare Hukukunda Ölçülülük İlkesi**, Seçkin Yayınları, Ankara, 2002, s. 36.
[244] Özbudun, **a.g.e.**, s. 114.

2. Özel Hayatın Gizliliğinin Sınırlandırmasının Sınırları

Avrupa İnsan Hakları Sözleşmesine göre özel ve aile hayatına saygı hakkına ilişkin sınırlandırmanın kanunla yapılması, 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 gerekmektedir. Anayasamız açısından ise 13. maddede yer alan temel hak ve özgürlüklerin sınırlandırılmasına ilişkin hüküm, özel hayatın gizliliği açısından da geçerlidir. Bu çerçevede özel hayatın gizliliğine getirilecek bir sınırlandırmanın bu hakkın özüne dokunmaksızın yalnızca Anayasanın söz konusu hak ve özgürlüğü düzenleyen 20. maddesinde belirtilen sebeplere bağlı olarak ve ancak kanunla yapılabileceği, Anayasanın sözüne ve ruhuna, demokratik toplum düzeninin ve laik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamayacağı şüphesizdir.

Bunun yanısıra, kişisel verilerin korunması açısından bazı sınırlar 20. maddenin son fıkrasında öngörülmüştür. Buna göre kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir.

Haberleşme özgürlüğü açısından ise sadece 22. maddede öngörülen sebeplere bağlı olarak usulüne göre verilmiş hakim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; haberleşme engellenemez ve gizliliğine dokunulamaz. Yetkili merciin kararı yirmidört saat içinde görevli hakimin onayına sunulur. Hakim, kararını kırksekiz saat içinde açıklar; aksi halde, karar kendiliğinden kalkar. İstisnaların uygulanacağı kamu kurum ve kuruluşları kanunda belirtilir.

IV. İDARENİN DÜZENLEME YETKİSİ ÇERÇEVESİNDE İNTERNETİN DÜZENLENMESİ

Bu bölüm altında öncelikle internetin düzenlenmesi konusunda yetkili kılınan düzenleyici kurumlar ele alınmış; devamında ise idarenin internet alanında düzenleyici işlem yapma yetkisi incelenmiştir.

A. Düzenleyici Kurumlar

İdari yapı içerisinde, etkinliği, yapısı, yetki alanının genişliği birbirinden farklılık göstermekle birlikte internet ile ilgili konularda yetkili kılınmış çeşitli kuruluşlar bulunmaktadır. Bu kuruluşlar internet içeriğinin düzenlenmesinde sorumluluk üstlenmektedir. Örneğin, İngiltere'de, internette çocukların cinsel istismarıyla mücadele etmek amacıyla kamu kurumları ile işbirliği içerisinde özel bir kuruluş olarak İnternet İzleme Kuruluşu (Internet Watch Foundation) kurulmuştur. Avusturalya'da yayın, internet, telekomünikasyon ve radyo iletişiminin düzenlenmesi konularında ulusal düzeyde sorumlu federal resmi bir kuruluş olarak Avustralya İletişim ve Medya Kurumu (The Australian Communications and Media Authority) [245]; İtalya'da Telekomünikasyon Kurumu (Agcom); Almanya'da internet ortamında küçüklere karşı zararlı içeriğin engellenmesi amacıyla Gençleri Medyada Yer Alan Zararlı İçerikten Koruma Birimi (Federal Department for Media Harmful to Young Persons (BPjM))[246] oluşturulmuştur. Bu kuruluşların sayısı artırılabilir.

Doğrudan internet içeriğinin düzenlenmesine ilişkin olmamakla birlikte internetle ilgili bazı alanların dolaylı bir şekilde düzenlenmesini sağlayan kuruluşlar da bulunmaktadır. Kişisel verilerin korunması, e-devlet hizmetlerinin yürütülmesi ve ulusal siber güvenliğin sağlanması gibi alanlar idari yapılanma şeklinde teşkilatlandırılmaktadır.

Kişisel verilerin korunması alanında veri koruma komiseri, veri koruma kurulu ve veri koruma kurumu gibi idari yapılar oluşturulmaktadır[247]. Bu yapılar genellikle bağımsız idari kuruluşlar olarak tasarlanmaktadır. Örneğin, İngiltere'de bağımsız bir kuruluş olarak Bilgi Komiseri Ofisi (The Information Commissioner's Office), bilgi edinme hakkı ve kişisel verilerin korunması

---

[245] http://www.acma.gov.au/WEB/STANDARD/pc=ACMA_ORG_OVIEW, 30.01.2013. ACMA'nın organizasyonel yapısı için bakınız: http://www.acma.gov.au/webwr/aca_home/about_aca/organisational_structure/acma_org_structure-1_aug_2012.pdf, 30.01.2013.

[246] http://bundespruefstelle.de/bpjm/information-in-english.html, 15.03.2013.

[247] Avrupa Konseyi üyesi devletlerin veri koruma kurumlarının listesi ve iletişim bilgileri için bkz. http://www.coe.int/t/dghl/standardsetting/DataProtection/Liste_autorites_fr.pdf, 29.01.2013.

konusunda görevli kılınmıştır[248]. Kişisel verilerin korunmasından Fransa'da bağımsız bir kuruluş olarak Bilişim ve Özgürlük Ulusal Komisyonu (National Commission for Informatics and Liberty)[249] sorumlu kılınmıştır. Almanya'da kişisel verilerin korunmasından Kişisel Verilerin Korunması ve Bilgi Edinme Hakkı Federal Komiseri (Federal Commissioner for Data Protection and Freedom of Information) sorumludur[250].

e-Devlet yapılanmaları birbirinden oldukça farklılık göstermekle birlikte genellikle bir bakanlık bünyesinde teşkilatlandırılmaktadır[251]. Örneğin, ABD'de e-devlet hizmetlerinin koordinasyonundan sorumlu bir kuruluş olarak e-Devlet ve Bilgi Teknolojileri Ofisi (Office of E-Government & Information Technology), Başkanlık Yönetim ve Bütçe Ofisi (Office of Management and Budget) bünyesinde oluşturulmuştur[252]. İngiltere'de Kabine Ofisi bünyesinde Bilişim Yöneticileri Kurulu (The Chief Information Officer Council), kamu sektöründe görevli IT yöneticilerin katılımı ile oluşturulmuş ve kamu sektöründe bilgi ve iletişim teknolojilerinin geliştirilmesine ilişkin koordinasyon görevini üstlenmiştir[253]. Teknik Bilişim Yöneticileri Kurulu (The Chief Technology Officers Council) ve Bilişim Yöneticileri Sunum Kurulu (The Chief Information Officers Delivery Board), kamu sektöründe bilgi ve iletişim teknolojilerinin kullanımı ve uygulanmasından sorumlu tutulmuştur. Almanya'da, e-Devlet politika ve stratejilerinin belirlenmesi ve koordinasyonun sağlanması açısından Federal İçişleri Bakanlığı, Bilgi Teknolojisi Federal Hükümet Komiseri Ofisi (The Office of the Federal Government Commissioner for Information Technology) ve IT Kurulu (IT Council) görevlendirilmiştir. Estonya Bilgi Sistemleri Kurumu (Estonian Information System's Authority) ise, Ekonomik İşler ve İletişim Bakanlığı bünyesinde bir alt birim olarak yapılandırılmıştır[254].

---

[248] http://www.ico.gov.uk/about_us.aspx, 29.01.2013.
[249] http://www.cnil.fr/english/the-cnil/status/, 29.01.2013.
[250] http://www.bfdi.bund.de/EN/Home/homepage_node.html, 29.01.2013.
[251] Türkiye Bilişim Derneği, **e-Devlet Üst Yapısı Nihai Rapor**, http://www.tbd.org.tr/usr_img/cd/kamubib14/raporlarPDF/RP1-2011.pdf, 29.01.2012.
[252] http://www.whitehouse.gov/omb/e-gov, 29.01.2012.
[253] http://www.cabinetoffice.gov.uk/resource-library/chief-information-officers-council, 29.01.2013.
[254] https://www.ria.ee/about-estonian-information-systems-authority/, 29.01.2013.

Siber güvenliği sağlayan kamu kuruluşlarına çoğu ülkede özel bir önem verilmekte ve bunlar ayrı bir teşkilat olarak düzenlenmektedir. Örneğin, Almanya'da Federal Bilgi Güvenliği Ofisi (Federal Office for Information Security), Alman hükümet kuruluşlarının merkezi olarak IT güvenliğini sağlayan bir kuruluştur[255].

Ülkemizde, internetin düzenlenmesi konusunda Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, bu Bakanlık bünyesinde oluşturulan İnternet Geliştirme Kurulu ve Bakanlık ilişkili kuruluşu olarak Bilgi ve Teknolojileri ve İletişim Kurumu (BTK)[256] yetkili kılınmıştır.

Bakanlık, ulaştırma ve denizcilik alanları yanında esasen genel olarak elektronik haberleşme sektörü, özelde ise internet alanına ilişkin konularda strateji ve politika belirleme yetkisi ile donatılmıştır[257]. Ayrıca, Bakanlık bünyesinde internet alanına ilişkin konularda çalışmalarda bulunmak, araştırma, inceleme ve değerlendirme yapmak üzere bakanlık, kurum ve kuruluş, sivil toplum kuruluşları temsilcileri ve konuyla ilgili uzmanların katılımıyla bir İnternet Geliştirme Kurulu oluşturulması öngörülmüştür[258]. İnternet Geliştirme Kuruluna, internet 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, Türk Kültürü, Türk Tarihi ve Türk Dünyasıyla ilgili bilgilerin internet ortamında daha fazla yer alması ve bunların tanıtılması hususunda çalışmalar yapmak, yaptırmak ve öneriler hazırlamak, internet ortamının güvenli, serbest, özgür ve faydalı kullanımı ile katma değer üretmesine yönelik öneriler hazırlamak

---

[255] https://www.bsi.bund.de/EN/Home/home_node.html, 29.01.2013.

[256] Kurumun adı, Telekomünikasyon Kurumu iken 10.11.2008 tarihli ve 5809 sayılı Elektronik Haberleşme Kanunu ile Bilgi Teknolojileri ve İletişim Kurumu olarak değiştirilmiştir.

[257] Bkz. 5809 sayılı Elektronik Haberleşme Kanunu, md. 5. Söz konusu Kanunun 35. maddesine göre "*İnternet alan adlarının tahsisini yapacak kurum veya kuruluşun tespiti ile alan adı yönetimine ilişkin usul ve esaslar Bakanlık tarafından belirlenir".*

[258] Bkz. 655 sayılı Ulaştırma, Denizcilik ve Haberleşme Bakanlığının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname, md. 29. 655 sayılı KHK ile daha önce adı İnternet Kurulu olan bu Kurulun adı, yapısı ve görevleri değiştirilmiştir. İnternet Kurulunun hukuksal dayanağını oluşturan 9/4/1987 tarihli ve 3348 sayılı Ulaştırma Bakanlığının Teşkilat ve Görevleri Hakkında Kanun yürürlükten kaldırılmıştır. Kurulun bir diğer hukuksal dayanağı olan 5651 sayılı Kanunun 10. maddesinin beşinci fıkrası ise açıkça yürürlükten kaldırılmamış olsa da söz konusu fıkrada atıf yapılan 3348 sayılı Ulaştırma Bakanlığının Teşkilat ve Görevleri Hakkında Kanun yürürlükten kaldırıldığı için bu fıkra da zımni olarak yürürlükten kaldırılmış olmaktadır.

görevleri verilmiştir[259]. Bu çerçevede, Kurulun alacağı kararlar Bakanlık strateji ve politikalarının oluşturulmasında tavsiye niteliğinde kararlar olacaktır.

BTK[260] ise genel olarak elektronik haberleşme sektörünün regülasyonunda yetkili iken[261] bu Kuruma bağlı olarak kurulan Telekomünikasyon İletişim Başkanlığı (TİB), telekomünikasyon yoluyla yapılan iletişimin tespiti, dinlenmesi, sinyal bilgilerinin değerlendirilmesi ve kayda alınmasına ilişkin görevleri yanında doğrudan internet alanı konusunda da yetkili kılınmıştır[262]. Ayrıca, bu başkanlık bünyesinde oluşturulan internet Dairesi Başkanlığının görev alanı sadece internet alanına hasredilmiştir.

Doktrinde bazı yazarlar, TİB'in oluşturulmasının yasal dayanaktan yoksun olduğunu ve bu kuruluşun bir yönetmelikle ile oluşturulmasının hukuken mümkün olmadığını ileri sürmüştür. Bizce, TİB'in kuruluşunun yasal dayanaklarına bakıldığında kuruluşun yasal dayanaktan yoksun olmadığı görülmektedir. TİB'in sahip olduğu görevler, 2559 sayılı Polis Vazife ve Salahiyet Kanununun[263] ek 7 nci maddesi, 2803 sayılı Jandarma Teşkilat, Görev ve Yetkileri Kanununun[264] ek 5 inci maddesi, 2937 sayılı Devlet

---

[259] Ayrıca, 5651 sayılı Kanunun 10. maddesinin beşinci fıkrasında 655 sayılı Ulaştırma, Denizcilik ve Haberleşme Bakanlığının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname ile yürürlükten kaldırılmış olan İnternet Kuruluna, izleme, filtreleme ve engelleme yapılacak içeriği haiz yayınların tespiti konusunda TİB'e önerilerde bulunma yetkisi verilmişti. Ulaştırma, Denizcilik ve Haberleşme Bakanlığının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname ile İnternet Kurulunun oluşumuna imkan tanıyan 3348 sayılı Ulaştırma Bakanlığının Teşkilat ve Görevleri Hakkında Kanun yürürlükten kaldırılmış olduğu için 5651 sayılı Kanunun anılan atfının bir anlamı da kalmamıştır.

[260] BTK'nın kuruluşu, 5809 sayılı Elektronik Haberleşme Kanununun 67. maddesi ile düzenlenmiştir. Söz konusu madde ile 2813 sayılı Telsiz Kanununda değişiklik yapılmış ve anılan Kanunun ismi Bilgi Teknolojileri ve İletişim Kurumunun Kuruluşuna İlişkin Kanun olarak değiştirilmiştir. Söz konusu Kanun ile, kanunlarla verilen görevleri yerine getirmek ve yetkileri kullanmak üzere kamu tüzel kişiliğini haiz, idari ve mali özerkliğe sahip Bilgi Teknolojileri ve İletişim Kurumu kurulmuştur. Kurum, görevlerini yerine getirirken bağımsızdır. Hiçbir organ, makam, merci veya kişi Kuruma emir ve talimat veremez. Kurum'un ilişkili olduğu bakanlık Ulaştırma, Denizcilik ve Haberleşme Bakanlığıdır. Bkz. http://www.mevzuat.gov.tr/Kanunlar.aspx, 16.10.2012.

[261] İçel / Ünver, **a.g.e.**, s. 442.

[262] Bkz. 5651 sayılı Kanun md. 10 ve 10.11.2005 tarihli ve 25989 sayılı Resmi Gazete'de yayımlanan Telekomünikasyon Yoluyla Yapılan İletişimin Tespiti, Dinlenmesi, Sinyal Bilgilerinin Değerlendirilmesi ve Kayda Alınmasına Dair Usul ve Esaslar İle Telekomünikasyon İletişim Başkanlığının Kuruluş, Görev ve Yetkileri Hakkında Yönetmelik.

[263] RG. 14.7.1934, 2751.

[264] RG. 12.3.1983, 17985.

İstihbarat Hizmetleri ve Millî İstihbarat Teşkilatı Kanununun[265] 6 ncı maddesi, 5271 sayılı CMK' nın[266] 135 ila 138 inci maddeleri ile 5651 sayılı Kanunun 10 uncu maddesinden kaynaklanmaktadır. Söz konusu kanunlarda sadece TİB'in görevleri düzenlenmemiş; aynı zamanda kuruluşuna ilişkin hükümlere de yer verilmiştir. Bu çerçevede, Polis Vazife ve Salahiyet Kanununun ek 7 nci maddesinde *"Bu maddede belirtilen telekomünikasyon yoluyla yapılan iletişime ilişkin işlemler ile 5271 sayılı Kanunun 135 inci maddesi kapsamında yapılacak dinlemeler, Telekomünikasyon Kurumu bünyesinde, Kurum başkanına doğrudan bağlı 'Telekomünikasyon İletişim Başkanlığı' adıyla kurulan tek bir merkezden yürütülür. Oluşturulan bu Başkanlık bir başkan ile daire başkanlıklarından oluşur. Bu Başkanlıkta Milli İstihbarat Teşkilatı, Emniyet Genel Müdürlüğü ve Jandarma Genel Komutanlığının ilgili birimlerinden birer temsilci bulundurulur"* hükmüne yer verilmiştir[267]. Anılan hükmün sonunda bu maddenin uygulanmasına ilişkin usul ve esasların Başbakanlık tarafından çıkarılacak yönetmelikle düzenlenmesi öngörülmüştür[268]. Bu hükümlere dayanılarak Başbakanlık tarafından, Telekomünikasyon Yoluyla Yapılan İletişimin Tespiti, Dinlenmesi, Sinyal Bilgilerinin Değerlendirilmesi ve Kayda Alınmasına Dair Usul ve Esaslar İle Telekomünikasyon İletişim Başkanlığının Kuruluş, Görev ve Yetkileri Hakkında Yönetmelik yürürlüğe konulmuştur. Anılan Yönetmelik ile telekomünikasyon yoluyla yapılan iletişimin tespiti, dinlenmesi, sinyal bilgilerinin değerlendirilmesi ve kayda alınmasına ilişkin usul ve esasların belirlenmesinin yanı sıra, TİB'in kuruluş, görev ve yetkileri de ayrıntılı bir şekilde düzenlenmiştir. Kuruluş açısından TİB'in, BTK bünyesinde doğrudan BTK Başkanına bağlı olarak faaliyet göstereceği ve Telekomünikasyon İletişim Başkanı ile Hukuk, Teknik İşletme, Bilgi Sistemleri, İdari ve internet

---

[265] RG. 3.11.1983, 18210.
[266] RG. 17.12.2004, 25673.
[267] Benzer hükümlere 2803 sayılı Jandarma Teşkilat, Görev ve Yetkileri Kanununun ek 5 inci maddesinde ve 2937 sayılı Devlet İstihbarat Hizmetleri ve Millî İstihbarat Teşkilatı Kanununun 6 ncı maddesinde de yer verilmiştir.
[268] Benzer bir düzenleme 5651 sayılı Kanunda da yer almıştır (md. 11/1). Hüküm şu şekildedir: *"Bu Kanunun uygulanmasına ilişkin esas ve usuller, Adalet, İçişleri ve Ulaştırma Bakanlıklarının görüşleri alınarak Başbakanlık tarafından çıkarılacak yönetmeliklerle düzenlenir. Bu yönetmelikler, Kanunun yürürlüğe girdiği tarihten itibaren dört ay içinde çıkarılır."*

Daire Başkanlıklarından oluşacağı öngörülmüştür (md. 16). Ayrıca, 5651 sayılı Kanunda Başkanlık, BTK bünyesinde bulunan Telekomünikasyon İletişim Başkanlığı olarak tanımlanmış ve 10. maddede Kanunla verilen görevlerin Kurum bünyesinde bulunan Başkanlıkça yerine getirileceği düzenlenmiştir.

Söz konusu kanun ve yönetmelik hükümleri bir bütün olarak ele alındığı zaman TİB'in bizzat; İnternet Dairesi Başkanlığının ise dolaylı bir şekilde (yönetmeliğe gönderme yapılarak) kanun tarafından kurulmuş olduğu ve yasal dayanak sorununun bulunmadığı söylenebilir.

TİB'in internet alanına ilişkin görevleri ana başlıklar halinde, 5651 sayılı Kanunda yer verilen suçların önlenmesine ilişkin çalışmalar yapmak, bu Kanunda yer verilen suçların işlendiğinin tespiti halinde suç oluşturan içeriğe erişimin engellenmesi için Kanun çerçevesinde gerekli tedbirleri almak, internet servis sağlayıcıların yetkilendirilmeleri ile ticari amaçlı toplu kullanım sağlayıcılara verilecek izin belgelerinde filtreleme ve bloke etmede kullanılacak sistemlere ve yapılacak düzenlemelere yönelik esas ve usulleri belirlemek, internet ortamında herkese açık çeşitli servislerde yapılacak filtreleme, perdeleme ve izleme esaslarına göre donanım üretilmesi veya yazılım yapılmasına ilişkin asgari kriterleri belirlemek, izleme, filtreleme ve engelleme yapılacak içeriği haiz yayınları tespit etmek, hakim, mahkeme veya Cumhuriyet savcısı tarafından verilen erişimin engellenmesi kararlarını uygulamak, Kanun çerçevesinde re'sen erişimi engelleme kararı almak şeklinde sıralanabilir[269]. Başkanlığın söz konusu görevlerine ilişkin ayrıntılı açıklamalar aşağıda ilgili yerlerde yapılmıştır.

İnternetin düzenlenmesi konusunda öngörülen bu kuruluşlar yanında internetin çeşitli alanlarına ilişkin başka bazı kuruluşlar da öngörülmüştür. 641 sayılı Kalkınma Bakanlığının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname ile bilgi toplumuna ilişkin politika, hedef ve stratejileri hazırlamak, bu alanda kamu kurum ve kuruluşları, sivil toplum örgütleri ve

[269] 5651 sayılı Kanun, md. 10 ve Telekomünikasyon Yoluyla Yapılan İletişimin Tespiti, Dinlenmesi, Sinyal Bilgilerinin Değerlendirilmesi ve Kayda Alınmasına Dair Usul ve Esaslar İle Telekomünikasyon İletişim Başkanlığının Kuruluş, Görev ve Yetkileri Hakkında Yönetmelik, md. 17.

özel sektör arasındaki koordinasyonu sağlamak ve uygulamayı etkin bir biçimde yönlendirmek görevi Kalkınma Bakanlığına verilmiştir. Bu görevleri yürütmek üzere Kalkınma Bakanlığı bünyesinde Bilgi Toplumu Dairesi Başkanlığı kurulmuştur[270]. Yine, Bakanlar Kurulunun 11.6.2012 tarihli ve 2012/3842 sayılı Kararı ile Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar yürürlüğe konulmuş[271] ve bu karar ile Siber Güvenlik Kurulu oluşturulmuştur. Siber Güvenlik Kurulu, esas olarak siber güvenlikle ilgili alınacak önlemleri belirlemek, hazırlanan strateji ve planları onaylamak ve bunların uygulanmasını ve koordinasyonunu sağlamakla görevli kılınmıştır. Nihayet, en son 2012 yılında Adalet Bakanlığı tarafından Başbakanlığa gönderilen taslakta Adalet Bakanlığı ile ilişkili bir kuruluş olarak Kişisel Verileri Koruma Kurumunun oluşturulması öngörülmüştür[272].

B. İnternet ve İdarenin Düzenleyici İşlemleri

İnternete ilişkin hususların idarenin düzenleyici işlemleri ile düzenlenmesi yaygın bir uygulamadır. Bu düzenlemenin şartları ve usulünün incelenmesi, internet düzenlemesinin daha iyi anlaşılması açısından faydalı olacaktır.

1. İdarenin Düzenleme Yetkisi

İdarenin düzenleme yetkisi, Anayasa ve kanunlar çerçevesinde idarenin genel, kişilik dışı ve soyut nitelikte düzenlemeler yapabilme yetkisi olarak tanımlanabilir[273]. Türk hukuk sisteminde idare, düzenleme yetkisini ancak kanun çerçevesinde kullanabilmektedir. Kanun ile düzenlenmemiş bir alanda idarenin doğrudan düzenleme yapması mümkün değildir[274]

---

[270] RG. 08.06.2011, 27958 Mük.
[271] RG. 20.10.2012, 28447.
[272] http://www.memurlar.net/haber/309117/, 31.01.2013.
[273] Bahtiyar Akyılmaz, Murat Sezginer, Cemil Kaya, **Türk İdare Hukuku**, 2. Güncellenmiş Baskı, Seçkin Yayınları, Ankara, 2011, s. 68. Metin Günday, **İdare Hukuku**, İmaj Yayıncılık, Ankara, 2011, s. 193.
[274] Celal Erkut, **İptal Davasının Konusunu Oluşturma Bakımından İdari İşlemin Kimliği**, Danıştay Yayınları, Ankara, 1990, s. 69. Öztürk, **a.g.e.**, s. 143.

(*secundum legem*). Anayasa'da yer alan tüzük ve yönetmelik hükümleri ile idarenin hangi çerçevede düzenleme yetkisine sahip olduğunun çerçevesi çizilmiştir. Anayasamızın 115. maddesine göre, Bakanlar Kurulu, kanunun uygulanmasını göstermek veya emrettiği işleri belirtmek üzere, kanunlara aykırı olmamak ve Danıştayın incelemesinden geçirilmek şartıyla tüzükler çıkarabilir. Tüzükler, Cumhurbaşkanınca imzalanır ve kanunlar gibi yayımlanır. Anayasamızın 124. maddesine göre ise Başbakanlık, bakanlıklar ve kamu tüzelkişileri, kendi görev alanlarını ilgilendiren kanunların ve tüzüklerin uygulanmasını sağlamak üzere ve bunlara aykırı olmamak şartıyla, yönetmelikler çıkarabilir. Hangi yönetmeliklerin Resmi Gazetede yayımlanacağı kanunda belirtilir. Ayrıca, tüzük ve yönetmelikler dışında idarenin takdir yetkisini diğer alt düzenleyici işlemlerle kullanması da mümkündür.

2. İnternet Alanının Düzenleyici İşlemlerle Düzenlenmesi

Ülkemizde internetin düzenlenmesini çeşitli yönleriyle amaçlayan birçok yönetmelik yürürlüğe konulmuştur. Bunlardan bazılarının burada ele alınması faydalı olacaktır.

5651 sayılı Kanuna göre, bu Kanunun uygulanmasına ilişkin esas ve usuller, Adalet, İçişleri ve Ulaştırma Bakanlıklarının görüşleri alınarak Başbakanlık tarafından çıkarılacak yönetmeliklerle düzenlenir (md. 11/1). 5651 sayılı Kanunun uygulanmasına ilişkin hususlarda Ulaştırma, Denizcilik ve Haberleşme Bakanlığı doğrudan yetkili kılınmamış, internet alanının gerektirdiği işbirliği ve koordinasyonun gerektiği gibi karşılanabilmesi için bu Bakanlık ile birlikte Adalet ve İçişleri Bakanlıklarının görüşlerinin alınması ve yönetmeliklerin Başbakanlık tarafından yürürlüğe konulması öngörülmüştür. Bu çerçevede, Başbakanlık tarafından "*İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik*"[275] ile

[275] RG. 30.11.2007, 26716.

"*İnternet Toplu Kullanım Sağlayıcıları Hakkında Yönetmelik*"[276] Resmi Gazete'de yayımlanmıştır.

Benzer şekilde, 5397 sayılı Kanunla[277] üzerinde değişiklik yapılan 2559 sayılı Polis Vazife ve Selahiyet Kanunu (Ek madde 7), 2803 sayılı Jandarma Teşkilat, Görev ve Yetkileri Kanunu (Ek madde 5) ve 2937 sayılı Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanununun (md. 6) Başbakanlığa verdiği yetki çerçevesinde "*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*"[278] Başbakanlık tarafından yürürlüğe konulmuştur. Yine, 5809 sayılı Elektronik Haberleşme Kanununda, BTK'nın, elektronik haberleşme sektörüyle ilgili kişisel verilerin işlenmesi ve gizliliğinin korunmasına yönelik usul ve esasları belirlemeye yetkili olduğu düzenlenmiş (md. 51) ve bu çerçevede Telekomünikasyon Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğin Korunması Hakkında Yönetmelik[279] yayımlanmıştır.

Söz konusu yönetmelikler bazı açılardan doktrinde eleştiri konusu olmuştur. Doktrinde bir görüş, internet alanına ilişkin düzenlemelerin, özellikle erişimin engellenmesine ilişkin düzenlemelerin, Anayasamızın 13. maddesi çerçevesinde yer alan kanunilik ilkesi gereği idarenin düzenleyici işlemlerine hiçbir şekilde konu yapılamayacağını ileri sürmektedir[280]. Bu görüşe, kanunla düzenlenmemiş bir alanda idarenin doğrudan bir düzenleyici işlem yürürlüğe koyması noktasında tam olarak katılmaktayız. Ancak, öncelikle kanunla düzenlenmiş bir alanda kanunun uygulanmasını sağlamak veya emrettiği işleri belirtmek ve bir üst hukuk normuna aykırı olmamak üzere idarenin düzenleyici işlem yapma yetkisinin de göz ardı edilmesi söz konusu

[276] RG. 1.11.2007, 26687.
[277] Bkz. 03.07.2005 tarihli ve 5397 sayılı Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun (2559, 2803, 2937 sayılı Kanunlara İlişkin), Md. 1, 2 ve 3. RG. 23.07.2005, 25884.
[278] RG. 10.11.2005, 25989.
[279] RG. 24.07.2012, 28363.
[280] Özen / Baştürk, **a.g.e.**, s. 72.

olamaz[281]. Elbette temel hak ve özgürlüklere müdahale niteliğinde olan internet düzenlemesine ilişkin hususlar Anayasamızın 13. maddesi gereği ancak kanun konusu olabilir. Anayasamızda yer alan bu hükümle, kişiler temel hak ve özgürlükler açısından idarenin keyfi uygulamalarına karşı güvence altına alınmaya çalışılmıştır. Ancak bu hüküm, bu alanın hiçbir şekilde düzenleyici işlemlerce düzenlenemeyeceği şeklinde yorumlanamaz.

Bir diğer eleştiri, Telekomünikasyon Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğin Korunması Hakkında Yönetmelik açısındandır. Bu Yönetmelik, haberleşme özgürlüğü bağlamında kişisel verilerin korunmasına ilişkin yeterli güvencelerin öncelikle kanun ile düzenlenmesi gerektiği gerekçesiyle eleştirilmektedir. Söz konusu Yönetmelik ile haberleşme sektöründe kişisel verilerin işlenmesi düzenlenmiştir; ancak bu Yönetmeliğin dayanağını oluşturan kanun hükmü kişisel verilerin işlenmesine ilişkin genel bir çerçeve çizmemiş ve yeterli hukuksal güvenceler sağlamamıştır. Bizce de kanunun bu yaklaşımı eleştirilebilir. Söz konusu güvenceler kanun ile sağlandıktan sonra bu kanunun uygulanmasına yönelik hususlar yönetmelikle düzenlenebilir[282]. Ancak, Elektronik Haberleşme Kanunu ile aksi yönde bir yaklaşım izlenmiş ve yeterli hukuksal güvenceler sağlanmadan doğrudan yönetmeliğe gönderme yapılmıştır. Bizce bu yaklaşım söz konusu Kanun hükmünü Anayasamızın 13. maddesinde yer alan "*kanunla sınırlama ilkesine"* aykırı hale getirmektedir.

Bu doğrultuda bir kararında Anayasa Mahkemesi, TİB tarafından yapılan iletişimin tespitine ilişkin hususların ilgili kamu kurum ve kuruluşlarınca ayrı ayrı denetiminde "*Başbakanın özel olarak yetkilendireceği kişi veya komisyonun"* da yetkili kılınmasına ilişkin 5397 sayılı Kanunda[283] yer alan hükümleri iptal etmiştir[284]. Bu Kararda Anayasa Mahkemesi iletişimin tespitini, "*Anayasa'nın kişinin dokunulmazlığı, maddi ve manevi varlığını koruma hakkına ilişkin 17., özel hayatın gizliliğinin korunmasına ilişkin 20.,*

[281] Öztürk, **a.g.e.**, s. 137. Onur Karahanoğulları, **İdarenin Hukukla Kavranması: Yasallık ve İdari İşlemler**, Turhan Kitabevi, Ankara, 2011, s. 64.
[282] Bkz. Öztürk, **a.g.e.**, s. 144.
[283] Bkz. 03.07.2005 tarihli ve 5397 sayılı Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun (2559, 2803, 2937 sayılı Kanunlara İlişkin), Md. 1, 2 ve 3. RG. 23.07.2005, 25884.
[284] AYM, 29.01.2009, E. 2005/85, K. 2009/15.

haberleşme hürriyetine ilişkin 22., düşünceyi açıklama ve yayma hürriyetine ilişkin 26. maddeleri gibi bir çok temel hak ve hürriyetle ilgisi olan" bir faaliyet olarak nitelendirmiş ve anılan kanun hükümlerini, Başbakanın özel olarak yetkilendireceği kişi veya komisyon üyelerinin nitelikleri açıkça belirlenmediği gerekçesiyle Anayasanın 128. maddesine aykırı bularak iptal etmiştir.

Bir diğer eleştiri açısından 5651 sayılı Kanunda, yer veya erişim sağlayıcı olarak faaliyet icra etmek isteyen kişilere, telekomünikasyon yoluyla iletişim konusunda yetkilendirme belgesi olup olmadığına bakılmaksızın, yer veya erişim sağlayıcı olarak faaliyet icra etmesi amacıyla yetkilendirme belgesi verilmesine ilişkin esas ve usullerin, BTK tarafından çıkarılacak yönetmelikle düzenleneceği öngörülmüştür (md. 11/2). Bu çerçevede, BTK tarafından "*Telekomünikasyon Kurumu Tarafından Erişim Sağlayıcılara ve Yer Sağlayıcılara Faaliyet Belgesi Verilmesine İlişkin Usul ve Esaslar Hakkında Yönetmelik"* yürürlüğe konulmuştur[285]. Bu Yönetmeliğin 8. maddesinde başvuru sahibinde bulunması gereken şartlar belirlenirken, erişim sağlayıcısı faaliyet belgesi için başvuru yapacak sermaye şirketi olan tüzel kişilerin hisselerinden en az yüzde beşine sahip ortakların ve tüzel kişiliği idare ve temsile yetkili kişilerin, 3713 sayılı Terörle Mücadele Kanununda belirtilen suçlar ile 5237 sayılı TCK'da yer alan Millete ve Devlete karşı işlenen suçlardan hürriyeti bağlayıcı ceza ile hüküm giymiş olmaması şartı aranmaktadır. Doktrinde bazı yazarlar, söz konusu düzenlemenin Anayasamızın 13. maddesinde yer alan kanunilik ilkesine aykırılık oluşturduğunu ve hukuki temelinin olmadığını ileri sürmektedir[286]. Bizce, yönetmelikte yer alan söz konusu düzenlemenin hukuki temeli 5651 sayılı Kanunun 11. maddesinin ikinci fıkrasıdır[287]. Bu fıkra, BTK'ya söz konusu düzenlemeyi yapma yetkisi vermektedir. Bu nedenle BTK'nın yürürlüğe

---

[285] RG. 24.10.2007, 26680.

[286] Akdeniz / Altıparmak, **a.g.e.**, s. 36.

[287] 5651 sayılı Kanunun 11. maddesinin ikinci fıkrası şu şekildedir: *"(2) Yer veya erişim sağlayıcı olarak faaliyet icra etmek isteyen kişilere, telekomünikasyon yoluyla iletişim konusunda yetkilendirme belgesi olup olmadığına bakılmaksızın, yer veya erişim sağlayıcı olarak faaliyet icra etmesi amacıyla yetkilendirme belgesi verilmesine ilişkin esas ve usûller, Kurum tarafından çıkarılacak yönetmelikle düzenlenir. Bu yönetmelik, Kanunun yürürlüğe girdiği tarihten itibaren beş ay içinde çıkarılır".*

koyduğu Telekomünikasyon Kurumu Tarafından Erişim Sağlayıcılara ve Yer Sağlayıcılara Faaliyet Belgesi Verilmesine İlişkin Usul ve Esaslar Hakkında Yönetmeliğin anılan hükmünün 5651 sayılı Kanuna aykırılığından bahsedilemez. Ancak, 5651 sayılı Kanunda yer alan hükmün Anayasaya aykırılık oluşturup oluşturmadığı ayrı bir konudur. Bu noktada, hak ve özgürlükleri ilgilendiren her konunun Anayasamızın 13. maddesi gereği her yönüyle ancak kanun ile düzenlenebileceğini söylemek mümkün değildir. Kanunla genel çerçevesi çizilmiş ve hak ve özgürlükler açısından yeterli güvence sağlanmış konuların uygulanmasına yönelik hususlar elbette yönetmelikle düzenlenebilir. Bu noktada, Kanunun söz konusu hükmünün genel bir çerçeve çizip çizmediği ve kişiler açısından yeterli bir güvence oluşturup oluşturmadığına bakmak gerekir. Yer veya erişim sağlayıcı olarak faaliyet icra edilmesini sınırlandıran bir düzenleme, çalışma özgürlüğünü engelleyeceğinden aslında doğrudan kanun konusu yapılması gerekirdi. Bu nedenle anılan Kanun hükmünün Anayasaya aykırılığından söz edilebilir.

Nihayet, bir diğer eleştiri konusu idarenin muhakeme usulüne ilişkin alanlarda düzenleyici işlem yapmasına ilişkin hususdur. İdare, yürürlüğe koyduğu bazı yönetmelikler ile muhakemeye ilişkin alanlarda yönetmelik yürürlüğe koyabilmektedir. Örneğin, CMK, bu Kanunun uygulanmasına ilişkin bazı alanlarda idarenin yönetmelik çıkarabileceğine ilişkin hükümler içermektedir. Ancak, bu tür hükümlerin olmadığı durumlarda da idare, düzenleyici işlemlerle muhakeme alanına ilişkin hususlarda düzenleme yapabilmektedir. Ceza Muhakemesi Kanununda Öngörülen Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi, Gizli Soruşturmacı ve Teknik Araçlarla İzleme Tedbirlerinin Uygulanmasına İlişkin Yönetmeliğin[288] bazı hükümlerinin iptali istemiyle açılan davada Danıştay İdari Dava Daireleri Kurulu, *"Bu nedenle, genel anlamda, mahkemelerin yargılama faaliyeti içinde yer alan usul konusunun, idari alanın dışında kaldığının ve münhasıran yasa konusu olduğunun kabulü gerekmektedir. Yargılama usulü içinde düzenlenen bir konunun idari alan sayılabilmesi için*

[288] RG. 14.02.2007, 26434.

ise, bu konuların neler olduğunun ve sınırlarının Yasa koyucu tarafından açıkça gösterilmesi zorunludur. Yasa koyucunun düzenleme yapma yetkisi vermediği hususların da idarece düzenlenebileceğinin kabulü, yargı yetkisinin idare tarafından kullanılması anlamına gelir ki, bu durumun diğer bir ifadesi 'fonksiyon gaspı'dır" sonucuna varmıştır[289].

Danıştay aynı kararında, 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 açısından ise yerinde bir yaklaşım olarak, *"Diğer taraftan, 2559 sayılı Polis Vazife ve Selahiyet Yasası'nın ek 7. maddesinde ise, gerek bu maddede belirtilen telekomünikasyon yoluyla yapılan iletişime ilişkin işlemlerin, gerek Ceza Muhakemesi Yasası kapsamında yapılacak "dinlemeler"in Telekomünikasyon Kurumu bünyesinde "Telekomünikasyon İletişim Başkanlığı" adıyla kurulan tek bir merkezden yapılması esası benimsenmiş; aynı maddenin son fıkrasında, bu maddenin uygulanmasına ilişkin esas ve usullerin ise Adalet, İçişleri ve Ulaştırma bakanlıklarının görüşü alınarak Başbakanlık tarafından çıkarılacak yönetmelikle düzenleneceği belirtilmiş; bu doğrultuda, hazırlanan "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", 10.11.2005 günlü, 25989 sayılı Resmi Gazete'de yayımlanmıştır. Anılan Yönetmelikle yapılacak düzenlemenin, Ceza Muhakemesi Yasası çerçevesinden yürütülecek yargılama faaliyeti ilgili olmayıp, anılan Yasanın 135 ila 140. maddelerine göre verilecek kararların kamu kurum ve kuruluşları ile adli kolluk görevlilerince yerine getirilmesine yönelik usul ve esaslarla ilgili olması gerektiğinde de kuşku bulunmamaktadır"* değerlendirmesini de yapmıştır.

---

[289] DİDDK, 4.11.2010, E. 2010/2072, K. 2010/1467, http://www.danistay.gov.tr/e2010_2072.htm, 01.02.2013.

ÜÇÜNCÜ BÖLÜM
DÜZENLEME ALANLARI

Bugün ülkelerin tamamında internet içeriği; kapsamı, yoğunluğu, demokratikliği, etkinliği, hukukiliği, düzenleme araçları ve meşruluğu ülkeden ülkeye değişmekle birlikte şu veya bu şekilde düzenlenmektedir. Düzenleme öngörülen alanlar ise oldukça geniş bir yelpaze oluşturmaktadır. Ulusal güvenlik, özel hayatın gizliliği, hakaret, telif hakları, tüketici haklarının korunması, bilişim suçları, nefret söylemi, çocuk pornografisi ile mücadele, e-ticaret, e-imza, e-sözleşme gibi alanlar devletlerin düzenleme yaptığı başlıca alanlardır. Bunun dışında siyasi kontrol gibi nedenlerle de düzenleme öngörülebilmektedir. Ancak bu konu burada incelenmemiştir. Ayrıca, özel hukuk açısından internetin düzenlenmesi ile ilgili olan e-ticaret, e-sözleşme, tüketici haklarının korunması ve telif hakları gibi konular da bu çalışmada incelenmemiştir.

Bu bölümde bilişim suçlarıyla mücadele, internet ortamında kişisel verilerin korunması, önleme amaçlı internet iletişiminin denetlenmesi ve ulusal siber güvenliğin sağlanması konuları incelenmiştir.

I. BİLİŞİM SUÇLARIYLA MÜCADELE

Bilişim suçlarıyla mücadele için devletler çeşitli düzenlemeler yapmakta; sınır ötesi bilişim suçlarıyla mücadele için de uluslararası işbirliği ve uluslararası hukukun geliştirdiği imkanları kullanmaya çalışmaktadır.

Bilişim suçlarının kapsamı oldukça geniştir. Birçok suç, bilişim ortamında işlenmeye müsait bir yapıdadır. Bu çalışmada bilişim ortamda işlenebilen her suç açısından değil; ancak, belki de bilişim ortamında en çok karşılaşılan suçlar açısından bir değerlendirme yapılmıştır. Ayrıca, çalışma alanımız sadece bilişim suçları olarak belirlenmediği ve konunun kapsamının genişliği itibariyle her suç türü açısından suçun unsurları ayrı ayrı belirlenerek bir değerlendirme yapılmamış; bunun yerine, devletin bilişim suçları ile nasıl mücadele ettiği suç politikası açısından ele alınmıştır. Bir diğer deyişle, bu

bölümde devletin bilişim suçlarının düzenlenmesine ilişkin genel yaklaşımı incelenmiştir.

A. Tanımı

Bilişim sistemlerinin gelişimi, bazı yeni suç tipleri ortaya çıkarmış veya var olan suçların işlenmesini kolaylaştırmış ve suç oranlarını artırmıştır. Ortaya çıkan yeni suç tipleri, hukuka aykırı olarak bilişim sistemine girme, sistemin işleyişini engelleme veya bozma, sistemde yer alan verilere zarar verme veya hukuka aykırı olarak ele geçirme şeklinde doğrudan bilişim sistemini hedef alan suçlar olarak kendisini göstermiştir. Irkçılık, çocuk pornografisi, yabancı düşmanlığı, telif haklarının korunmasına ilişkin suçlar, sanal kumar, hakaret, terör suçları, müstehcenlik, uyuşturucu ticareti, dolandırıcılık gibi suçlar ise bilişim sistemlerinin gelişimi ile birlikte bilişim sistemleri aracılığıyla yaygın bir şekilde işlenmeye başlamıştır. Bu suçlar, bilişim sistemleri ile işlenebileceği gibi başka araçlarla da işlenebilir ve bilişim sistemlerinin gelişmediği zamanlarda da bu suçlar işlenebiliyordu[290]. İnternetin gelişimi ile birlikte anılan suçların yaygın bir şekilde internet aracılığıyla işlenmesi ise interneti söz konusu suçlar ile anılır hale getirmiştir. Ceza hukuku açısından bilişim sistemleri ve internetin gelişiminin ortaya çıkardığı bu tablo, genel olarak bilişim alanında işlenen suçları ifade etmek üzere *"bilgisayar suçu"*, *"bilişim suçu"*, *"siber suç"*, *"internet suçu"* gibi farklı kavramlarla açıklanmaya başlanmıştır. Kavramların bu şekilde farklı kullanımı hem doktrinde hem de uygulamada kendisini göstermiş ve ceza kanunlarında da farklı kavramlar kullanılabilmiştir. Bu çerçevede, bilgisayar suçu ile bilişim suçu birbirinden ayrılabilir ve bilişim suçu kavramı, bilgisayar suçu kavramını da kapsayan ancak, ondan daha geniş bir çerçeveye oturtulabilir. Çünkü, bilgisayar ile bilişim kavramı birbirinin aynı değildir ve bilgisayar dışında bilişim sistemleri de bulunmaktadır. Yine, siber suç kavramının siber ortamda işlenen suçları ifade ettiği ve siber ortamın interneti de kapsayan, ancak ondan daha geniş bir çerçevede bilginin elektronik ortamda dolaştığı her

[290] Özbek, **a.g.m.**, s. 107-108.

ortam anlamında kullanılabileceği belirtilebilir. Bu bağlamda, internet de bir siber ortam olarak değerlendirilebilir ve internet suçu kavramı, siber suç kavramı içinde mütalaa edilebilir. İnternet suçu kavramını, internet ortamında işlenebilen her türlü suç olarak nitelendirip[291], bilişim sistemlerine karşı işlenen suçları ise bilişim suçu olarak nitelendirmek de mümkündür. Nihayet, bilişim alanında işlenen suçlar internet açısından ele alınıp internet suçları, internet aracılığıyla işlenen suçlar ve internete özgü suçlar şeklinde bir ayırıma da tabi tutulabilir[292]. Farklı kavramları kullanarak bilişim alanında işlenen suçları tanımlama çabası bir tarafa bırakılarak bilişim suçu kavramı açısından konuya yaklaşıp, bilişim suçları da dar anlamda bilişim suçları ve geniş anlamda bilişim suçları olarak bir ayrıma da tabi tutulabilir. Bilişim sistemlerine karşı işlenen suçlar dar anlamda bilişim suçu, bilişim sistemleri aracılığıyla işlenen suçlar ise geniş anlamda bilişim suçları olarak ele alınabilir. Bu anlamda, internet aracılığıyla işlenen suçlar geniş anlamda bilişim suçu kavramının kapsamına girmektedir. Hatta bazı yazarlar geniş anlamda bilişim suçlarını gerçek anlamda bilişim suçu kabul etmemektedir[293]. Bu sınıflandırma ve tanımlamaların sayısı artırılabilir[294]. Bu tartışmalara daha derinlemesine girmeksizin bu çalışmada, bilişim suçları kavramı kullanılmış ve bu suçlar, dar ve geniş anlamda bilişim suçları ayrımı esas alınarak incelenmiştir[295]. İnternet aracılığıyla işlenebilen suçlar, geniş anlamda bilişim suçu kapsamında değerlendirilmiştir.

B. Genel Olarak Ceza Kanunlarında Bilişim Suçu

Ülkelerin bilişim suçlarını düzenleyen hukuk kurallarına bakıldığında esas olarak iki farklı temel yöntemin tercih edildiği görülmektedir. Bu yöntemlerden ilki, bilişim suçlarının ceza kanunları içerisinde düzenlenmesi,

---

[291] Özbek, **a.g.m.**, s. 106-107.
[292] Sevil Yıldız, **Suçta Araç Olarak İnternetin Teknik ve Hukuki Yönden İncelenmesi**, Nobel Yayın Dağıtım, Ankara, 2007, s. 38.
[293] Ketizmen, **a.g.e.**, s. 38-39.
[294] Uçkan / Beceni, **a.g.m.**, s. 389-394.
[295] Bilişim sistemlerine karşı suçlar ve bilişim sistemleri aracılığıyla işlenen suçlar ayrımı, suçun maddi konusu ve suçta kullanılan araç esas alınarak yapılan bir sınıflandırmadır. Bu sınıflandırma suçun hukuki konusunu esas almamakta, bu nedenle bilişim alanında farklı hukuki konu içeren suçların aynı kategoride değerlendirilmesi sonucunu doğurmaktadır. Ketizmen, **a.g.e.**, s. 38.

diğeri ise ayrı kanunlar ile düzenlenmesine ilişkin yaklaşımdır[296]. Bu iki yöntemi birleştiren ülke sistemleri de bulunmaktadır. Özel kanun uygulamasına ilişkin olarak ABD'de, Bilgisayarlarla İlgili Dolandırıcılık ve Bununla Bağlantılı Faaliyetler Hakkında Kanun (Fraud and Related Activity in Connection with Computers)[297] ve İngiltere'de Bilgisayarın Kötüye Kullanımı Kanunu (Computer Misuse Act 1990) örnek olarak verilebilir. Ceza kanunları içerisinde dar anlamda bilişim suçlarının düzenlenmesine ilişkin bir yaklaşım olarak ise Fransız, Alman ve Türk ceza kanunları örnek olarak gösterilebilir.

Dar anlamda bilişim suçlarına bazı ceza kanunlarında toplu halde bir bölüm altında yer verilmiştir. Örneğin, bu suçlar Fransız Ceza Kanununda "*otomatik veri işleme sistemlerine yetkisiz erişim"* bölümünde toplu halde düzenlenmiştir (md. 323 vd.)[298]. Bilişim suçlarına ayrı bir bölüm altında toplu olarak yer vermek yerine, ilgili suçun hukuki konusuna göre bölümler içerisinde dağınık bir şekilde de yer verilebilmektedir[299]. Örneğin, Alman Ceza Kanununda özel hayatın gizliliğinin ihlali bölümünde, veri casusluğu (data espionage), elektronik dolandırıcılık (phishing), veri casusluğu ve dolandırıcılığına ilişkin hazırlık hareketleri (acts preparatory to data espionage and phishing) suçları öngörülmüş (md. 202a, 202b, 202c); bilgisayar dolandırıcılığı (computer fraud) suçu, dolandırıcılık ve zimmet (fraud and embezzlement) bölümünde ayrı bir suç olarak (md. 263a) ele alınmış[300]; verinin değiştirilmesi ve bilgisayar sabotajı suçları ise malvarlığı aleyhine işlenen suçlar bölümünde düzenlenmiştir (md. 303a, 303b).

Türk hukukunda dar anlamda bilişim suçlarını ayrıca özel olarak düzenleyen bir kanun bulunmamaktadır. Bilişim suçları genel olarak TCK içerisinde; Kanunun ikinci kitabının topluma karşı suçlar başlıklı üçüncü kısmının onuncu bölümünde *"bilişim alanında suçlar"* başlığı ile düzenlenmiştir (md. 243-246)[301]. Bunun yanında, TCK'da yer alan birçok

---

[296] Yıldız, **a.g.e.**, s. 111.
[297] Ketizmen, **a.g.e.**, s. 71.
[298] http://legislationline.org/documents/section/criminal-codes, 14.02.2013.
[299] Ketizmen, **a.g.e.**, s. 59, 61.
[300] http://legislationline.org/documents/section/criminal-codes, 14.02.2013.
[301] Bilişim alanında suçlar, 765 sayılı Türk Ceza Kanununa 1991 yılında söz konusu Kanunda yapılan bir değişiklikle girmiştir.

suçun bilişim sistemi ve özellikle internet aracılığıyla işlenmesi mümkündür. Ayrıca, Kanunun bazı hükümlerinde tanımlanan suçların bilişim sistemleri ile işlenmesi söz konusu suçun nitelikli hali olarak öngörülmüştür. Örneğin, dolandırıcılık suçunun; bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle işlenmesi bu suçun nitelikli hallerinden biridir (md. 158/1, f). Nihayet, Kanunun tanımlar başlıklı 6. maddesinde "basın ve yayın yolu ile" deyimi, "*her türlü yazılı, görsel, işitsel ve elektronik kitle iletişim aracıyla yapılan yayın"* olarak, interneti de kapsamına alacak şekilde tanımlanmış ve bazı suç tanımlamalarında söz konusu suçların basın ve yayın yolu ile işlenmesi daha ağır ceza gerektiren bir hal olarak öngörülmüştür.

Türk hukuk sisteminde bilişim suçlarının özel olarak ayrı bir kanunla düzenlenmesine ilişkin bir çalışma da yapılmış; ancak öngörülen sonuç alınamamıştır. Adalet Bakanlığı tarafından 2006 yılında hazırlanan "*Bilişim Ağı Hizmetlerinin Düzenlenmesi ve Bilişim Suçları Hakkında Kanun Tasarısının"*[302] amacı; içerik sağlayıcı, yer sağlayıcı, erişim sağlayıcı, bilişim ağı hizmet sağlayıcı ve toplu kullanım olanağı sağlayıcılarının sorumlulukları ile bilişim sistemi veya bilişim ağı kullanılarak işlenen suçları, bu suçların soruşturulması ve kovuşturulmasına ilişkin esas ve usulleri düzenlemek olarak belirlenmiştir. Bu Tasarı ile öngörülen suç tipleri şunlardır: Bilgilerin gizliliği, bütünlüğü ve elde edilmesine ilişkin suçlar (bilişim sistemine girme ve veri elde etme, hukuka aykırı izleme, veriler veya programların bütünlüğüne müdahale, sistemin çalışmasına müdahale, araçları kötü amaçla kullanma), bilişim sistemi bağlantılı suçlar (bilişim sistemini kullanarak sahtecilik, bilişim ortamında yarar sağlamak, yanıltarak bilgi toplamak, taklit yoluyla yanıltmak), içerik bağlantılı suçlar (çocuk pornografisi bağlantılı suçlar, Devletin güvenliğine ve kamu barışına karşı işlenen suçlar, tehdit, şantaj, hakaret veya iftira suçları, kişisel veriler ile ilgili suçlar, kumar ve kararın yerine getirilmemesi). Bilişim Ağı Hizmetlerinin Düzenlenmesi ve Bilişim Suçları Hakkında Kanun Tasarısı, internetin yanısıra elektronik ortamın tamamını

[302] Bkz: http://www.turkhukuksitesi.com/showthread.php?t=6203, 19.12.2012.

kapsamına almıştı. Bu çerçevede, mobil ve sabit telefon, fax, telsiz, telgraf, radyo ve televizyon, söz konusu Kanun kapsamına girmekteydi. Anılan Tasarı yerine kanunlaşan 5651 sayılı Kanunda ise kural olarak yeni bilişim suçu tipi öngörülmemiştir. Anılan Kanunda "*internet ortamında yapılan yayınlar yoluyla işlenen suçlar"* kavramı kullanılmış ve 8. maddede sayılan suçlarla mücadele etmenin bir yöntemi olarak, internet içeriğine erişimin engellenmesi müessesesi düzenlenmiştir.

C. Avrupa Konseyi Siber Suç Sözleşmesi

Her devletin imzasına açık olan Avrupa Konseyi Siber Suç Sözleşmesi 2001 yılında imzaya açılmış ve 2004 yılında yürürlüğe girmiştir. Sözleşme, toplumun siber suçlara karşı korunması için ulusal düzeyde yeterli yasal düzenlemelerin yapılması ve uluslararası işbirliğinin teşvik edilmesi amacını taşımaktadır. Böylece, uluslararası düzeyde siber suçlara karşı ortak bir suç politikası gerçekleştirilebilecektir. Siber Suç Sözleşmesinin giriş bölümünde, siber suçlara karşı ortak bir cezai politikanın oluşturulması için ulusal hukuk kurallarının oluşturulması ve uluslararası işbirliğinin geliştirilmesinin önemi üzerinde durulmuş; siber suçlara karşı etkili bir mücadele için cezai konularda hızlı ve iyi işleyen uluslararası işbirliğinin gerekliliğinden bahsedilmiştir. Sözleşmeyi, 35 tane Avrupa Komisyonu üyesi devlet onaylamıştır. Avrupa Komisyonu üyesi olan devletlerden Andorra, Monako, Rusya ve San Marino Sözleşmeyi henüz imzalamamış; Çek Cumhuriyeti, Yunanistan, İrlanda, Liechtenstein, Lüksemburg, Polonya, İsveç ve Türkiye[303] ise imzalamış ancak henüz onaylamamıştır. Ayrıca Sözleşmeyi, Avrupa Komisyonu üyesi olmayan 3 tane daha devlet onaylamıştır. Bunlar, Avustralya, Japonya ve ABD'dir. Kanada ve Güney Afrika ise Sözleşmeyi imzalamış, ancak henüz onaylamamıştır[304]. Bilişim suçlarının yoğun bir şekilde üretildiği Rusya, Çin ve Kore gibi devletlerin Sözleşmeyi imzalamamış olması bilişim suçları ile uluslarası alanda mücadeleyi olumsuz etkilemektedir.

---

[303] Türkiye, 10.11.2010 tarihinde Sözleşmeyi imzalamasına rağmen henüz onaylamamıştır.
[304] http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG, 31.12.2012.

Sözleşme 4 kısımdan oluşmaktadır. Birinci kısımda terimlerin kullanımı, ikinci kısımda ulusal düzeyde alınacak önlemler, üçüncü kısımda uluslararası işbirliği, dördüncü kısımda ise son hükümler düzenlenmiştir. İkinci kısım maddi ceza hukuku, usul hukuku ve yargı yetkisi (jurisdiction) olmak üzere üç bölümden oluşmuştur. Maddi ceza hukuku bölümünde, bilgisayar veri ve sistemlerinin gizlilik, bütünlük ve ulaşılabilirliğine karşı suçlar (kanuna aykırı erişim, kanuna aykırı müdahale, veriye müdahale, sisteme müdahale, araçların kötüye kulanımı), bilgisayar ile ilgili suçlar (bilgisayar ile ilgili sahtekarlık, bilgisayar ile ilgili dolandırıcılık), içerikle ilgili suçlar (çocuk pornografisi ile ilgili suçlar), telif hakları ve ilgili hakların ihlaline ilişkin suçlar (telif hakları ve ilgili hakların ihlaline ilişkin suçlar), sorumluluk ve yaptırımlar (teşebbüs, yardım veya teşvik etme, birleşik sorumluluk, yaptırım ve önlemler) hakkında hükümlere yer verilmiştir. Usul hukuku bölümünde ise genel hükümler (usul hükümlerinin kapsamı, şartlar ve güvenceler), saklanan bilgisayar verisinin korunmasının kolaylaştırılması (saklanan bilgisayar verisinin korunmasının kolaylaştırılması, trafik verilerinin korunmasının kolaylaştırılması ve kısmen açıklanması), üretim emri (üretim emri), saklanan bilgisayar verisinin araştırılması ve el konulması (saklanan bilgisayar verisinin araştırılması ve el konulması), bilgisayar verisinin gerçek zamanlı toplanması (trafik verisinin gerçek zamanlı toplanması, içerik verisine müdahale) ve yargı yetkisi hakkında hükümler yer almaktadır. Sözleşmenin uluslararası işbirliği kısmı ise genel ilkeler ve özel hükümler başlıklı iki bölümden oluşmaktadır. Genel ilkeler bölümünde uluslararası işbirliğine ilişkin genel hükümler, suçluların iadesi, karşılıklı yardımlaşmaya ilişkin genel ilkeler, uygulanabilir uluslararası anlaşmaların yokluğunda karşılıklı yardımlaşma taleplerine ilişkin usuller; özel hükümler bölümünde ise geçici önlemlere ilişkin karşılıklı yardımlaşma, soruşturma yetkileri konusunda karşılıklı yardımlaşma ve 24/7 Ağ hakkında hükümler yer almıştır.

Siber Suç Sözleşmesinde siber suç kavramı kullanılmış; ancak tanımlanmamıştır. Ancak, "*bilgisayar sistemi*" ve "*bilgisayar verisi*" kavramlarının tanımının yapılması ile Sözleşme kapsamında öngörülen suçların çerçevesi çizilmiştir. Sözleşmeye göre bilgisayar sistemi, bir veya

birden fazlası bir program dahilinde otomatik olarak veri işleyen herhangi bir cihaz veya birbirine bağlı veya birbiri ile ilişkili bir grup cihaz olarak; bilgisayar verisi ise bir bilgisayar sisteminin belli bir işlevi yerine getirmesini sağlayan yazılımlar da dahil olmak üzere bir bilgisayar sistemi içerisinde işlenmeye uygun formdaki olaylar, bilgi veya konseptlerin herhangi bir şekilde temsili olarak tanımlanmıştır. Böylece, Siber Suç Sözleşmesinde siber suç yaklaşımı çok geniş bir çerçeveye oturtulmuştur. Siber Suç Sözleşmesi, sadece internet suçlarını değil; genel olarak bilgisayar suçlarını kapsamına almıştır.

Siber Suç Sözleşmesi bazı özellikler taşımaktadır. Sözleşmede yer alan suçların taraf devletlerin iç hukukunda uygulanmasının zorunlu olması, sözleşmede yer alan tüm suçların kasıtlı olarak işlenebilmesi, internet içeriğine erişimin engellenmesi ve filtreleme gibi konuların Sözleşme kapsamında düzenlenmemesi bu özelliklerden bazılarıdır. Ayrıca, Sözleşmeye ek olarak Bilgisayar Sistemleri ile İşlenen Irkçılık ve Yabancı Düşmanlığının Cezalandırılması Hakkında Siber Suç Sözleşmesine Ek Protokol[305] yürürlüğe konulmuştur. Protokol ile, bilgisayar sistemleri aracılığıyla ırkçılık ve yabancı düşmanlığına ilişkin suçların işlenmesinin önlenmesi amaçlanmıştır.

Siber Suç Sözleşmesi ve Ek Protokol hükümlerinden aşağıda yeri geldikçe bahsedilecektir.

Ç. Geniş Anlamda Bilişim Suçları

Aslında geniş anlamda bilişim suçu kategorisinde ele alınabilecek suçlar, bilişim sistemlerine (daha spesifik olarak internete) özgü suçlar değildir. Bu suçlar bilişim sistemlerinin gelişimi ile birlikte ortaya çıkmamıştır. Bu suçların başka araçlarla da işlenmesi gayet mümkündür[306]. Bu nedenle aslında bilişim sistemi aracılığıyla işlenebilen suçların böyle bir başlık altında ele alınması çok mantıklı görülmeyebilir. Bu suçlar özgünlüğünü bilişim sistemi aracılığıyla işlenmiş olmalarından almamaktadır. Örneğin,

[305] Additional Protocol to the Convention on Cybercrime, Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems, http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm, 13.02.2013.
[306] Yıldız, **a.g.e.**, s. 73.

dolandırıcılık suçuna özgünlüğü veren bu suçun bilişim sistemi aracılığıyla da işlenebiliyor olması değildir. Bu suçun özgünlüğü, hileli davranışlarla bir kimsenin aldatılıp, aldatılan veya başkasının zararına olarak, aldatana veya başkasına bir yarar sağlanmasıdır. Bilişim sistemi aracılığıyla işlenebilen diğer suçları da düşündüğümüz zaman geniş anlamda bilişim suçu sınıflandırmasının çok da anlamlı olmadığı söylenebilir. Ancak, özellikle internetin gelişimi klasik anlamda bazı suçların işlenişini oldukça kolaylaştırmış ve suç oranlarını ciddi derecede artırmıştır. Bu olumsuz gelişim, devletleri acilen tedbir almaya yönlendirmiştir. Bu tedbirlerden birisi de ceza hukuku kurallarının devreye sokulmasıdır. Bir diğer deyişle, bilişim sistemi aracılığıyla işlenebilen söz konusu fiillerin cezai yaptırım altına alınarak bu fiillerle mücadelede etkin bir ceza politikası geliştirilmesidir. Bu noktada burada geniş anlamda bilişim suçları başlığı altında, bu kavram içerisine giren her suç tek tek ele alınıp incelenmeyecektir. Aksine, internet ile işlenmesi kolaylaşan ve artan suçlara karşı devletin öngördüğü yeni ceza politikasına ve düzenlemelerine ilişkin yaklaşımlar ortaya konulmaya çalışılacaktır. Örneğin, terör propagandası internet ortamı dışında başka şekillerde de gerçekleştirilebilir. İnternet ortamında olsun veya başka şekillerde gerçekleşsin her halde terör propagandası suçtur. Ancak, internetin gelişimi ile birlikte internet ortamında terör propagandasının da artmış olması nedeniyle devlet, internet ortamında terör propagandasını önlemek amacıyla, sadece bu alana özgü olmak üzere ne tür bir ceza politikası öngörmektedir? Bunun yansıması ceza kanunlarında kendisini nasıl göstermektedir?

Devletin bazı suç türleri açısından yeni cezai düzenlemeler öngörme hususunda sessiz kaldığı söylenebilir. Bunun birçok nedeni olabilir. Örneğin, hakaret suçu açısından internet ortamına özgü bir düzenleme yapmak çok anlamlı olmayabilir. Elbette, internetin gelişimi hakaret suçunun işlenmesini kolaylaştırmış ve artırmıştır. Ancak mevcut düzenlemeler, internet ortamında işlenen hakaret suçuna gerekli karşılığı vermekte yeterli görülebilir. Ayrıca, hakaret suçu açısından internet ortamına özgü bir düzenleme yapmak ulusal güvenlik, gençliğin korunması veya kamu düzeninin sağlanması nedenlerinde olduğu gibi devlet açısından acil bir neden de oluşturmayabilir.

Bazı durumlarda ise bilişim sistemine özgü bir düzenleme yapmanın pratik bir faydası bulunmayabilir. Örneğin, TCK'nın 135. maddesinde düzenlenen kişisel verilerin kaydedilmesi suçu hem bilişim sisteminde hem de yazılı ortamda kişisel verilerin kaydedilmesini kapsamaktadır. Bu düzenleme yapılırken bilişim sistemine özgü olarak hukuka aykırı bir şekilde kişisel verilerin işlenmesinin suç olarak öngörülmesinin pratik bir faydası görülmemiştir. Yasa koyucunun yaklaşımı farklı bir yönde de olabilirdi. Örneğin, kişisel verilerin bilişim sistemi kullanılarak hukuka aykırı bir şekilde işlenmesi söz konusu suçun ağırlaştırıcı bir nedeni olarak düzenlenebilirdi. Ancak, yasa koyucunun takdiri farklı yönde olmuştur. Benzer şekilde uyuşturucu ile mücadele açısından mevcut düzenlemeler gereken ihtiyacı karşılayabilir. TCK'nın 190. maddesinde "*uyuşturucu veya uyarıcı madde kullanılmasını kolaylaştırma"* suçu düzenlenmiştir. Bu madde, internet açısından da önem taşımaktadır. Maddeye göre uyuşturucu veya uyarıcı madde kullanılmasını kolaylaştırmak için kullanma yöntemleri konusunda başkalarına bilgi verme veya söz konusu maddelerin kullanılmasını alenen özendirme veya bu nitelikte yayın yapma filleri suç olarak düzenlenmiştir. Bu fiiller internet ortamında da işlenebilecek fiillerdir. Ancak, suçun bu şekline özgünlüğünü veren uyuşturucu veya uyarıcı madde kullanılmasını alenen özendirme veya bu nitelikte yayın yapma fiilleridir. Bunun hangi araç kullanılarak yapıldığı çok önem taşımamaktadır.

Bazı suç türleri açısından ise internet veya bilişim ortamına özgü düzenleme yapmak kendisini bir zorunluluk olarak hissettirebilir. Bunun da birçok nedeni olabilir. Bazı suçlar açısından özel düzenleme yapmanın söz konusu suçla mücadelede daha etkin bir yöntem olması bu nedenlerin en önemlisidir. Özel düzenleme yapılan suçların başında çocuk pornografisi ile mücadele amacıyla öngörülen suçlar gelmektedir. Avrupa Konseyi Siber Suç Sözleşmesi bu yaklaşımın başını çekmektedir. Sözleşmenin "*çocuk pornografisi ile ilgili suçlar"* başlıklı 9. maddesine göre, taraflardan her biri kasıtlı olarak işlenen aşağıdaki fiillerin cezai bir suç olarak ulusal hukuklarında yer almasına ilişkin yasal ve diğer önlemleri alacaktır.

a. Bir bilgisayar sistemi aracılığıyla ve dağıtmak amacıyla çocuk pornografisi üretmek.

b. Bir bilgisayar sistemi aracılığıyla çocuk pornografisi sunmak veya ulaşılabilir kılmak.

c. Bir bilgisayar sistemi aracılığıyla çocuk pornografisi dağıtmak veya iletmek.

d. Kendisi veya başka birisi için bir bilgisayar sistemini kullanarak çocuk pornografisi temin etmek.

e. Bir bilgisayar sistemi içinde veya bilgisayar verisi depolamaya yarayan cihazlarda çocuk pornografisi bulundurmak.

Bu çerçevede çocuk pornografisi kavramı, aşağıdakileri görsel olarak ortaya koyan pornografik materyali kapsar:

a. Bir küçüğün cinsel olarak açık bir şekilde gösterilmesi.

b. Küçük birisi olarak görünen bir kişinin cinsel olarak açık bir şekilde gösterilmesi.

c. Bir küçüğün cinsel olarak açık bir şekilde bulunmasını simgeleyen gerçekçi görüntüler.

Maddede küçük kavramının, 18 yaşın altındaki kişileri ifade ettiği belirtilmiştir. Bununla birlikte taraf devletler bu yaşın altında bir yaş belirleyebileceklerdir. Ancak, bu yaş 16 yaşından daha aşağı bir yaş olamaz. Maddenin son fıkrasında ise taraf devletlerin, tamamen veya kısmen birinci fıkranın (d) ve (e) bendi ile ikinci fıkranın (b) ve (c) bendini uygulamama hakkını saklı tutabileceği öngörülmüştür[307].

Alman Ceza Kanununun 184. maddesinde her ne şekilde olursa olsun çocuk pornografisinin üretimi, dağıtımı, erişim sağlanması, teşhir edilmesi, bulundurulması, kabul edilmesi ve indirilmesi cezai yaptırım altına alınmıştır[308]. Gençliği Koruma Kanunu (Youth Protection Law) ve Medyada Gençliğin Korunmasına İlişkin Sözleşme (the State Treaty on Youth

[307] Sözleşmenin bu son fıkrasını anlamak mümkün gözükmemektedir. Bu düzenleme ile sanki çocuk pornografisini temin eden ve depolayan kişiler ile küçük gibi görünen kişilere ya da küçüklere ilişkin gerçekmiş gibi görünen görüntülere ilişkin pornografi aklanmıştır. Bizce, Sözleşmede yer alan bu hüküm çocuk haklarını ihlal etmektedir.

[308] http://www.iuscomp.org/gla/statutes/StGB.htm, 15.03.2013.

Protection in the Media) ile gençliğin internet ortamında yer alan yayınlara karşı korunmasına yönelik ayrıntılı düzenlemelere yer verilmiştir.

Türk hukuk sisteminde ise Anayasamızın 41. maddesine 2010 yılında, *"Devlet, her türlü istismara ve şiddete karşı çocukları koruyucu tedbirleri alır"* hükmü eklenmiştir[309]. Bu hükmün gereği olarak çocuk pornografisi ile mücadele etmek devlete bir yükümlülük olarak yüklenmiştir[310]. Öte yandan, ülkemizde çocuk pornografisinin önlenmesine ilişkin temel düzenleme TCK'nın "*müstehcenlik"* başlıklı 226. maddesidir[311]. Ancak, bu madde sadece çocuk pornografisini[312] suç olarak öngören bir madde değildir. Maddede, çocuk pornografisi yanında müstehcenlik oluşturabilecek başka fiiller de suç olarak öngörülmüştür. Bir başka deyişle söz konusu madde, sırf çocuk pornografisinin suç olarak öngörülmesi amacıyla ele alınmamış; ancak çocuk pornografisi suçunu da kapsamına almıştır. Maddede çocuk pornografisi suçu, fiziksel ve sanal ortamı kapsayacak şekilde düzenlenmiştir. 226. maddenin üçüncü fıkrasına göre, *"Müstehcen görüntü, yazı veya sözleri içeren ürünlerin üretiminde çocukları kullanan kişi beş yıldan on yıla kadar hapis ve beşbin güne kadar adli para cezası ile cezalandırılır. Bu ürünleri ülkeye sokan, çoğaltan, satışa arz eden, satan, nakleden, depolayan, ihraç eden, bulunduran ya da başkalarının kullanımına sunan kişi, iki yıldan beş yıla kadar hapis ve beşbin güne kadar adli para cezası ile cezalandırılır."* Aynı maddenin beşinci fıkrasına göre ise söz konusu ürünlerin *"içeriğini basın ve yayın yolu ile yayınlayan veya yayınlanmasına aracılık eden ya da*

---

[309] RG. 13.05.2010, 27580.

[310] Gerçi bu hüküm öncesinde de anılan maddede yer alan diğer hükümler aynı yükümlülüğü öngörmekteydi. *"Ailenin korunması ve çocuk hakları"* başlıklı Anayasamızın 41. maddesinin son hali şu şekildedir:

"Madde 41 – *Aile, Türk toplumunun temelidir ve eşler arasında eşitliğe dayanır.*
Devlet, ailenin huzur ve refahı ile özellikle ananın ve çocukların korunması ve aile planlamasının öğretimi ile uygulanmasını sağlamak için gerekli tedbirleri alır, teşkilatı kurar.
Her çocuk, korunma ve bakımdan yararlanma, yüksek yararına açıkça aykırı olmadıkça, ana ve babasıyla kişisel ve doğrudan ilişki kurma ve sürdürme hakkına sahiptir.
Devlet, her türlü istismara ve şiddete karşı çocukları koruyucu tedbirleri alır."

[311] TCK'nın 103. maddesinde yer alan *çocukların cinsel istismarı* suçu, çocuk pornografisi ile ilgili bir suç değildir. Ancak, bu suçu barındıran internet içeriği bir erişimi engelleme nedenidir.

[312] Anılan maddede *çocuk pornografisi* isimli bir suç bulunmamaktadır. Suçun genel adı *müstehcenlik* suçudur; ancak içeriği doktrinde çocuk pornografisi olarak tanımlanan suçu da kapsamaktadır. Burada yaptığımız *çocuk pornografisi* suçu isimlendirmesi, bu çerçevede doktrinde yapılan tanımlamayı ifade etmektedir.

çocukların görmesini, dinlemesini veya okumasını sağlayan kişi, altı yıldan on yıla kadar hapis ve beşbin güne kadar adli para cezası ile cezalandırılır"[313]*.* Maddenin son fıkrası ile bu kurallara bir tane istisna getirilmiştir. Bu istisna, bilimsel eserler hakkında bu hükmün uygulanmayacağına yönelik bir istisnadır. Diğer taraftan böyle bir istisna getirilirken, sanatsal ve edebi değeri olan eserler açısından bu istisnanın uygulanmayacağı da açıklığa kavuşturulmuştur.

İnternet üzerinden çocuk pornografisi yayını yapan, bu içeriği başkalarına gönderen veya indiren kişiler, TCK'nın 226. maddesine göre bu suçu işlemiş olacaktır.

Özel cezai düzenleme gerektiren alanlardan birisi de internetin getirmiş olduğu zararlı içeriğe karşı çocukların korunmasına ilişkin düzenlemelerdir. Örneğin, Amerika Birleşik Devletlerinde, internette pornografi ile mücadelede ilk önemli hukuksal düzenleme[314] olan "*İletişim Ahlak Kanunu" (Communications Decency Act),* 1996 yılında yürürlüğe konulmuştur[315]. Bu Kanun ile 18 yaş altında bulunan kişilerin ulaşımına imkan sağlayan uygunsuz iletişim yasaklanmış[316] ve cezai yaptırım altına alınmıştır[317]. Kanun, yürürlüğe girmesi ile birlikte ciddi eleştiriler almaya başlamıştır. Eleştirilerden biri de uygunsuz içeriğin ne olduğu konusundaki belirsizlik olmuştur[318]. Bunun üzerine, kanuna karşı Birinci Değişikliğe (First Amendment) aykırılık oluşturduğu gerekçesiyle dava açılmıştır (*ACLU v. Reno).* Amerika Birleşik Devletleri Yüksek Mahkemesi (the United States Supreme Court), 1997 yılında söz konusu kanunu içerdiği belirsizlik

---

[313] TCK'da "*basın ve yayın yolu"* kavramı, her türlü yazılı, görsel, işitsel ve elektronik kitle iletişim aracıyla yapılan yayın olarak tanımlanmıştır. Bu çerçevede internet, bir basın ve yayın yolu aracıdır.
[314] http://en.wikipedia.org/wiki/Communications_Decency_Act, 11.10.2012.
[315] İçel / Ünver, **a.g.e.**, s. 7.
[316] Goldsmith / Wu, **a.g.e.**, s. 19.
[317] İlgili hüküm şu şekildedir (md. 223): *Kasten, çağdaş toplum standartlarına göre açıkça mütecavüz kabul edilen cinsel içerikli faaliyetleri tanımlayan herhangi bir yorum, talep, öneri, teklif, görüntü veya diğer herhangi bir şeyi 18 yaşın altındaki belirli bir kişiye veya kişilere göndermek için bir interaktif bilgisayar hizmetini kullanan veya 18 yaşın altındaki bir kişinin ulaşabileceği şekilde ifşa etmek için bir interaktif bilgisayar hizmetini kullanan kişi… cezalandırılır.*
[318] R. S. Rosenberg, "Controlling Access to the Internet: The Role of Filtering", **Ethics and Information Technology** 3 (1), 2001, s. 43.

nedeniyle Anayasaya aykırı bulmuştur[319]. Nihayet, bunun üzerine Çocukları İnternetten Koruma Kanunu (Children's Internet Protection Act (CIPA) of 2000) yürürlüğe konulmuş ve Birinci Değişikliğe aykırılığı iddiası reddedilmiştir. Bu Kanun, okul ve kütüphanelerde yer alan bilgisayarların kullanımında çocukların müstehcen (obscene) veya zararlı (harmful) içeriğe erişiminin engellenebilmesi için filtrelemeyi zorunlu kılmaktadır[320].

Alman Ceza Kanununun 184. maddesine göre ise 18 yaşının altındaki kişilere pornografik içeriği sunan, veren veya erişim sağlayan kişiler cezalandırılır[321]. Pornografik içerikli internet sitelerinin, sıkı bir şekilde küçüklerin erişimini engellemek amacıyla kimlik doğrulama sistemi kurmaları zorunlu kılınmaktadır.

Sanal kumarla (web gambling) mücadele de özel cezai düzenleme gerektirebilmektedir. İnternet ortamında kumar oynanması oldukça kolaylaşmış ve ciddi sorunlar doğurur hale gelmiştir. Kumarla mücadeleye ilişkin mevcut düzenlemeler, internet ortamında kumarla mücadele açısından yetersiz kalabilmektedir. Bu nedenle çoğu devlet, internet ortamında oynanan kumarla mücadele amacıyla özel cezai düzenleme öngörmektedir. Türk hukukunda kumar oynanması için yer ve imkan sağlama fiili, internet veya bilişim ortamına özgü bir düzenleme olmaksızın her türlü araçla işlenebilmesini kapsamına alacak bir şekilde cezai yaptırım altına alınmıştır. TCK'nın 228. maddesine göre kumar oynanması için yer ve imkan sağlayan kişi cezalandırılır. Bu suçun internet ortamında da işlenmesi mümkündür. Kumar oynanması için internette imkan sağlayan kişi bu suçun faili konumundadır. Bu genel düzenleye rağmen, 7258 sayılı Futbol ve Diğer Spor Müsabakalarında Bahis ve Şans Oyunları Düzenlenmesi Hakkında Kanun ile internet ortamına özgü suçlar öngörülmüştür. Anılan Kanunun 5. maddesine göre, *"Kanunun verdiği yetkiye dayalı olmaksızın, spor müsabakaları ile ilişkili olarak sabit ihtimalli veya müşterek bahis oynatanlar, oynanmasına yer veya imkân sağlayanlar, bir yıldan üç yıla kadar hapis ve onbin güne kadar adlî*

[319] Henn, **a.g.m.**, s. 167. Rosenberg, **a.g.m.**, s. 43
[320] http://www.fcc.gov/guides/childrens-internet-protection-act, 11.10.2012.
[321] http://www.iuscomp.org/gla/statutes/StGB.htm, 15.03.2013.

para cezasıyla cezalandırılır. Yurt dışında oynatılan her çeşit bahis veya şans oyunlarının internet yoluyla ve sair suretle erişim sağlayarak Türkiye'den oynanmasına imkân sağlayan kişiler, iki yıldan beş yıla kadar hapis cezasıyla cezalandırılır…"

Özel cezai düzenleme gerektiren bir diğer alan nefret suçlarına (hate crime) ilişkindir. İnternetin gelişimi ile birlikte nefret suçlarının işlenişinde önemli derecede artış gerçekleşmiştir. Örneğin, Youtube'da Türkiye ile ilgili Türkçe veya İngilizce yüklenmiş videolara yapılan yorumların, ilgili veya ilgisiz neredeyse tamamında PKK'lı teröristler ya da sempatizanları tarafından Türklüğe karşı nefret içerikli yazılar (hate speech) yazılmaktadır. Bu durum internet ortamında sadece Türlüğe karşı değil, başka milletler açısından da geçerlidir.

İnternette ırkçılıkla mücadele konusunda en duyarlı ve etkili sisteme sahip olan devletler, Avrupa devletleridir. Avrupa, ırkçılık ve yabancı düşmanlığı konusunda oldukça kötü tecrübeler yaşamıştır. Bu tecrübelerin bir kez daha yaşanmaması amacıyla ırkçılık ve yabancı düşmanlığının önlenmesi amacıyla etkili cezai düzenlemeler yapılmaya çalışılmaktadır. Bu alanda internet ortamına özgü olmak üzere ilk uluslararası sözleşme Bilgisayar Sistemleri ile İşlenen Irkçılık ve Yabancı Düşmanlığının Cezalandırılması Hakkında Siber Suç Sözleşmesine Ek Protokoldür[322]. Ek Protokol ile, bilgisayar sistemleri ile ırkçılık veya yabancı düşmanlığı yapılmasının cezalandırılması öngörülmüştür. Protokolde ırk, renk, soy, ulusal veya etnik köken veya dine dayalı olarak herhangi bir kişi veya gruba karşı nefret, ayrımcılık veya şiddeti savunan, destekleyen veya teşvik eden yazılı herhangi bir materyal, herhangi bir şekil veya düşünce veya teorilerin diğer bir şekilde ortaya konulması "*ırkçı ve yabancı düşmanlığı içeren materyal"* olarak tanımlanmıştır.

[322] Additional Protocol to the Convention on Cybercrime, Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems, http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm, 13.02.2013.

İnternette özel düzenleme gerektiren bu alanlar yanında özellikle fikri mülkiyet haklarının ihlali, müstehcenlik, dolandırıcılık ve hakaret gibi fiillerin önlenmesine yönelik özel cezai düzenlemeler de yürürlüğe konulabilmektedir.

D. Bilişim Alanında Suçlar

Bilişim alanında suçlar, dar anlamda bilişim suçları olarak tanımlanabilir. Bilişim sistemine girme, sistemi engelleme, bozma, verileri yok etme veya değiştirme, bilişim sistemlerinin kullanarak haksız yarar sağlama gibi fiiller dar anlamda bilişim suçu tanımlamasına girmektedir.

Bilişim suçu oluşturan fiiler çok çeşitli şekillerde gerçekleştirilebilmektedir. Virus, solucan, bukalemun, tavşanlar (rabbits), Truva atı, DOS (Denial of Service) veya DDoS (Distributed Denial of Service) saldırıları, spoofing, spam, mantık bombaları (logic bombs) dar anlamda bilişim suçlarının işlenmesinde başvurular yöntemlerden bazılarıdır[323].

1. Bilişim Sistemine Girme

TCK'nın bilişim sistemlerine girme başlıklı 243. maddesine göre, *" (1) Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren ve orada kalmaya devam eden kimseye bir yıla kadar hapis veya adli para cezası verilir. (2) Yukarıdaki fıkrada tanımlanan fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi halinde, verilecek ceza yarı oranına kadar indirilir. (3) Bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse, altı aydan iki yıla kadar hapis cezasına hükmolunur".*

TCK'da yer alan söz konusu hüküm zarar suçu değil; bir tehlike suçu olarak öngörülmüştür[324]. Bu suçun oluşması için, bir bilişim sisiteminin bütününe veya bir kısmına hukuka aykırı olarak girilmesi ve bir müddet orada kalınmaya devam edilmesi gerekir. Suçun oluşması için ayrıca girilen bilişim sistemi içindeki verilerin ele geçirilmesi gerekmemektedir. Ancak, bilişim sistemine girme nedeniyle sistemin içerdiği verilerin yok olması veya

[323] Ayrıntılı bilgi için bkz. Yıldız, **a.g.e.**, s. 51 vd.
[324] Ketizmen, **a.g.e.**, s. 80.

değişmesi durumunda kişiye verilecek ceza artırılmıştır. Hukuka aykırı olarak girilen bilişim sistemindeki verilerin ele geçirilmesi durumunda ise TCK'nın 136. maddesinde yer alan "*verileri hukuka aykırı olarak verme veya ele geçirme suçu"* oluşacaktır.

Bu suç ile korunan hukuksal yarar, özel hayatın gizliliğinin ve bilişim sistemlerinin güvenliğinin sağlanmasıdır.

Bilişim sistemlerine girme fiili başka suçların oluşmasına da neden olabilir. Örneğin, bir bilişim sistemine girilmesi TCK'nın 132. maddesinde düzenlenen haberleşmenin gizliliğini ihlal suçu veya 134. maddesinde düzenlenen özel hayatın gizliliğini ihlal suçunu oluşturabilir. Bu durumda fikri içtima kurallarının uygulanması söz konusu olacaktır. TCK'nın 44. maddesine göre işlediği bir fiil ile birden fazla farklı suçun oluşmasına sebebiyet veren kişi, bunlardan en ağır cezayı gerektiren suçtan dolayı cezalandırılır.

TCK'da yer alan bu hüküm Siber Suç Sözleşmesinin 2. maddesinde öngörülen "*kanunsuz erişim"* suçunun karşılığıdır. 2. maddeye göre her taraf devlet, kasıtlı olarak ve haksız bir şekilde bir bilgisayar sisteminin tamamına veya bir kısmına erişim fiilinin iç hukukunda suç olarak öngörülmesine ilişkin gerekli düzenlemeyi yapmalıdır. Taraf devletler, bu suçun bilgisayar verisi elde etme niyeti veya diğer dürüst olmayan başka bir niyetle güvenlik önlemlerinin ihlal edilerek işlenmesi şeklinde ya da başka bir bilgisayar sistemi ile bağlantılı bir bilgisayar sistemi ile ilişkili kılarak tanımlayabilirler.

2. Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme

TCK'nın sistemi engelleme, bozma, verileri yok etme veya değiştirme başlıklı 244. maddesine göre, *"(1) Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır. (2) Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi, altı aydan üç yıla kadar hapis cezası ile cezalandırılır. (3) Bu fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde, verilecek ceza yarı oranında artırılır…."*

Söz konusu kanun hükmü ile aslında iki farklı suç türü düzenlenmiştir. Birinci fıkrada bilişim sistemlerine müdahale suçu, ikinci fıkrada ise verilere müdahale suçu düzenlenmiştir. Ayrıca, üçüncü fıkrada söz konusu suçların nitelikli hali düzenlenmiştir. 244. maddede öngörülen suçlar zarar suçlarıdır. Bu suçlar ile korunan hukuksal yarar bilişim sistemlerinin ve sistem içerisinde yer alan verilerin güvenliğinin sağlanmasıdır.

Bilişim sistemlerine ve verilere müdahale suçu, Siber Suç Sözleşmesinin 4. ve 5. maddelerinde de düzenlenmiştir. Sözleşmenin 4. maddesine göre, her taraf devlet, kasıtlı olarak ve haksız bir şekilde bir bilgisayar verisine zarar verme, silme, bozma, değiştirme veya erişilemez kılma fiilerinin işlenmesinin iç hukukunda suç olarak öngörülmesine ilişkin gerekli düzenlemeyi yapmalıdır. Taraf devletler birinci fıkrada tanımlanan suçun oluşmasını ciddi bir zarar doğma şartına bağlama hakkına sahiptir. Sözleşmenin 5. maddesine göre ise her taraf devlet, kasıtlı olarak ve haksız bir şekilde bilgisayar verisinin giriş yapılarak, iletilerek, zarar verilerek, silinerek, bozularak, değiştirilerek veya erişilemez kılınarak bir bilgisayar sisteminin işlevini yerine getirmesine ciddi bir şekilde engel olunmasına yönelik fiillerin işlenmesinin iç hukukunda suç olarak öngörülmesine ilişkin gerekli düzenlemeyi yapmalıdır.

3. Bilişim Sistemlerini Kullanarak Hukuka Aykırı Yarar Sağlama

Bilişim sistemlerinin kullanılarak hukuka aykırı olarak yarar sağlanmasınının önlenmesi amacıyla TCK'da birden fazla hükme yer verilmiştir. İlk olarak TCK'nın bilişim sistemlerine veya verilere müdahale suçlarını düzenleyen 244. maddesininin dördüncü fıkrasında *"Yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması halinde, iki yıldan altı yılan kadar hapis ve beşbin güne kadar adli para cezasına hükmolunur"* hükmüne yer verilmiştir. Doktrinde yardımcı nitelikte bir norm olarak kabul edilen bu suçun yanısıra hırsızlık ve dolandırıcılık suçunun nitelikli halleri olarak, bilişim sistemlerinin kullanılması suretiyle hırsızlık suçu (md. 142) ve bilişim sistemlerinin araç olarak

kullanılması suretiyle dolandırıcılık suçu (md. 158) ayrıca düzenlenmiştir[325]. Son olarak, banka veya kredi kartlarının kötüye kullanılmasına ilişkin 245. maddede özel bir düzenlemeye yer verilmiştir. Bu düzenlemeye göre, *"(1) Başkasına ait bir banka veya kredi kartını, her ne suretle olursa olsun ele geçiren veya elinde bulunduran kimse, kart sahibinin veya kartın kendisine verilmesi gereken kişinin rızası olmaksızın bunu kullanarak veya kullandırtarak kendisine veya başkasına yarar sağlarsa üç yıldan altı yılan kadar hapis ve beşbin güne kadar adli para cezası ile cezalandırılır. (2) Başkalarına ait banka hesaplarıyla ilişkilendirilerek sahte banka veya kredi kartı üreten, satan, devreden, satın alan veya kabul eden kişi üç yıldan yedi yıla kadar hapis ve onbin güne kadar adli para cezası ile cezalandırılır. (3) Sahte oluşturulan veya üzerinde sahtecilik yapılan bir banka veya kredi kartını kullanmak suretiyle kendisine veya başkasına yarar sağlayan kişi, fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde dört yıldan sekiz yıla kadar hapis ve beşbin güne kadar adli para cezası ile cezalandırılır. (4) Birinci fıkrada yer alan suçun; a) Haklarında ayrılık kararı verilmemiş eşlerden birinin, b) Üstsoy veya altsoyunun veya bu derecede kayın hısımlarından birinin veya evlat edinen veya evlatlığın, c) Aynı konutta beraber yaşayan kardeşlerden birinin, zararına olarak işlenmesi halinde, ilgili akraba hakkında cezaya hükmolunmaz. (5) Birinci fıkra kapsamına giren fiillerle ilgili olarak bu Kanunun malvarlığına karşı suçlara ilişkin etkin pişmanlık hükümleri uygulanır".*

Bu hükümde üç farklı suç tipi düzenlenmiştir. Birinci fıkrada gerçek banka veya kredi kartlarının kötüye kullanılması, ikinci fıkrada sahte banka veya kredi kartı üretilmesi, satılması, devredilmesi, satın alınması veya kabul edilmesi, üçüncü fıkrada ise sahte bir banka veya kredi kartının kullanılması suçu düzenlenmiştir. İlk bakışta bu suç tiplerinin internet aracılığıyla işlenmesi mümkün gözükmemektedir. Maddede banka veya kredi kartının fiziksel varlığının aranmasına yönelik bir tanımlama yapılmıştır. Ancak, 5464 sayılı Banka Kartları ve Kredi Kartları Kanununun 3. maddesinde yer alan

[325] Ketizmen, **a.g.e.**, s. 178.

banka kartı ve kredi kartının tanımlanmasına yönelik hüküm, bu tanımlamanın yönünü kısmen değiştirmektedir. Söz konusu Kanunun 3. maddesinde banka kartı, mevduat hesabı veya özel cari hesapların kullanımı dahil bankacılık hizmetlerinden yararlanmayı sağlayan kart olarak; kredi kartı ise nakit kullanımı gerekmeksizin mal ve hizmet alımı veya nakit çekme olanağı sağlayan basılı kart veya fiziksel varlığı bulunmayan kart numarası olarak tanımlanmıştır. Bu durumda, fiziksel varlığı bulunmayan kredi kartı numarası da kredi kartı sayılacaktır[326]. Ancak, bu durum banka kartları açısından geçerli değildir.

Bilgisayarlarla ilgili sahtecilik ve dolandırıcılık suçu, Siber Suç Sözleşmesinde de düzenlenmiştir (md. 7 ve 8).

II. İNTERNET ORTAMINDA KİŞİSEL VERİLERİN KORUNMASI

Kişisel verilerin korunması (the protection of data privacy) konusu internetin gelişimi ile birlikte daha fazla önem kazanmış olmakla birlikte, bu alanı genel bir çerçevede internetten bağımsız olarak düzenleyen hukuksal kurallar evvelden beri mevcuttu. Fakat, internetin kişisel verilerin işlenmesini ve kötüye kullanımını kolaylaştırması nedeniyle bu alan, internetle birlikte özellikle 1980'li yıllarda önem kazanmaya başlamış ve günümüzde insan hakları açısından vazgeçilmez bir özgürlük alanı haline gelmiştir.

Kişisel verilerin korunması bir bütünlük arz etmekle birlikte özellikle internet özelinde ayrı bir bakış açısını gerektirmektedir[327]. Gerçi, kişisel verilerin korunması hukuku açısından bu verilerin internet bağlantılı işlenip işlenmediği önem taşımamaktadır. Bu çalışmada bu iki hususu göz önünde bulundurarak kişisel verilerin korunması bir bütünlük içerisinde incelenmiş, ancak internet özelinde bir bakış ortaya konulmaya çalışılmıştır.

Kişisel verilerin korunmasının hukuksal açıdan üç boyutu bulunmaktadır. Birinci boyut, korumanın hukuksal ilke ve kurallarının belirlenmesi, ikinci boyut ilke ve kurallara uyulmasının sağlanması, üçüncü

---

[326] Ketizmen, **a.g.e.**, s. 187-188.
[327] Oğuz Şimşek, **Anayasa Hukukunda Kişisel Verilerin Korunması**, Beta, 1. Baskı, İstanbul, Şubat 2008, s. 176.

boyut ise ilke ve kurallara uyulmamasından dolayı ortaya çıkan zararların giderilmesidir. Söz konusu üç boyut sırasıyla devletin düzenleme, cezai veya idari yaptırım uygulama ve hukuksal sorumluluğu sağlama yetkileri ile ilgilidir. Düzenleme yetkisi bu bölümde, cezai ve idari yaptırım uygulama yetkisi sorumluluk bölümünde incelenmiştir. Hukuksal sorumluluk ise çalışmanın kapsamı dışında kalmaktadır.

Kişisel verilerin korunması konusu esas olarak AB Veri Koruma Direktifi (95/46/EC) çerçevesinde değerlendirilmiştir. AB ülkeleri, yürürlüğe koyduğu veri koruma kanunlarında bu Direktifi esas almaktadır.

A. Özel Hayatın Gizliliği ve Kişisel Verilerin Korunması

Özel hayatın gizliliği (the right to privacy), öz bir ifadeyle "*yalnız bırakılma hakkı"* (*right to be left alone)* olarak tanımlanabilir[328]. Kişi varlığı ve onuru açısından taşıdığı önemden dolayı özel hayatın gizliliği, uluslararası sözleşmelerde temel bir hak ve özgürlük olarak öngörülmüştür. İnsan Hakları Evrensel Bildirgesi'nin 12. maddesine göre, hiç kimsenin özel yaşamına, ailesine, konutuna ya da haberleşmesine keyfi olarak karışılamaz, onuruna ve adına saldırılamaz. Herkesin, bu gibi müdahale ya da saldırılara karşı yasa tarafından korunma hakkı vardır. Benzer bir koruma Avrupa İnsan Hakları Sözleşmesi ile de güvence altına alınmıştır. Bu Sözleşmenin "*özel hayatın ve aile hayatının korunması"* başlıklı 8. maddesine göre herkes özel ve aile hayatına, konutuna ve haberleşmesine saygı gösterilmesi hakkına sahiptir. Bununla birlikte birçok hak gibi özel hayatın gizliliği de mutlak bir hak niteliğinde değildir ve bu hak için bazı sınırlar öngörülmüştür. Ulusal güvenlik, kamu emniyeti, ülkenin ekonomik refahı, dirlik ve düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için bu hak sınırlandırılabilir (md. 8/2).

---

[328] Althaf Marsoof, "Online Social Networking and The Right to Privacy: The Conflicting Rights of Privacy and Expression", **International Journal of Law and Information Technology**, Oxford University Press, Vol. 19, No. 2, 2011, s. 112. Saadet Yüksel, **Özel Yaşamın Bir Parçası Olarak Telekomünikasyon Yoluyla Yapılan İletişimin Gizliliğine Önleyici Denetimle Müdahale**, Beta, İstanbul, 2012, s. 9-16.

Özel hayatın gizliliğine bazı sınırlar getirilmekle birlikte, bu hakkın kullanılmasının ortadan kaldırılmasını engellemek ve kişilere hukuksal güvence oluşturmak amacıyla bu sınırların belirlenmesi de belli kurallara bağlanmıştır. Anılan sözleşmeye göre, özel hayatın gizliliği ancak Sözleşmede sayılan nedenlerle, demokratik bir toplumda zorunlu olduğu ölçüde ve yasayla sınırlandırılabilecektir.

Özel hayatın gizliliği, kapsam alanı itibariyle oldukça geniş bir konudur. Özel hayatın gizliliği ile kişisel verilerin korunması, birbiri ile bağlantılı ancak farklı hukuksal müesseselerdir[329]. Kişisel verilerin korunması, özel hayatın gizliliğine ilişkin spesifik bir düzenleme alanı olarak tanımlanabilir[330]. AİHS'de kişisel verilerin korunmasına ilişkin özel bir düzenleme öngörülmemiş; bu hak, özel hayatın gizliliğine ilişkin özgürlük çerçevesinde ele alınmıştır[331]. Çoğu ülkenin Anayasasında kişisel verilerin korunmasına ilişkin özel düzenlemeler yer almaktadır.

B. Kişisel Verilerin Genel Korunması

Kişisel verilerin korunması alanında düzenleme içeriği açısından iki yaklaşım bulunmaktadır. Birincisi, bu alanın genel olarak düzenlenmesi yaklaşımıdır. Diğeri ise spesifik alanlara yönelik özel düzenleme yaklaşımıdır. Çoğu hukuk sisteminde bu iki yaklaşımı bir arada görmek mümkündür. Konu burada genel düzenleme yaklaşımı çerçevesinde ele alınmış, aşağıda spesifik bir alan olarak elektronik haberleşme sektöründe kişisel verilerin korunması incelenmiştir.

1. Uluslararası Hukukun Kaynakları

Kişisel verilerin korunması konusunda genel nitelikli uluslararası sözleşmelerden ziyade bölgesel nitelikli sözleşmeler yapılmıştır. Avrupa

---

[329] Civelek, **a.g.e.**, s. 7.
[330] Mahremiyeti, bölgesel mahremiyet, haberleşme mahremiyeti, vücut bütünlüğüne ilişkin mahremiyet ve veri mahremiyeti olarak sınıflandıran ve kişisel verilerin korunması konusunu, veri mahremiyeti çerçevesinde değerlendiren görüş için bkz. Ketizmen, **a.g.e.**, s. 192-193.
[331] Şimşek, **a.g.e.**, s. 37.

Konseyi ve Avrupa Birliğince yürürlüğe konulan sözleşme ve direktifler bu anlamda önem taşımaktadır[332].

Kişisel verilerin korunmasını sağlamak için yapılan ilk uluslararası sözleşme, Avrupa Konseyi tarafından 1981 yılında imzaya açılan Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşmedir (108 sayılı Sözleşme)[333]. Bu sözleşmeye ek, Denetleyici Kurumlar ve Sınır Ötesi Veri Akışına Dair Protokol ise 2001 tarihinde imzaya açılmıştır (181 sayılı Sözleşme)[334]. Sözleşmenin ülkeler açısından yürürlüğe girebilmesi için, Sözleşmede öngörülen güvencelerin üye devletlerce ulusal hukukta garanti altına alınması bir şart olarak öngörülmüştür (md. 4). Ülkemiz açısından kişisel verilerin korunması, genel bir kanun ile düzenlenmemiş olduğundan bu şart henüz yerine getirilememiş ve Sözleşmeye taraf olunamamıştır[335].

Avrupa Konseyi Bakanlar Komitesi, kişisel verilerin korunması konusunda bazı spesifik alanlara ilişkin olarak 1980'lerden günümüze çeşitli tarihlerde tavsiye kararları (recommendation) ve kararlar (resolution) almıştır[336]. Bu kararlar Konsey üyesi ülkeler açısından yol gösterici mahiyet taşımaktadır.

AB ise kişisel verilerin korunmasında genel ilke ve kuralları belirlemek amacıyla AB Veri Koruma Direktifini [337] 1995 yılında yürürlüğe koymuştur. AB'nin veri koruma alanında yürürlüğe koyduğu tek direktif, AB Veri Koruma

---

[332] Ayrıntılı bilgi için bkz. Elif Küzeci, **Kişisel Verilerin Korunması**, Turhan Kitabevi, Ankara, 2010, s. 116 vd.

[333] Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data 1981, http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm, 17.09.2012. Ayrıca bkz. Şimşek, **a.g.e.**, s. 22.

[334] Additional Protocol to the Convention for the Protection of Individuals With Regard to Automatic Processing of Personal Data Regarding Supervisory Authorities and Transborder Data Flows, http://conventions.coe.int/Treaty/EN/treaties/html/181.htm, 18.9.2012.

[335] Akıllıoğlu, **a.g.m.** s. 7. Şimşek, **a.g.e.**, s. 30.

[336] Bu kararlar için bkz. http://www.coe.int/t/dghl/standardsetting/dataprotection/legal_instruments_en.asp, 18.09.2012. Bu kararlardan birisi de 23.02.1999 tarihinde kabul edilen internette Kişisel Verilerin Korunmasına İlişkin Tavsiye Kararıdır.

[337] The Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:html, 18.09.2012.

Direktifi değildir. Telekonünikasyon sektöründe kişisel verilerin korunmasına yönelik 2002/58/EC sayılı Direktif ile veri saklamayı düzenleyen 2006/24/EC sayılı Direktif de kişisel verilerin korunmasına yönelik özel nitelikli direktiflerdir.

Nihayet, Ekonimik İşbirliği ve Kalkınma Teşkilatı (OECD) ve Birleşmiş Milletler de kişisel verilerin korunması konusunda önemli düzenlemeler yapmaktadır. OECD tarafından 1981 yılında kabul edilen Mahremiyetin Korunması ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber İlkeler (Guidelines on The Protection of Privacy and Transborder Flows of Personal Data) ile Birleşmiş Milletler tarafından 1990 yılında kabul edilen Bilgisayarlarla İşlenen Kişisel Veri Dosyaları Hakkında Yönlendirici İlkeler (Guidelines Concerning Computerized Personal Data Files), kişisel verilerin korunması konusunda ülkeler arası uyumlaştırıcı ve yol gösterici kurallar içermektedir[338].

Bu bölümde ele alınan konular esas itibariyle AB direktifleri çerçevesinde incelenmiştir.

2. Kişisel Veri ve İşlenmesi

"*Kişisel veri" (personal data)*, AB Veri Koruma Direktifinde belirli veya belirlenebilir gerçek bir kişi ile ilgili herhangi bir bilgi olarak; belirlenebilir kişi ise doğrudan veya dolaylı olarak, özellikle bir kimlik numarası veya kişinin fiziksel, psikolojik, zihinsel, ekonomik, kültürel veya sosyal kimliği ile tanımlanabilen kişi olarak tanımlanmaktadır (md. 2/1, a). Bu tanım, kişisel veriyi gerçek kişi ile sınırlandırmakta; verinin kapsamını herhangi bir veri olarak oldukça geniş tutmakta, ancak bu verinin belirli veya belirlenebilir bir kişiyle bağlantısını aramaktadır[339].

Bu çerçevede özellikle, internet bağlamında işlenebilecek veya yayınlanabilecek ad, soyad, adres, kimlik numarası, doğum yeri, aile bilgileri, telefon numarası, e-mail, meslek, eğitim bilgileri, adli sicil kayıtları, şifre, kredi kartı bilgileri, faturalar, resim, görüntü, etnik köken, din, siyasi veya felsefi

---

[338] Şimşek, **a.g.e.**, s. 13, 16.
[339] Şimşek, **a.g.e.**, s. 43.

görüş, cinsel yönelim, sağlık bilgisi, banka hesap bilgileri, seyahat bilgileri, otel kayıtları, meslek örgütlerinin tuttuğu kayıtlar, sosyal paylaşım sitelerinin kayıtları, arama motorlarında yapılan aramaların tutulduğu kayıtlar, gezilen internet sitesi bilgilerine ilişkin tutulan kayıtlar kişisel veri bağlamında örnek olarak verilebilecek verilerden sadece bazılarıdır[340].

Kişisel veri içerisinde yer alan bazı veriler "*hassas kişisel veri" (sensitive data)* olarak tanımlanmaktadır. Hassas kişisel veri kategorisi oluşturulmasının amacı bazı bilgilerin daha fazla mahremiyet ve hassasiyet gösteriyor olmasıdır[341]. Örneğin, bir kişinin dini inancı veya cinsel tercihine ilişkin bilgi, bu kişinin ad ve soyadına ilişkin bilgiden daha mahrem ve hassastır. Ad ve soyadınızın başkaları tarafından öğrenilmesi sizi çok rahatsız etmeyebilir; ama dini inancınız veya cinsel tercihinizin başkaları tarafından öğrenilmesini istemeyebilirsiniz[342]. Ayrıca, kişilerin etnik kökenine ilişkin bilgilerin toplanması örneğinde olduğu gibi bazı hassas bilgilerin yeterli derecede güvence altına alınmadığı toplumlarda bu bilgilerin kötüye kullanılması diğer bilgilerin kötüye kullanılmasından daha vahim sonuçlar ortaya çıkarabilir[343]. Bu nedenle bu tür bilgiler, diğer bilgilere göre daha fazla güvence gerektirmektedir.

AB Veri Koruma Direktifinde hassas kişisel verilerin işlenmesi özel bir düzenleme ile güvence altına alınmıştır. Direktifte hassas kişisel veri tanımlanmamıştır. Bunun yerine hassas veriler sayılarak kural olarak bu verilerin işlenemeyeceği öngörülmüş, ancak bu kurala birçok istisna getirilmiştir. 8. maddede kural olarak, üye devletlerin kişilerin ırksal veya etkin kökenlerini, siyasi görüşlerini, dini veya felsefi inançlarını, meslek birliği üyeliğini ve sağlık ve cinsel yaşamlarına ilişkin bilgilerin işlenmesini

---

[340] Civelek, **a.g.e.**, s. 19-21.
[341] Şimşek, **a.g.e.**, s. 86.
[342] David L. Baumer, Julia B. Earp, J.C. Poindexter, "Internet Privacy Law: A Comparison Between the United States and the European Union", **Computers & Security**, 23, 2004, s. 402-403.
[343] Örneğin, Nazi Almanya'sında Yahudilerin ortadan kaldırılması için etnik kökenlerine ilişkin bilgiler merkezi bir sistemde toplanmış ve bu bilgiler soykırımda kullanılmıştır. Bkz. Baumer / Earp / Poindexter, **a.g.m.**, s. 401. Buna rağmen, İngiltere Veri Koruma Kanununda etnik kökene ilişkin verilerin tutulabileceği düzenlenmiştir.

engelleyecekleri öngörülmüştür[344]. Kural bu olmakla birlikte ikinci fıkra ile bu kurala bazı sıkı şartlar altında; kişinin açık rızası veya hayati çıkarları, istihdam hukuku açısından ortaya çıkan zorunluluklar, kar amacı gütmeyen kuruluşların faaliyetlerinin yürütülmesi, verilerin kamuya açık olması, savunma hakkının kullanılması, sağlık hizmetlerinin yürütülmesi, kamu yararının gerektirmesi, adli ve idari yaptırımlar ve özel hukuk yargı kararlarının kayıt altına alınması durumlarında uygulanabilecek istisnalar getirilmiştir.

Kişisel verilerin korunması bağlamında önem taşıyan bir diğer önemli kavram "*kişisel verilerin işlenmesi"* kavramıdır. Kişisel verilerin işlenmesi, AB Veri Koruma Direktifinde; toplama, kaydetme, organize etme, depolama, uyarlama veya değiştirme, geri alma, kullanma, ileti ile ifşa, yayma veya başka bir şekilde ulaşılabilir yapma, hizalama veya birleştirme, engelleme, silme veya yok etme gibi otomatik olan veya olmayan yöntemlerle kişisel veri üzerinde yürütülen herhangi bir işlem olarak tanımlanmıştır. Görüldüğü üzere, kişisel verilerin işlenmesi kavramı hem şekil yönünden hem de araç yönünden oldukça geniş tanımlanmıştır. Burada belirtilmesi gereken önemli bir nokta kişisel verilerin işlenmesinin elektronik ortamda işlenen kişisel verileri kapsadığı gibi yazılı ortamda işlenen kişisel verileri de kapsamasıdır.

Diğer taraftan, AB Veri Koruma Direktifinin 3. maddesinde bu Direktifin kapsam alanı ayrıca belirlenmiş olduğundan kişisel verilerin işlenmesi konusunda çerçeveyi bu açıdan çizmek gerekir. Bu çerçevede, topluluk hukuku dışında kalan alanlar, kamu güvenliği, ulusal savunma, ekonomik güvenlik dahil devletin güvenliği ve ceza hukukundan doğan kamu faaliyetleri gibi alanlar ile kişilerin sırf kişisel ve ailevi faaliyetlerinde AB Veri Koruma Direktifi uygulanmayacaktır (md. 3). Şu halde, kişisel verilerin işlenmesi kavramını bu istisnalarla birlikte değerlendirmemiz gerekecektir.

---

[344] AB Veri Koruma Direktifinde yer verilen hassas kişisel veriler yanında kimi ülke uygulamalarında genetik ve biometrik veriler, özür durumu ve sosyal yardımlara ilişkin veriler de hassas kişisel veri kabul edilmektedir. Ayrıca, AB Veri Koruma Direktifinin 8. maddesinin beşinci fıkrası gereği kişilerin mahkumiyetlerine ilişkin bilgiler de hassas kişisel veri kategorisi içerisinde yer almaktadır. Cemil Kaya, "Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi", **İÜHFM**, C. LXIX, S. 1-2, 2011, s. 319-320.

AB Veri Koruma Direktifine göre "*veri işleme sorumlusu" (controller)*, kişisel verilerin işlenmesinin amaç ve yöntemlerini tek başına veya diğerleriyle birlikte belirleyen gerçek veya tüzel kişi, kamu kurum veya kuruluşu veya herhangi bir kuruluşu ifade etmektedir (md. 2/1, d). "*Veri İşleyici" (processor)* ise veri işleme sorumlusu adına kişisel verileri işleyen gerçek veya tüzel kişi, kamu kurum veya kuruluşu veya herhangi bir kuruluş anlamına gelmektedir (md. 2/1, e).

3. Amaç

Kişisel verilerin korunması açısından ortaya çıkan uluslararası sorunlar, bu alandaki diğer sorunlar gibi uluslararası işbirliği gerektirmektedir. Uluslararası işbirliğinin sağlanması için bazı adımlar atılmış olmakla birlikte genel itibariyle bu alanda başarılı olunduğu söylenemez. AB ve Avrupa Konseyi gibi bazı bölgesel örgütler bu işbirliğinin sağlanması noktasında önemli mesafe kat etmiştir. AB, kişisel verilerin korunması konusunun birlik içerisinde bilginin serbest dolaşımı açısından taşıdığı önemi de göz önünde bulundurarak bu alanda aktif bir rol üstlenmiştir. AB Veri Koruma Direktifi, AB ülkelerinde kişisel verilerin korunması, bu alanda hukuksal bir standardizasyonun sağlanması ve bu ülkeler arasında bilginin transferinin kolaylaştırılması amacıyla 1995 yılında yürürlüğe konulmuştur.

İçeriksel olarak öz bir ifade ile kişisel verilerin korunmasına yönelik hukuksal düzenlemelerin amacı, kişisel verilerin işlenmesini belli kurallara bağlamak; böylece kişisel verilerin işlenmesindeki yarar ile özel hayatın gizliliği arasındaki dengeyi sağlamaktır[345]. Bir başka açıdan bu düzenlemelerin amacı, kişisel verilerin haksız bir şekilde kullanımının önüne geçilmek istenmesidir[346].

Gerek devlet ve gerekse özel hukuk tüzel kişileri tarafından her geçen gün artan şekilde kişisel veriler işlenmekte ve kullanılmaktadır. Kişisel verilerin işlenmesinin temel hak ve özgürlükler ile olan doğrudan bağlantısı nedeniyle bu alana müdahale edilebilmesinin hukuksal gerekçeleri yasal bir

---

[345] Civelek, **a.g.e.**, s. 72.
[346] Maier, **a.g.m.**, s. 156.

çerçeve içerisinde düzenlenmek zorundadır. Örneğin, terörle veya organize suçlarla mücadele edilebilmesi için kişisel verilerin hangi kapsamda işlenebileceği hususu, kişisel verilerin korunmasına ilişkin kanunlar ile düzenlendikten sonra hukuksal bir meşruiyet kazanabilmektedir.

4. Önemi

Toplumsal yaşantı açısından kişisel verilerin işlenmesini gerekli kılan bazı nedenler olabilir. Bu nedenler, devletin kişisel verileri işlemesine ilişkin olabileceği gibi özel hukuk kişilerinin işlemesine de ilişkin olabilir. Demokratik hukuk devleti niteliğinin bir gereği olarak devlet, özel hayatın korunmasını güvence altına almak zorundadır. Kişilerin özel hayatının korunması hususu, demokratik devletin kaçınılmaz bir gerekliliğidir.

Kişisel verilerin gerek kamu ve gerekse özel sektörde işlenmesini gerekli kılan ulusal güvenlik, kamu düzeni, genel sağlık, kamu hizmetlerinin sunumu, ticari hayatın gereklilikleri gibi nedenler olabilir. Günümüzde kişisel verilerin elektronik ortamda işlenmesi kamu ve özel sektör açısından önemli bir değer haline gelmiştir. Kamu kuruluşlarının kamu hizmetlerini bilgi ve iletişim teknolojilerinin sunduğu imkanlar ile yürütmeye başlaması önemli derecede kişisel verinin işlenmesi sonucunu beraberinde getirmiştir[347]. Taşıdığı ticari değer nedeniyle kişisel verilerin işlenmesi özel sektör kuruluşları açısından kaçınılmaz bir hale gelmiş ve rekabet, kişisel verilerin önemini oldukça artırmıştır.

Kişisel verilerin kamu ve özel sektör tarafından işlenmesinin gerekliliği ile birlikte bu faaliyetin sınırlarının belirlenmesi özel hayatın gizliliği açısından kaçınılmaz bir hal almıştır. "*Kişisel veriler, hangi amaçlar için nereye kadar ve hangi kişisel güvenceler çerçevesinde işlenebilmelidir"* sorusu[348] kişisel verilerin korunması hukukunun çağdaş hukuk sistemlerinde hak ettiği yeri almasını sağlamıştır.

Kişisel verilerin korunması, hukuka uygun bir şekilde işlenen verilerin yetkisiz kişilerin eline geçmesinin önlenmesi açısından da önem

[347] Şimşek, **a.g.e.**, s. 4. Küzeci, **a.g.e.**, s. 322.
[348] Kılınç, "Anayasal Bir Hak", s. 1092.

taşımaktadır. Bilgi ve iletişim teknolojileri sektöründeki gelişmeler, büyük miktardaki kişisel verilerin merkezi sistemlerde tutulmasını kolaylaştırmakta[349] ve bu gelişim, kişisel verilerin korunmasının ehemmiyetini artırmaktadır[350]. Örneğin, bir kamu bilişim sistemi olan MERNİS veri tabanında tüm vatandaşların nüfus bilgileri merkezi bir sistem içerisinde tutulmakta, bu durum sistemin ve dolayısıyla tüm vatandaşların kişisel verilerinin korunmasının ehemmiyetini artırmaktadır. Önemine rağmen maalisef ülkemizde tüm vatandaşların kimlik bilgilerinin yer aldığı MERNİS verileri çalınmış; internette paket programlar halinde belli bir ücret karşılığında satışa sunulmuş ve birçok hukuk bürosu da (1500 civarında olduğu ileri sürülüyor) bu çalınmış verileri satın almıştır[351]. Yine, sosyal paylaşım siteleri, önemli derecede artan bir şekilde özel hayatın ihlal edildiği alanlardan birisi haline gelmiştir[352]. Sosyal paylaşım sitelerinde, kimlik hırsızlığı (identity theft) yapılarak isim hakkının kötüye kullanılması çok yaygın bir hal almıştır. Kimlik hırsızlığı ile birçok şekilde kişiler istismar edilebilmektedir. Kullanıcı profilleri oluşturulurken girilen hassas kişisel bilgileri ve fotoğrafları da düşündüğümüz zaman sosyal paylaşım sitelerinin özel hayatın gizliliğini ne şekilde olumsuz etkileyebileceği kolaylıkla görülebilir.

Diğer önemli bir konu kişisel verilerin paylaşımında ortaya çıkan sorunların çözüme kavuşturulması gerekliliğidir. Bir vergi idaresinin görev alanı çerçevesinde elde ettiği kişilere yönelik vergisel bilgilerin, yine görev alanları çerçevesinde diğer kamu kurumları ile paylaşılmasının mümkün olup olmadığı[353] veya bir özel hukuk tüzel kişisi tarafından işlenen verilerin diğer özel hukuku kişileri veya kamu kurumları ile paylaşılıp paylaşılamayacağı gibi

---

[349] Bu gelişimi, *"gözetim toplumu"* olarak adlandıran yazarlar da vardır. Bkz. David Lyon, **Elektronik Göz Gözetim Toplumunun Yükselişi**, Çev. Dilek Hattatoğlu, Sarmal Yayınevi, İstanbul, 1997, s. 16.
[350] Marsoof, **a.g.m.**, s. 122.
[351] http://www.turkhukuksitesi.com/showthread.php?t=52705
ve http://www.sabah.com.tr/Yasam/2010/07/28/yetmis_milyon_kisinin_kimlik_bilgileri_calindi, 18.09.2012.
[352] Kılınç, "Anayasal Bir Hak", s. 1091-1092.
[353] Akıllıoğlu, **a.g.m.** s. 3.

konuların hukuk kurallarınca belirlenmesi gerekir. Aksi takdirde, kişisel verilerin yetkisiz kişilerin eline geçmesi söz konusu olabilir.

Kişisel verilerin işlenmesine ilişkin yeni teknolojiler geliştirilmektedir. "*Bulut bilişim" (cloud computing)* bu teknolojilerden biridir. Bulut bilişim ile bilgisayarlar arasında ortak bilgi paylaşımı sağlanmaktadır. Bu tür yeni teknolojiler, kişisel verilerin korunmasının ehemmiyetini daha fazla artırmaktadır.

Ülkemizde kişisel verilerin korunması açısından önem taşıyan bir başka konu da fişleme veya fişlenme olgusudur[354]. Arkasında kötü bir şöhret bırakan fişleme faaliyetleri, kişisel verilerin korunması hakkının önemini daha da artırmaktadır. Bu hak, siyasi, ideolojik ya da kişisel çıkarlar uğruna kişisel verilerin işlenmesini imkansız kılmaktadır.

5. İlkeler

Kişisel verilerin korunması açısından bazı ilkeler geliştirilmiştir. Amerikan Federal Ticaret Komisyonunun (Federal Trade Commission) 1973 yılında yayınladığı ilkeleri (Fair Information Practices Principles), Avrupa Komisyonunun 1981 yılında kabul ettiği 108 sayılı Sözleşme ve OECD'nin 1980 yılında yayınladığı bir kılavuz ile belirlenen ilkeler takip etmiştir. Sonrasında bu ilkeler AB Veri Koruma Direktifinin düzenleme alanında da geniş bir yer bulmuştur.

Fair Information Practices Principles ile beş ilke kabul edilmiştir. Bunlar; bilgilendirme, onay, katılım, güvenlik ve sorumluluk ilkeleridir[355]. Daha geniş bir çerçevede OECD kılavuzu ile sekiz ilke kabul edilmiştir. Bu ilkeler: toplamanın sınırlanması, veri kalitesi, amacın sınırlandırılması, kullanımın sınırlandırılması, güvenlik önlemleri, açıklık, kişisel katılım ve hesap verilebilirliktir[356]. AB Veri Koruma Direktifinde ise kişisel verilerin işlenmesinde bilgilendirme, veri kalitesi, gizlilik, güvenlik, onay ve erişim

---

[354] Civelek, **a.g.e.**, s. 156.
[355] http://www.ftc.gov/reports/privacy3/fairinfo.shtm, 13.09.2012.
[356] Guidelines on The Protection of Privacy and Transborder Flows of Personal Data. Bkz. http://oecdprivacy.org/, 12.09.2012. Şimşek, **a.g.e.**, s. 15.

hakkı gibi bazı ilkeler yer almıştır. Bu ilkelerin kısaca AB Direktifi çerçevesinde ele alınması faydalı olacaktır.

Direktifte bilgilendirme ilkesi, verinin bizzat veri sahibinden toplanıp toplanmamasına göre ayrı ayrı düzenlenmiştir. Verinin, veri sahibinden elde edilmesi halinde veri işleme sorumlusu veya temsilcisinin kimliği, verinin işlenmesinin amacı, verinin alıcıları, veri işleme aşamasında sorulan soruları cevaplamanın zorunlu veya gönüllü olup olmadığı, cevap verilmemesi durumunda bunun sonuçları, kişinin hakkında tutulan veriye erişim ve düzeltme hakkının bulunduğu gibi bilgiler veri sahibinin bilgisine sunulmak zorundadır. Verinin, veri sahibinden elde edilmemesi durumunda ise veri işlenirken veya açıklanacaksa açıklanmasından önce veri sahibinin bilgilendirilmesi gerekir. Bilgilendirme yapılırken veri işleme sorumlusu veya temsilcisinin kimliği, verinin işlenmesinin amacı, verinin alıcıları, veri işleme aşamasında sorulan soruları cevaplamanın zorunlu veya gönüllü olup olmadığı, cevap verilmemesi durumunda bunun sonuçları, kişinin hakkında tutulan veriye erişim ve düzeltme hakkının bulunduğu gibi bilgilerin de veri sahibine sunulması gerekir. Bu ilkeye göre örneğin, bir internet sayfasını ziyaret eden kişiden kişisel bilgi elde edilecekse bu hususa ilişkin bilgilendirmenin ilgili internet sitesinde açıklanması zorunludur[357].

Verinin kaliteli olması açısından kişisel veri adil ve hukuka uygun bir şekilde işlenmeli[358]; spesifik, açık ve meşru amaçlar için toplanmalıdır. Üye devletler tarafından yeterli güvencelerin sağlanması şartıyla tarihi, istatistiki ve bilimsel amaçlar için veri işlenebilir. Kişisel verilerin işlenmesi öngörülen amaçla ilgili ve amacı gerçekleştirmeye yeterli olması gerekir. Kişisel verilerin amacı aşan şekilde işlenmesi mümkün değildir. İşlenen veriler doğru olmalı ve gerekli olduğu süreden daha uzun bir süre tutulmamalıdır.

Kişisel veri, kural olarak veri sahibinin açık rızası ile işlenebilir. Ancak bu kuralın yanısıra kişisel veriler, bir sözleşmenin uygulanması, veri işleme sorumlusunun kanunen yerine getirmekle yükümlü olduğu bir hususun uygulanması, veri sahibinin önemli bir menfaatine ilişkin olması, kamu

---

[357] Yüksel, **a.g.e.**, s. 118.
[358] Şimşek, **a.g.e.**, s. 83.

yararına ilişkin veya kamu kurumlarının görevini yerine getirmesinin gereği olması veya veri işleme sorumlusu ya da üçüncü kişi için meşru bir amaç taşıması durumlarında işlenebilir.

Veriye erişim hakkı, veri sahibinin veri işleme sorumlusundan herhangi bir sınırlandırma, gecikme ve masraf olmaksızın kendisi hakkında bir verinin işlenip işlenmediği, işlemenin amacı, verinin ilgili olduğu kategoriler, verinin açıklanacağı alıcılar ve alıcı kategorileri, veri işleme süreci gibi hususlarda bilgilere erişim hakkına sahip olduğunu ifade etmektedir. Kişinin hakkında işlenen verilere itiraz etme hakkı ayrıca düzenlenmiştir.

İşlenen kişisel veriler açısından veri gizliliği ve güvenliğinin sağlanması gerekir. Kişisel verilere erişim imkanına sahip veri işleme sorumlusu tarafından görevlendirilen kişiler ve veri işleyicileri, veri işleme sorumlusunun talimatları veya kanuni zorunluluk dışında kişisel verileri işleyemez. Veri işleme sorumlusu, kişisel verilere kazaen veya hukuka aykırı bir şekilde zarar verilmesi, kaybedilmesi, değiştirilmesi, yetkisiz erişim ve ifşanın önlenmesi amacıyla uygun teknik ve organizasyonel önlemleri almak zorundadır. Bu çerçevede örneğin, kamu ve özel sektör kuruluşlarınca kimlik doğrulama sisteminin özel hayatın gizliliğini sağlayacak bir sistem içerisinde bütüncül bir yaklaşımla ele alınması gerekir[359].

6. Kişisel Verilerin Korunmasını Sağlayan Kurumsal Yapı

AB Veri Koruma Direktifinin 28. maddesinde göre her üye devlet, Direktif doğrultusunda yürürlüğe konulan ulusal kişisel verilerin korunmasına ilişkin kanunların uygulanmasını gözetmek üzere bir veya birden fazla kamu denetim kuruluşu (supervisory authority) oluşturmak zorundadır. Bu kuruluşlar görevlerini yerine getirirken tam bağımsızlık içerisinde hareket etmelidir. Kişisel verilerin korunmasına ilişkin idari tedbirler alınırken ve düzenlemeler yapılırken denetim kuruluşuna danışılmasını sağlamaya yönelik tedbirlerin de alınması gerekir.

---

[359] Muammer Ketizmen, Çağlar Ülküderner, "e-Devlet Uygulamalarında Kişisel Verilerin Korun(ma)ması", **XII. "Türkiye'de İnternet" Konferansı**, Ankara, 8-10 Kasım 2007, s. 190.

Oluşturulacak denetim kuruluşunun bazı yetkiler ile donatılması zorunlu kılınmıştır. Bu çerçevede öncelikle denetim kuruluşları, kişisel verilerin işlenmesine ilişkin faaliyetlerle ilgili verilere erişme ve denetim görevine ilişkin gerekli olan bilgileri toplama gibi inceleme ve araştırma yetkilerini haiz olmalıdır. İkinci olarak denetim kuruluşları, kişisel verilerin işlenmesinin engellenmesi, silinmesi veya yok edilmesine ilişkin kararlar verebilme, kişisel verilerin işlenmesi konusunda geçici veya sürekli yasaklama, konuyu ulusal parlamentolara veya siyasi kuruluşlara taşıma, veri işleme sorumlusunun uyarılması veya ihtarda bulunulması, denetim kurumunun bu çerçevede aldığı kararların yayınlanmasını sağlama gibi yetkilere de sahip olmalıdır[360]. Son olarak, kişisel verilerin hukuka aykırı olarak işlenmesi durumunda konuyu hukuksal olarak soruşturma yetkisi ile adli mercilere taşıma yetkisi de bu kuruluşlara verilmelidir. Denetleme kuruluşları açısından rapor yayınlama ve gizlilik ilkesine uyma gibi bazı sorumluluklar da öngörülmüştür.

7. Sorumluluk

Kişisel verilerin hukuka aykırı işlenmesi cezai, idari ve hukuksal sorumluluk doğurabilir. Cezai sorumluluk, kişisel verileri hukuka aykırı işleme fiilinin ceza kanunlarında suç olarak yer almasını gerekli kılmakta; idari sorumluluk, kişisel verileri işlemekten yasaklama veya idari para cezası uygulanması gibi sonuçlar ortaya çıkarabilmektedir. Hukuksal sorumluluk ise kişilerin zarara uğraması durumunda zararlarının zarar veren tarafından tazminine yönelik hukuksal bir güvence niteliği taşımaktadır. Kamu kurumları açısından sorumluluk, ülkemizde idari sorumluluk kurallarının uygulanmasını gerektirir. 2577 sayılı İdari Yargılama Usul Kanununa göre idari eylem ve işlemlerden dolayı kişisel hakları doğrudan muhtel olanlar tarafından ancak tam yargı davası açılabilir[361] ve bu davaların görüm yeri idari yargı mercileridir.

---

[360] Şimşek, **a.g.e.**, s. 50.

[361] İdari işlem veya eylemin bir kamu görevlisinin kişisel kusurundan kaynaklanması durumunda özel hukuk sorumluluk hükümlerinin uygulanacağı ve adli yargı mercilerinin görevli olacağı yargı

İdare, bir işlemi ile kişisel verileri hukuka aykırı işleyebileceği gibi bu aykırılığı bir eylemi ile de gerçekleştirebilir. İşlenmemesi gereken hassas kişisel verilerin alınan idari bir kararla işlenmesi idari işlemin ortaya çıkarabileceği zarar verici bir davranış iken konut edindirme yardımı ödemeleri için birçok kişinin TC kimlik numaraları ile birlikte kimliklerinin internette açıklanması idari bir eylemin ortaya çıkarabileceği zarar verici davranıştır.

8. Ülke Düzenlemeleri

Kişisel verilerin korunmasına ilişkin yasal düzenlemelerde bazı temel ilkeler benzerlik göstermekle birlikte, düzenlemeler arasında önemli farklılıklar bulunmaktadır[362]. Bu benzerlik ve farklılıkları tüm ülke uygulamalarını göz önüne alarak ayrıntısı ile ortaya koymak pek mümkün değildir. Bu nedenle burada, bu alanda olumlu/olumsuz tarafı ile ilgi çeken veya ön plana çıkan bazı ülke düzenlemeleri genel bir bakış açısı içerisinde incelenmiştir.

Ülkemizdeki gelişime benzer şekilde çoğu ülkede kişisel verilerin korunmasına yönelik spesifik kanunlar yürürlüğe konulmadan önce de kişisel verilerin veya daha geniş çerçevede özel hayatın gizliliğini sağlamaya yönelik kanunlar veya düzenlemeler mevcuttu. Örneğin, çoğu common law ülkesinde gizlilik ihlali (breach of confidence), telif hakları hukuku (copyright law) veya hakaret hukuku (the law of defamation) gibi kurallar, özel hayatın gizliliğinin sağlanması için kullanılmaktaydı. Ancak zamanla bu kuralların özel hayatın gizliliğinin korunması açısından yeterli olmadığı görülmüş[363] ve bu alanı düzenlemeye yönelik özel ve spesifik kanunlar yürürlüğe konulmuştur.

Avrupa ülkelerinde kişisel verilerin korunmasına ilişkin ilk yasal düzenlemeler 1970'li yıllarda yapılmıştır[364]. Almanya'da Hessen Eyaleti Veri

---

içtihatlarında ve doktrinde genel olarak kabul görmektedir. Kişisel kusur oluşturan haller ise kamu görevlisinin suç oluşturan davranışları, yargı kararlarının uygulanmaması, kamu görevlisinin kötü niyetli davranması veya ağır kusuru olarak kabul edilmektedir. Şeref Gözübüyük, **Yönetsel Yargı**, 30. Bası, Turhan Kitabevi, Ankara, 2010, s. 300. Günday, **a.g.e.**, s. 326-327.

[362] Kuner, **a.g.m.**, s. 177.

[363] Marsoof, **a.g.m.**, s. 116-122.

[364] Şimşek, **a.g.e.**, s. 10.

Koruma Kanunu (Data Protection Act of the German Federal State of Hessen 1970), Fransa'da Veri İşleme, Veri Dosyaları ve Kişisel Haklar Kanunu (Data Processing, Data Files and Individual Liberties 1978), İsveç'te Veri Koruma Kanunu (Data Protection Act 1973) bu yasal düzenlemelerden bazılarıdır[365]. İngiltere'de kişisel verilerin korunması amacıyla Veri Koruma Kanunu (Data Protection Act 1998) kabul edilmiş ve 2000 yılında yürürlüğe girmiştir[366]. Bu Kanunun uygulanmasının sağlanması amacıyla bugüne kadar 30 civarında ikincil düzenleme yapılmıştır[367].

Avrupa ülkelerinde kişisel verilerin korunmasına yönelik özel kanunlar bulunmakla birlikte ABD'de genel bir kişisel verilerin korunması kanunu bulunmamaktadır. ABD'de 1974 tarihli Özel Yaşamın Gizliliği Kanunu (The Privacy Act) ve 1966 tarihli Bilgi Edinme Hakkı Kanunu (The Freedom of Information Act) kişisel verilerin korunmasına yönelik bazı kanunlardır.

Ülke uygulamalarına bakıldığında dikkat çeken bir diğer husus genel nitelikli kişisel verilerin korunması kanunlarının yanısıra bazı spesifik alanlara yönelik olarak da özel nitelikli kişisel verilerin korunması kanunlarının yürürlüğe konuluyor olmasıdır[368]. Çoğu hukuk siteminde aslında kişisel verilerin korunmasına yönelik genel düzenlemeler bulunmakla birlikte düzenlemelerin bu alanda yeterli hukuksal güvenceyi oluşturamadığı düşünülmekte ve bazı özel alanlara yönelik spesifik düzenlemelere ihtiyaç duyulmaktadır[369]. Örneğin, genel nitelikte bir kişisel verilerin korunması kanunu bulunmamakla birlikte ABD'de The Health Insurance Portability and Accountability Act of 1996 (HIPAA) kişisel sağlık verilerinin, The Children's Online Privacy Protection Act of 1998 (COPPA) çocuklara ilişkin kişisel bilgilerin, Financial Services Modernization Act of 1999 finansal açıdan kişisel verilerin korunmasını sağlayan yasal düzenlemelerdir[370].

---

[365] Kuner, **a.g.m.**, s. 176.
[366] Bu Kanun öncesinde İngiltere'de Data Protection Act 1984 yürürlükteydi. Peter Carey, **Data Protection A Practical Guide to UK and EU Law**, Third Edition, Oxford University Press, 2009, s. 9.
[367] Carey, **a.g.e.**, s. 10.
[368] Kılınç, "Anayasal Bir Hak", s. 1116.
[369] Akıllıoğlu, **a.g.m.** s. 7.
[370] Baumer / Earp / Poindexter, **a.g.m.**, s. 402.

Nihayet, doktrinde kişisel verilerin korunmasına ilişkin uluslararası yaklaşımlar kişi veya sektör odaklı olmasına göre bir ayrıma tabi tutulmaktadır. AB'nin kişisel verilerin korunmasına ilişkin direktifleri ve üye ülkelerin bu direktif çerçevesinde yaptığı düzenlemeler, AB'nin bu konudaki yaklaşımının başlı başına bir model olarak ele alınması sonucunu doğurmuştur[371]. Bu model genel olarak demokratik ve insan haklarına saygılı bir yaklaşım olarak değerlendirilmektedir. Bu yaklaşımın karşısına ise kişisel verilerin korunmasında kişilerin haklarından çok şirketlerin çıkarlarına hizmet eden bir model olarak ABD yaklaşımı konulmuştur[372]. Bu açıdan bakıldığında, kişisel verilerin korunması hukukunun farklı hukuk sistemlerinde farklı amaçlara hizmet edecek şekilde tasarlandığı görülmektedir[373]. ABD, kişisel verilerin korunması ile ulusal güvenliğin sağlanması arasındaki dengeyi ulusal güvenliğin sağlanması yönünde de kullanmaktadır[374]. Bunun tipik örneği olarak AB ile ABD arasında yapılan Yolcu İsmi Kaydı Anlaşmasına göre ABD'ye yolculuk yapan yolcuların kimlik bilgilerinin ABD'ye verilmesini gösterebiliriz[375].

9. Türk Hukukundaki Durum

Türk hukuk sisteminde özel hayatın korunmasına ilişkin hükümler evvelden beri yürürlüktedir. Kişisel verilerin korunması özelinde genel bir kanun bulunmamasından dolayı ülkemiz bu alanda kimi çevrelerce eleştiri konusu olmaktadır. Bu eleştirilerde haklılık payı bulunmaktadır; ancak Türk hukuk sisteminde kişisel verilerin korunmasını sağlayan hukuksal düzenlemelerin bulunmadığı söylenemez[376]. Belki, bu düzenlemelerin etkin bir bakış açısı içerisinde bütüncül bir yaklaşımla ele alınmadığından dolayı

---

[371] Bu yaklaşımın Kanada, Avustralya, Yeni Zelanda ve Hong Kong gibi ülkeleri etkilediği belirtilmiştir. Segura-Serrano, **a.g.m.**, s. 216.
[372] Segura-Serrano, **a.g.m.**, s. 214. Maier, **a.g.m.**, s. 157. Bu farklılığın karşılaştırmalı olarak incelendiği bir çalışma için bkz. Baumer / Earp / Poindexter, **a.g.m.**, s. 400-412.
[373] Yüksel, **a.g.e.**, s. 123.
[374] Yüksel, **a.g.e.**, s. 110.
[375] Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS) (2007 PNR Agreement), http://eur-lex.europa.eu/LexUriServ/site/en/oj/2007/l_204/l_20420070804en00180025.pdf, 03.12.2012.
[376] Kılınç, "Anayasal Bir Hak", s. 1130.

kişisel verilerin korunmasında yetersiz kalındığı söylenebilir. Bu nedenle, Türk hukuk sisteminde kişisel verilerin korunmasına yönelik düzenlemeler bulunmadığı yönündeki görüşlerin doğruluk payı bulunmamaktadır.

Ülkemizde genel olarak özel hayatın gizliliği, özel olarak ise kişisel verilerin korunması bağlamında değerlendirilebilecek birçok hukuksal düzenleme bulunmaktadır. Kişisel verilerin korunmasına ilişkin temel düzenleme Anayasamızın 20. maddesinin dördüncü fıkrasında yer almıştır[377]. Söz konusu düzenlemede yer alan *"Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak, kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir"* hükmü ile kişisel verilerin korunması hakkı Türk hukuk sisteminde anayasal bir güvenceye kavuşturulmuştur.

Anılan anayasal hüküm yanında kişisel verilerin korunmasına ilişkin olarak TCK (md. 135-138)[378], Türk Medeni Kanunu (md. 24, 25) ve Türk Borçlar Kanununda (md. 49) da düzenlemeler bulunmaktadır. Ayrıca, bu düzenlemelerin yanısıra birçok özel kanunda ve ikincil düzenlemede kişisel verilerin korunmasına ilişkin hükümler bulunmaktadır. Örneğin, elektronik haberleşme sektöründe kişisel verilerin korunması amacıyla Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik yürürlüğe konulmuştur[379]. Ayrıca, ülkemizde bilgi edinme hakkı ayrı bir kanun ile düzenlenmiştir[380]. Bilgi edinme hakkının, kişisel verilerin korunması konusu ile yakın ilişkisi bulunmaktadır[381]. Bilgi

---

[377] Söz konusu fıkra Anayasamızın 20. maddesine 2010 yılında eklenmiştir. 5982 sayılı Türkiye Cumhuriyeti Anayasasının Bazı Maddelerinde Değişiklik Yapılması Hakkında Kanun. RG. 13.05.2010.

[378] Kişisel verilerin korunmasına ilişkin TCK'nın söz konusu maddelerinde yer alan "*kişisel verilerin kaydedilmesi suçu", "verileri hukuka aykırı olarak verme veya ele geçirme suçu" ve "verileri yok etmeme suçunun"* ayrıntılı açıklaması için bkz. Ketizmen, **a.g.e.**, s. 230 vd.

[379] RG. 24.07.2012, 28363.

[380] Bkz. 4982 sayılı Bilgi Edinme Hakkı Kanunu, RG. 24.10.2003, 25269.

[381] Akıllıoğlu, **a.g.m.** s. 2.

Edinme Hakkı Kanunu kapsamında kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşları, kişilere ilişkin kayıt altına aldıkları her türlü bilgi veya belgeyi bir menfaat koşulu da aranmaksızın kişilerin bilgisine sunmak zorundadır. Kişisel verilerin korunması bağlamında, kamu kurum ve kuruluşları tarafından kayıt altına alınan verilere kişilerin erişim hakkının bulunduğuna dair bu ilke (katılım ilkesi) Bilgi Edinme Hakkı Kanunu ile düzenlenmiş ve güvence altına alınmıştır.

Türk hukukunda bu düzenlemeler yanında ayrıca kişisel verilerin korunmasına yönelik genel kanun niteliğinde bir tasarı (Kişisel Verilerin Korunması Kanunu Tasarısı) hazırlanmıştır. Tasarı henüz yasalaşmamıştır. Tasarının amacı, *"kişisel verilerin işlenmesinde kişinin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin uyacakları esas ve usulleri düzenlemektir"* olarak belirlenmiştir. Tasarı ile kişisel verilerin işlenmesinde uyulacak ilkeler, kişisel verilerin işlenmesinin usul ve esasları, hassas kişisel verilerin işlenmesine ilişkin esaslar, veri sahibinin hakları, verilerin üçüncü kişilere aktarımı, kişisel verilerin işlenmesinde yetkili kılınan Kişisel Verileri Koruma Kurumunun kuruluş esasları ve görevleri, şikayet usulü gibi hususlar düzenlenmektedir[382].

C. Elektronik Haberleşme Sektöründe Kişisel Verilerin Korunması

Elektronik haberleşme sektöründe kişisel verilerin korunması, internet ortamında yapılan iletişimi kapsayacak şekilde geniş bir çerçevede düzenlenmektedir.

1. 2002/58/EC Sayılı Direktif

Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğin Sağlanması Hakkında 2002/58/EC sayılı AB Direktifi[383], elektronik haberleşme alanında kişisel verilerin özel olarak düzenlenmesi amacıyla

[382] Tasarı için bkz. http://www2.tbmm.gov.tr/d23/1/1-0576.pdf, 20.08.2013.

[383] The Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector. Metin için bkz. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2002L0058:20091219:EN:PDF, 04.02.2013.

yürürlüğe konulmuştur[384]. Direktif, Birliğe üye devletlerin elektronik haberleşme sektöründe kişisel veriler işlenirken mahremiyet ve gizlilik hakkının korunması ve verilerin Birlik bünyesinde serbest dolaşımının sağlanmasını hedeflemektedir. Direktif, 95/46/EC sayılı Direktif yanında kişisel verilerin korunması açısından ek güvence niteliğinde görülmektedir[385]. Bir diğer deyişle, 95/46/EC sayılı Direktifinin özel bir görünümü olarak bu Direktifi tamamlamaktadır. Kamu güvenliği, savunma, devletin ekonomik varlığı dahil ulusal güvenlik, ceza hukuku alanındaki faaliyetler ve Avrupa Topluluğunu kuran anlaşmanın dışında kalan konular Direktifin kapsamına girmemektedir.

2002/58/EC sayılı Direktifte "*iletişim" (communication)*, kamusal olarak ulaşılabilir bir elektronik iletişim servisi aracılığıyla sınırlı sayıda taraf arasında değişim yapılan veya iletilen bilgi olarak tanımlanmıştır. Bir elektronik iletişim ağı üzerinden radyo ve televizyon yayıncılığının bir parçası olarak iletilen bilgi bu kavramın kapsamına dahil değildir. Ancak bu durumda da söz konusu bilginin belirlenebilir abone veya bilgiyi kabul eden kullanıcıya ilişkin olmaması gerekir. "*Elektronik posta"* ise bir kamusal iletişim ağı üzerinden gönderilen ve ağ içerisinde veya alıcı tarafından alınana kadar alıcı tarafında depolanabilen metin, ses, konuşma veya görüntü içeren mesaj olarak tanımlanmıştır. Direktifte, elektronik haberleşme sektöründe kişisel veriler işlenirken uyulması gereken güvenlik ve gizlilik ilkeleri ile trafik verilerinin işlenmesine ilişkin usul ve esaslar gibi hususlar ayrıca düzenlenmiştir.

2. AB Veri Saklama Direktifi

AB Veri Saklama Direktifi (EU Data Retention Directive)[386], 13 Nisan 2006 tarihinde Avrupa Birliği Resmi Gazete'sinde yayımlanarak aynı yıl

---

[384] Şimşek, **a.g.e.**, s. 62.
[385] Carey, **a.g.e.**, s. 12. Baumer / Earp / Poindexter, **a.g.m.**, s. 405. Şimşek, **a.g.e.**, s. 57.
[386] Directive 2006/24/EC Of The European Parliament And Of The Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

içerisinde yürürlüğe girmiştir. 2004-2005 yıllarında gerçekleştirilen Madrid ve Londra saldırıları, bu Direktifin yürürlüğe konulmasında önemli etki doğurmuştur. Direktif, her devletin iç hukuk kurallarına göre belirlenecek ciddi suçların soruşturulması ve kovuşturulması için elektronik haberleşme hizmeti veya kamusal iletişim ağı sağlayan kişilerin tutmakla yükümlü oldukları verilerin, her üye devlet açısından paralel bir şekilde uygulanabilmesi amacıyla yürürlüğe konulmuştur. Direktifte, trafik ve yer verileri ile abone ya da kullanıcının belirlenmesi amacıyla gerekli olan verilerin tutulması kapsama alınmış; iletişim içeriğinin tutulması kapsam alanı dışında bırakılmıştır.

Tutulacak verinin niteliği açısından iletişim verisinin tutulması, önemli bir suçtan dolayı olmalıdır. Her ne kadar iletişim verisinin tutulabileceği önemli suçlar Direktifte belirlenmemiş ve bu konuda devletlere takdir yetkisi verilmiş olsa da devletlerin her suçtan dolayı böyle bir yola gitmesi mümkün değildir.

Direktife göre, üye devletler tutulan verilerin ulusal hukuka uygun ve spesifik olaylara özgü olarak yetkili ulusal otoriteler tarafından kullanılmasını sağlama yükümlülüğü altındadır. Bu çerçevede, internet servis sağlayıcılardan genel bir iletişim verisi talep etmek mümkün değildir. Ayrıca, erişime ilişkin esaslar ulusal hukuk tarafından düzenlenmeli ve ulusal hukukca; AB hukuku, uluslararası kamu hukuku ve Avrupa İnsan Hakları Sözleşmesinde yer alan ilke ve kurallar gözetilmelidir.

Direktif, telefon iletişimini kapsadığı gibi internet iletişimini de kapsamaktadır. Bununla birlikte, kapsama bazı sınırlar konulmuştur. Tutulacak verinin niteliği, süresi, usulü ve şekli sınırlandırılmıştır. Direktife göre, internet erişimi, e-mail ve internet ortamında yapılan telefon görüşmesine ilişkin olarak;

1. İletişimin kaynağı,
2. İletişimin hedefi,
3. Tarih, zaman ve iletişim süresi,
4. İletişim türü,

---

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF, 22.8.2012.

5.Tarafların kullandığı iletişim cihazı,

6. Mobil cihazın yeri,

hakkındaki verilerin tutulması gerekir.

İletişim verisinin tutulma süresi, iletişim tarihinden itibaren en az 6 ay, en fazla 2 yıl olarak belirlenmiş ve bu süreler arasında bir belirleme yapma yetkisi devletlere bırakılmıştır. Usul açısından önemli olan husus iletişim verilerinin servis sağlayıcılar tarafından tutulabileceğidir. Bir diğer deyişle, bizzat devletlerin böyle bir iş yapması mümkün değildir.

Direktif, tutulan verilerin korunması ve veri güvenliği açısından ek güvenceler de getirmiştir (md. 7).

Direktifin getirmiş olduğu düzenlemeler bazı Avrupa ülkelerinde özel hayatın gizliliği açısından ciddi eleştirilere maruz kalmış ve yürürlüğe girdiği tarihten bugüne, bu Direktif esas alınarak bazı üye ülkelerde ulusal düzeyde yürürlüğe konulan veri saklama kanunları, bu ülke Anayasa Mahkemelerince iptal edilmiştir. Almanya, Romanya ve Bulgaristan Anayasa Mahkemeleri çıkarılan veri saklama kanunlarını anayasalarında yer alan özel hayatın korunması hükümlerine aykırı bulmuştur.

3. Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik

2002/58/EC sayılı Direktif ile 2006/24/EC sayılı Direktif'in uygulanmasını sağlamak amacıyla Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik[387] yürürlüğe konulmuştur. Bu Yönetmeliğin amacı, elektronik haberleşme sektöründe kişisel verilerin işlenmesi, saklanması ve gizliliğinin korunması için bu sektörde faaliyet gösteren işletmecilerin uyacakları usul ve esasları düzenlemektir. Haberleşmenin içeriğine ilişkin verilerin saklanması, bu Yönetmeliğin kapsamına dahil değildir.

Yönetmelik ile kişisel verilerin işlenmesinde bazı ilkeler öngörülmüştür. Kişisel verilerin hukuka ve dürüstlük kurallarına uygun olarak işlenmesi, ilgili

[387] RG. 24.07.2012, 28363.

kişinin rızasına dayalı olarak işlenmesi, elde edilme amacıyla bağlantılı, yeterli ve orantılı olması, doğru olması ve gerektiğinde güncellenmesi, ilgili kişilerin kimliklerini belirtecek biçimde ve kaydedildikleri veya yeniden işlenecekleri amaç için gerekli olan süre kadar muhafaza edilmesi bu ilkelerden bazılarıdır. Yönetmelikte, kişisel verilerin işlenmesine ilişkin güvenlik kuralları, haberleşmenin gizliliği ilkesi, trafik verisinin işlenmesine ilişkin usul ve esaslar, saklanacak veri kategorileri, veri saklama süresi, saklanan verinin korunması ve güvenliğine ilişkin hususlar ayrıca düzenlenmiştir. Söz konusu düzenlemeler, genel olarak ilgili AB Direktifleri ile uyumlu düzenlenmiştir. Örneğin, saklanacak veri kategorileri 2006/24/EC sayılı Direktifte yer alan düzenleme ile örtüşmektedir[388].

---

[388] Yönetmeliğin 13. maddesi, 2006/24/EC Sayılı Direktifin 5. maddesinde yer alan hükümle uyumludur. Yönetmeliğin 13. maddesi şu şekildedir:

*"**Saklanacak veri kategorileri***

***MADDE 13 –**(1) Bu Yönetmelik kapsamında saklanması öngörülen veri kategorileri, aşağıda belirtilmiştir.*

a) Haberleşmenin takibi ve kaynağının tanımlanmasıiçin:

1) Sabit ve mobil telefon hizmetleriyle ilgili olarak; gerçekleşmeyen aramalar da dâhil olmak üzere haberleşmenin başlatıldığı hatta ait telefon numarası, abonenin adı ve adresi, hattın hangi tarihte hangi aboneye tahsis edildiğine ait bilgi.

2) internet ortamına erişim, elektronik posta ve internet telefonu ile ilgili olarak; tahsis edilmiş kullanıcı kimliği ve/veya telefon numarası, haberleşmenin gerçekleştiği andaki internet protokol adresi, abonenin/kullanıcının adı ve adresi.

b) Haberleşmenin sonlandırılacağı noktayı belirlemek için:

1) Sabit ve mobil telefon hizmetleriyle ilgili olarak; haberleşmenin sonlandırıldığı/sonlandırılacağı numara veya numaralar, çağrıiletme ve çağrı transferi gibi ek hizmetlerin olması durumunda çağrının yönlendirildiği numara veya numaralar, abonelerin adı ve adresi.

2) Elektronik posta ve internet telefonu ile ilgili olarak; elektronik posta alıcılarına ait kullanıcı kimliği, internet telefonu ile aranan alıcılara ait kullanıcı kimliği veya telefon numarası, internet telefonu veya elektronik posta alıcılarının adı ve adresi.

c) Haberleşmenin tarihi, zamanı ve süresini belirlemek için:

1) Sabit ve mobil telefon hizmetleriyle ilgili olarak; haberleşmenin başlangıç ile bitiş tarih ve zamanı.

2) internet erişimi, elektronik posta ve internet telefonu ile ilgili olarak; internet erişimi ile ilgili oturum açma, kapatma tarihi ve zamanı, tahsis edilen dinamik veya statik internet protokol adresi, abone/kullanıcı kimliği, elektronik posta veya internet telefonu ile ilgili oturum açma ile kapatma tarihi ve zamanı.

ç) Haberleşmenin türünü tanımlamak için:

1) Sabit ve mobil telefon hizmetleriyle ilgili olarak; kullanılan elektronik haberleşme hizmeti.

2) Elektronik posta ve internet telefonu ile ilgili olarak; kullanılan internet hizmeti.

d) Kullanıcıların haberleşme cihazlarını veya bunların ekipmanlarını tanımlamak için:

1) Sabit telefon hizmetiyle ilgili olarak; haberleşmenin başlatıldığı ve sonlandırıldığı telefon numaraları.

4. 5651 sayılı Kanun Çerçevesinde Trafik Bilgisi Tutma Yükümlülüğü

5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunda "*trafik bilgisi"*, internet ortamında gerçekleştirilen her türlü erişime ilişkin olarak taraflar, zaman, süre, yararlanılan hizmetin türü, aktarılan veri miktarı ve bağlantı noktaları gibi değerler olarak tanımlanmıştır. İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelikte ise trafik bilgisi, yer ve erişim sağlayıcılar açısından ayrı ayrı öngörülmüştür. Buna göre erişim sağlayıcı trafik bilgisi, internet ortamında yapılan her türlü erişime ilişkin olarak abonenin adı, kimlik bilgileri, adı ve soyadı, adresi, telefon numarası, sisteme bağlantı tarih ve saat bilgisi, sistemden çıkış tarih ve saat bilgisi, ilgili bağlantı için verilen IP adresi ve bağlantı noktaları gibi bilgileri; yer sağlayıcı trafik bilgisi ise internet ortamındaki her türlü yer sağlamaya ilişkin olarak; kaynak IP adresi, hedef IP adresi, bağlantı tarih ve saat bilgisi, istenen sayfa adresi, işlem bilgisi (GET, POST komut detayları) ve sonuç bilgileri gibi bilgileri ifade eder[389].

Yer sağlayıcı, yer sağlayıcı trafik bilgisini altı ay saklamakla, bu bilgilerin doğruluğunu, bütünlüğünü oluşan verilerin dosya bütünlük değerlerini zaman damgası ile birlikte saklamak ve gizliliğini temin etmekle (md. 7); erişim

---

2) Mobil telefon hizmetiyle ilgili olarak; haberleşmenin başlatıldığı ve sonlandırıldığı telefon numaraları, haberleşmenin başlatıldığı ve sonlandırıldığı tarafa ait IMSI ve IMEI numaraları; abone kaydıolmayan arama kartlı hizmetlerin olması durumunda hizmetin aktif hale getirildiği tarih ve zaman ile hizmetin aktif hale getirildiği hücre kimliği.

3) internet ortamına erişim, elektronik posta ve internet telefonu ile ilgili olarak; çevirmeli ağ erişimi için arayan telefon numarası, sayısal abone hattı numarası ya da haberleşmenin kaynaklandığı diğer nokta.

e) İlgili mevzuatın öngördüğü hallerde mobil haberleşme cihazının konumunu tespit etmek için; haberleşmenin başladığı hücre kimliği, haberleşme verilerinin saklandığı sürede hücre kimlikleri ile ilgili olarak hücrelerin coğrafi konumlarını tanımlayan veri, hücre adresi ve hücre kimliğinin o adrese atanma ve kaldırılma tarihleri.

(2) Bu Yönetmelik kapsamında, elektronik posta ve internet telefonu ile ilgili olarak verilerin saklanmasına ilişkin getirilen yükümlülükler, sadece işletmecilerin kendilerinin sundukları hizmetler ile sınırlıdır."

[389] Avrupa Konseyi Siber Suç Sözleşmesinde trafik verisi, bir bilgisayar sistemi aracılığıyla yapılan bir iletişim ile ilgili, iletişim zincirinin bir parçasını oluşturan bir bilgisayar sistemi tarafından üretilen, iletişimin kaynağını, varış noktasını, rotasını, zamanını, tarihini, boyutunu, süresini veya söz konusu hizmetin tipini gösteren herhangi bir bilgisayar verisi olarak tanımlanmıştır (md. 1).

sağlayıcı ise sağladığı hizmetlere ilişkin olarak Başkanlığın Kanunla ve ilgili diğer mevzuatla verilen görevlerini yerine getirebilmesi için, erişim sağlayıcı trafik bilgisini bir yıl saklamakla, bu bilgilerin doğruluğunu, bütünlüğünü oluşan verilerin dosya bütünlük değerlerini zaman damgası ile birlikte muhafaza etmek ve gizliliğini temin etmekle, internet trafik izlemesinde Başkanlığa gerekli yardım ve desteği sağlamakla (md. 8) yükümlü kılınmıştır.

Ç. Kişisel Verilerin Korunması ve İfade Özgürlüğü Arasındaki Denge

İfade özgürlüğü ile özel hayatın gizliliği arasındaki dengenin kurulması oldukça önemli bir konudur. Bu dengenin iyi sağlanamaması durumunda, bir taraftan özel hayatın gizliliğinin sağlanması amaçlanırken diğer taraftan ifade özgürlüğü güvenceleri zayıflatılabilir veya aksine ifade özgürlüğünün güçlendirilmesi amaçlanırken özel hayatın gizliliği haksız bir şekilde ihlal edilebilir[390].

İnternet alanında ifade özgürlüğünün sınırlanmasını gerektiren hususlardan birisi özel hayatın gizliliği (privacy) ilkesidir. Kişilerin özel hayatına müdahale oluşturan internet yayınları ifade özgürlüğü kapsamında değerlendirilmemekte ve sınırlandırılmaktadır. Başkalarının haklarını ihlal edecek şekilde bir hakkın kullanılması özgürlük kavramı içerisinde yer bulamamaktadır. Bununla birlikte asıl tartışma ortaya çıkaran alan ifade özgürlüğünün kullanılmasının nerede, yani hangi noktada özel hayatın gizliliğinin ihlali anlamına geleceğidir[391]. Hakaret, iftira, kutsal şeylere hakaret, küfürlü konuşma, nefret içerikli konuşma gibi fiillerin ifade özgürlüğü kapsamında değerlendirilemeyeceği tartışmasızdır[392]. Ancak, örneğin bir forum sitesinde bir ürün hakkında edinilen olumsuz bir tecrübeyi paylaşmanın ifade özgürlüğü kapsamında değerlendirilip değerlendirilemeyeceği tartışmalıdır.

---

[390] Marsoof, **a.g.m.**, s. 130-132.
[391] Weckert, **a.g.m.**, s. 106.
[392] Weckert, **a.g.m.**, s. 106.

AB Veri Koruma Direktifinde ifade özgürlüğü ile kişisel verilerin işlenmesi arasında ortaya çıkan çatışmanın giderilmesi amacıyla sanatsal, edebi ve gazetecilikle ilgili kişisel verilerin işlenmesine bazı istisnalar getirilmiştir. Bu istisnalar çerçevesinde bu alanlara ilişkin olarak üye devletler kişisel verilerin işlenmesi açısından öngörülen genel kurallara bazı istisnalar getirebileceklerdir (md. 9).

III. ÖNLEME AMAÇLI İNTERNET İLETİŞİMİNİN DENETLENMESİ

Devletler bugün internet iletişimini bütün yönleriyle denetleme olanağına sahiptir. Şu veya bu şekilde her devletin önceliğine göre internet iletişimi denetlenmekte ve suçla mücadele yöntemleri geliştirilmektedir[393]. Bu yöntemler sadece anti-demokratik olduğu ileri sürülen devletler tarafından değil demokratik olduğu ileri sürülen Batı devletleri tarafından da ciddi bir şekilde uygulanmaktadır[394]. Elbette, devletlerin demokrasi, hukuk ve özgürlük anlayışları ile siyasi sistemleri ve içinde bulundukları sosyo-kültürel yapı bu yöntemlerin demokratik veya anti-demokratik olarak şekillendirilmesinde etkili olmaktadır.

Özellikle, 11 Eylül saldırılarından sonra internet iletişiminin tespitine yönelik yasal düzenlemelerde önemli bir artış olmuştur. ABD'de, 2001'in Ekim'inde Yurtseverlik Kanunu (USA Patriot Act) yürürlüğe konulmuş ve internet iletişimi gözetim altına alınmıştır[395]. ABD'de Ulusal Güvenlik Ajansı (National Security Agency), bir mahkeme kararı olmaksızın iletişimin tespit ve takibini doğrudan idari bir kararla yapabilmektedir[396]. Hepting v. AT&T davasında, AT&T'nin ABD Ulusal Güvenlik Ajansına, iletişim verilerinin tutulduğu veri tabanına hukuka aykırı olarak erişim imkanı sağladığı iddia edilmiş ve Bush yönetimi bu davayı etkisiz kılmak ve hukukileştirmek için

---

[393] Mustafa Taşkın, **Adli ve İstihbari Amaçlı İletişimin Denetlenmesi**, Seçkin Yayınları, Ankara, 2008, s. 28.
[394] Özbek, **a.g.m.**, s. 133-134. Deibert / Rohozinski, **a.g.m.**, s. 44.
[395] David Lyon, **Surveillance After September 11**, Polity Press, 2004, s. 45.
[396] Ian Brown, "Communications Data Retention in an Evolving Internet", **International Journal of Law and Information Technology**, Vol. 19, No. 2, Oxford University Press, 2010, s. 102.

Yabancı İstihbarat İzleme Kanununda (Foreign Intelligence Surveillance Act of 1978 (FISA)), 2008 yılında değişikliğe gitmiştir[397].

İngiltere'de 11 Eylül saldırılarının hemen akabinde yürürlüğe konulan Anti-Terörizm, Suç ve Güvenlik Kanunu (Anti-Terrorism, Crime and Security Act 2001)[398] ile iletişiminin tespitine imkan tanınmıştır. İnternet servis sağlayıcılar bünyesine yerleştirilen programlar ile iletişim verilerine istenilen şekilde erişilebilmektedir. Regulation of Investigatory Powers Act 2000 (md. 12), internet üzerinden yapılan iletişimin takibine bu şekilde imkan tanıyan bir hukuksal düzenlemedir[399]. İngiltere'de birçok kamu kurumu bir mahkeme kararı olmaksızın iletişim verilerine doğrudan idari bir kararla erişebilmektedir[400]. İngiltere'de bir veri tabanında telefon aramaları, e-posta ve ziyaret edilen web sitelerinin kaydının tutulduğu ileri sürülmektedir[401]. 2005 yılında yapılan Londra saldırılarından hemen sonra, devlet her türlü iletişim verisine genel bir kararla ulaşabilmiş ve bu imkan İngiliz devletine, İngiliz internet servis sağlayıcıları tarafından gönüllü olarak sağlanmıştır[402].

İnternet iletişiminin denetlenmesi bastırıcı (adli) veya önleyici (idari) nitelikte olabilir[403]. Bastırıcı nitelikte internet iletişiminin denetlenmesi, bir suç işlendikten sonra bu suçun soruşturma ve kovuşturulması aşamasına ilişkin iken önleyici denetim suç işlenmeden önce yapılan denetimdir[404]. Adli denetim, CMK'da bir koruma tedbiri olarak düzenlenmiştir (md. 135. vd). Bu çalışmada internet iletişiminin denetlenmesi sadece önleyici denetim açısından ele alınmıştır.

İnternet iletişiminin denetlenmesi, haberleşme özgürlüğü ve özel hayatın gizliliğine bir müdahale oluşturduğu için sıkı şartlar altında

---

[397] Brown, **a.g.m.**, s. 100.
[398] http://www.legislation.gov.uk/ukpga/2001/24/contents, 22.08.2012.
[399] Brown, **a.g.m.**, s. 101. https://opennet.net/research/profiles/united-kingdom, 14.03.2013.
[400] Brown, **a.g.m.**, s. 102. Taşkın, **a.g.e.**, s. 51. Ayrıca bkz. https://opennet.net/research/profiles/united-kingdom, 14.03.2013.
[401] https://opennet.net/research/profiles/united-kingdom, 14.03.2013.
[402] Brown, **a.g.m.**, s. 108. Almanya, Fransa, İrlanda ve İtalya'da da önleme amaçlı interrnet iletişimi denetlenmektedir. Taşkın, **a.g.e.**, s. 40-57. Diğer Avrupa devletleri de önleme amaçlı internet iletişimini denetlemektedir. Lyon, **Surveillance**, s. 46.
[403] Taşkın, **a.g.e.**, s. 65. Necati Meran, **Adli ve Önleme Amaçlı İletişimin Denetlenmesi**, Adalet Yayınevi, Ankara, 2009, s. 4-5.
[404] Handan Yokuş Sevük, "Kolluk Tarafından Suçun Önlenmesine Yönelik Yapılan İletişimin Denetlenmesine İlişkin Değerlendirmeler", **TBB Dergisi**, S: 67, 2006, s. 45.

gerçekleştirilebilir. Her demokratik hukuk devletinde bu şartlar açıkça belirlenir ve kişilerin haberleşme özgürlüğü güvence altına alınır.

A. Önleyici Denetim Açısından İnternet İletişimi

İnternet, diğer fonksiyonlarının yanısıra aynı zamanda telefon, posta ve faks gibi kişisel haberleşmeye imkan tanıyan bir iletişim aracıdır. E-mail, sohbet odaları, msn ve skpe gibi ortamlar internet üzerinden kişisel haberleşmeye imkan tanımaktadır. İnternet ortamında kişisel haberleşmenin bu şekilde yürütülmesi önleyici denetime konu olabilmektedir[405].

İletişimin Tespiti Yönetmeliğinde *telekomünikasyon,* her türlü işaret, sembol, ses ve görüntünün ve elektrik sinyallerine dönüştürülebilen her türlü verinin kablo, telsiz, optik, elektrik, manyetik, elektromanyetik, elektrokimyasal, elektromekanik ve diğer iletim sistemleri vasıtasıyla iletilmesi, gönderilmesi ve alınması olarak tanımlanmıştır. Bu tanım çerçevesinde internet ortamında yapılan kişisel iletişim telekomünikasyon kavramının kapsamına girmektedir. Bu çerçevede, internet ortamında yapılan kişisel iletişim önleyici denetim açısından tespit edilebilecek, dinlenebilecek ve kayıt altına alınabilecektir. İnternet iletişiminin denetlenmesi, telekomünikasyon yoluyla yapılan iletişimin denetlenmesinin özel bir görünümünü oluşturmaktadır.

B. Telekomünikasyon Yoluyla Yapılan İletişiminin Tespiti, Dinlenmesi ve Kayda Alınması, Sinyal Bilgilerinin Değerlendirilmesi

Önleme amaçlı denetime konu olacak telekomünikasyon yoluyla yapılan iletişim, yürütülecek denetim faaliyeti açısından iletişimin tespiti, dinlenmesi, sinyal bilgilerinin değerlendirilmesi ve kayda alınması olmak üzere dört farklı esasta ele alınmıştır. İletişimin Tespiti Yönetmeliğinde *iletişimin tespiti,* iletişimin içeriğine müdahale etmeden iletişim araçlarının diğer iletişim araçlarıyla kurduğu iletişime ilişkin arama, aranma, yer bilgisi ve kimlik bilgilerinin tespit edilmesine yönelik işlemler olarak tanımlanmıştır.

---

[405] Taşkın, **a.g.e.**, s. 193.

"*İletişimin dinlenmesi ve kayda alınması"*, telekomünikasyon yoluyla gerçekleştirilmekte olan konuşmalar ile diğer her türlü iletişimin uygun teknik araçlarla dinlenmesi ve kayda alınmasına yönelik işlemler, "*sinyal bilgisinin değerlendirilmesi"* ise bir şebekede haberleşmenin iletimi veya faturalama amacıyla işlenen her türlü verinin değerlendirilmesi olarak ele alınmıştır.

Türk hukuk sisteminde söz konusu tedbirler dışında başka bir tedbir türü öngörülmemiştir. Adli amaçlı iletişimin denetlenmesi açısından şüpheli veya sanığın yakalanabilmesi için, mobil telefonun yerinin, hakim veya gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısının kararına istinaden tespit edilebileceği düzenlenmiştir. Bu tedbir türü, önleme amaçlı iletişimin denetlenmesi açısından düzenlenmemiştir. Bu nedenle, önleme amaçlı iletişimin denetlenmesi açısından bu tedbir uygulanamaz.

Genel olarak önleme amaçlı telekomünikasyon yoluyla yapılan iletişimin denetlenmesi açısından öngörülen söz konusu tedbirler, internet iletişiminin denetlenmesi açısından da uygulanmaya müsaittir. Bu çerçevede örneğin e-mail, sohbet odaları, msn ve skpe gibi ortamlar üzerinden yapılan iletişim tespit edilebilir, sesli ve görüntülü konuşmalar veya yazışmalar kayıt altına alınabilir[406].

C. Önleme Amaçlı İletişimin Denetlenmesi ve Haberleşme Özgürlüğü

Önleme amaçlı iletişimin denetlenmesi, özel hayatın gizliliğine ve haberleşme özgürlüğüne müdahale oluşturur[407]. Özel hayatın gizliliğinin spesifik bir alanı olarak haberleşme özgürlüğü, Anayasamızda ayrı bir maddede düzenlenmiştir. Anayasamızın 22. maddesine göre herkes haberleşme özgürlüğüne sahiptir ve haberleşmenin gizliliği esastır. Bununla birlikte, birçok özgürlük gibi haberleşme özgürlüğü de mutlak bir özgürlük değildir. Bu özgürlüğün bazı sınırları bulunmaktadır. Ulusal güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlakın korunması veya başkalarının hak ve özgürlüklerinin korunması bu sınırları

[406] Yüksel, **a.g.e.**, s. 155. Taşkın, **a.g.e.**, s. 194.
[407] Taşkın, **a.g.e.**, s. 31.

oluşturmaktadır. Bir diğer deyişle, bu nedenlere bağlı olarak haberleşme özgürlüğü sınırlandırılabilir ve gizliliğine dokunulabilir[408].

Söz konusu nedenlere bağlı olarak haberleşme özgürlüğüne müdahale edilmesi mümkün olmakla birlikte bu müdahalenin de sınırları bulunmaktadır. Anayasamızın 13. maddesi çerçevesinde haberleşme özgürlüğünün özüne dokunulamaz ve sadece 22. maddede sayılan nedenlere bağlı olarak bu özgürlüğe müdahale edilebilir. Sınırlandırma ancak kanunla öngörülebilir, Anayasanın sözüne ve ruhuna, demokratik toplum düzeninin gereklerine ve ölçülülük ilkesine aykırı olamaz. Ayrıca, 22. maddeye göre hakim kararı olmadıkça veya gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça haberleşme engellenemez ve gizliliğine dokunulamaz. Yetkili merciin kararı yirmidört saat içinde görevli hakimin onayına sunulur. Hakim, kararını kırksekiz saat içinde açıklar; aksi halde, karar kendiliğinden kalkar.

Bu çerçevede Türk hukuk sisteminde önleme amaçlı iletişimin denetiminde kanunilik ilkesi, denetimin suç işlenmesinin önlenmesi amacına yönelik olması, gizlilik ilkesi, hakim kararının aranması, elde edilen bilgilerin başka bir amaç için kullanılamaması, denetimin belli bir süre için gerçekleştirilebilmesi, denetimin yer açısından sınırlandırılması, elde edilen bilgilerin belli bir süre içerisinde yok edilmesi, denetimi gerçekleştirecek kamu kurumlarının belirli ve sınırlı olması gibi bazı sınırlandırmalar öngörülmüştür.

1. Kanunilik İlkesi

Kanunilik ilkesi gereği önleme amaçlı iletişimin denetlenmesine ilişkin usul ve esasların öncelikle ve yeterli güvencelerle kanun ile düzenlenmesi gerekir. Bu çerçevede, Türk hukuk sisteminde önleme amaçlı iletişimin denetlenmesine ilişkin usul ve esaslar kanun konusu olmuştur[409]. 5397 sayılı Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun[410] ile, 2559 sayılı Polis

[408] Yokuş Sevük, **a.g.m.**, s. 42.
[409] Yokuş Sevük, **a.g.m.**, s. 44. Taşkın, **a.g.e.**, s. 64.
[410] RG. 23.07.2005, 25884.

Vazife ve Selahiyet Kanunu[411], 2803 sayılı Jandarma Teşkilat, Görev ve Yetkileri Kanunu[412] ve 2937 sayılı Devlet İstihbarat Hizmetleri ve Millî İstihbarat Teşkilatı Kanunda[413] değişiklik yapılmış ve iletişimin önleme amaçlı denetiminin usul ve esasları düzenlenmiştir.

Söz konusu kanun hükümlerinin uygulanmasını sağlamak amacıyla 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 (İletişimin Tespiti Yönetmeliği) yürürlüğe konulmuştur[414]. İletişimin Tespiti Yönetmeliğinde belirlenen esas ve usuller dışında hiç kimse, bir başkasının iletişimini önleme amacı güderek telekomünikasyon yoluyla tespit edemez, dinleyemez, sinyal bilgilerini değerlendiremez ve kayda alamaz.

Söz konusu kanunlar ve yönetmelik çerçevesinde belirlenen usul ve esaslara aykırı dinlemeler hukuka aykırılık oluşturmakta ve aykırı denetim yapan kişiler hakkında cezai sorumluluk öngörülmektedir.

2. Önleme Amaçlı İletişimin Denetlenmesinin Nedenleri

Adli amaçlı iletişimin denetlenmesinden farklı olarak önleme amaçlı iletişimin denetlenmesi, suç işlenmesinin önlenmesi amacına hizmet eden bir hukuksal araçtır[415]. Tedbirin bu niteliği, 2559 sayılı Kanun, 2803 sayılı Kanun ve 2937 sayılı Kanunda ayrı ayrı ve açıkça düzenlenmiştir. 2559 sayılı Kanuna göre polis, Devletin ülkesi ve milletiyle bölünmez bütünlüğüne, Anayasa düzenine ve genel güvenliğine dair önleyici ve koruyucu tedbirleri almak, emniyet ve asayişi sağlamak üzere, ülke seviyesinde istihbarat

---

[411] http://www.mevzuat.gov.tr/MevzuatMetin/1.3.2559.pdf, 08.02.2013.
[412] http://www.mevzuat.gov.tr/MevzuatMetin/1.5.2803.pdf, 08.02.2013.
[413] http://www.mevzuat.gov.tr/MevzuatMetin/1.5.2937.pdf, 08.02.2013.
[414] http://www.mevzuat.gov.tr/Metin.Aspx?MevzuatKod=7.5.9596&MevzuatIliski=0&sourceXmlSearch=telekomünikasyon, 08.02.2013. CMK'da yer alan iletişimin tespiti, dinlenmesi, kayda alınması ve sinyal bilgilerinin değerlendirilmesine ilişkin usul ve esaslar, "*Ceza Muhakemesi Kanununda Öngörülen Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi, Gizli Soruşturmacı ve Teknik Araçlarla İzleme Tedbirlerinin Uygulanmasına İlişkin Yönetmelik"* ile düzenlenmiştir. Bkz. http://www.mevzuat.gov.tr/Metin.Aspx?MevzuatKod=7.5.11092&MevzuatIliski=0&sourceXmlSearch=telekomünikasyon, 08.02.2013.
[415] Meran, **a.g.e.**, s. 44.

faaliyetlerinde bulunur, bu amaçla bilgi toplar, değerlendirir, yetkili mercilere veya kullanma alanına ulaştırır. Bu görevlerin yerine getirilmesine yönelik olarak, 4.12.2004 tarihli ve 5271 sayılı CMK'nın, casusluk suçları hariç, 250 nci maddesinin birinci fıkrasının (a), (b) ve (c) bentlerinde yazılı suçların işlenmesinin önlenmesi amacıyla, telekomünikasyon yoluyla yapılan iletişim tespit edilebilir, dinlenebilir, sinyal bilgileri değerlendirilebilir ve kayda alınabilir.

Jandarma; emniyet ve asayiş ile kamu düzenini sağlamak, korumak ve kollamak, kaçakçılığı men, takip ve tahkik etmek, suç işlenmesini önlemek için gerekli tedbirleri almak ve uygulamak, ceza infaz kurumları ve tutukevlerinin dış korunmalarını yapmaya ilişkin görevlerini[416] yerine getirirken önleyici ve koruyucu tedbirleri almak üzere, sadece kendi sorumluluk alanında 4.12.2004 tarihli ve 5271 sayılı CMK'nın, casusluk suçları hariç, 250 nci maddesinin birinci fıkrasının (a), (b) ve (c) bentlerinde yazılı suçların işlenmesinin önlenmesi amacıyla, telekomünikasyon yoluyla yapılan iletişimi tespit edebilir, dinleyebilir, sinyal bilgilerini değerlendirebilir ve kayda alabilir.

Milli İstihbarat Teşkilatı tarafından ise 2937 sayılı Kanunun 4. maddesinde belirtilen görevlerin[417] yerine getirilmesi amacıyla Anayasanın 2

---

[416] Jandarmanın genel olarak görevleri, 2803 sayılı Kanunun 7. maddesinde şu şekilde düzenlenmiştir: "***Jandarmanın genel olarak görevleri***
Madde 7 – *Jandarmanın sorumluluk alanlarında genel olarak görevleri şunlardır.*
a) Mülki görevleri;
Emniyet ve asayiş ile kamu düzenini sağlamak, korumak ve kollamak, kaçakçılığı men, takip ve tahkik etmek, suç işlenmesini önlemek için gerekli tedbirleri almak ve uygulamak, ceza infaz kurumları ve tutukevlerinin dış korunmalarını yapmak.
b) Adli görevleri;
İşlenmiş suçlarla ilgili olarak kanunlarda belirtilen işlemleri yapmak ve bunlara ilişkin adli hizmetleri yerine getirmek.
c) Askeri görevleri;
Askeri kanun ve nizamların gereği görevlerle Genelkurmay Başkanlığınca verilen görevleri yapmak.
d) Diğer görevleri;
Yukarıda belirtilen görevler dışında kalan ve diğer kanun ve nizam hükümlerinin icrası ile bunlara dayalı emir ve kararlarla Jandarmaya verilen görevleri yapmak".

[417] *"**Milli İstihbarat Teşkilatının görevleri***
Madde 4 *– Milli İstihbarat Teşkilatının görevleri şunlardır;*
a) Türkiye Cumhuriyetinin ülkesi ve milleti ile bütünlüğüne, varlığına, bağımsızlığına, güvenligine, Anayasal düzenine ve milli gücünü meydana getiren bütün unsurlarına karşı içten ve dıştan yöneltilen mevcut ve muhtemel faaliyetler hakkında milli güvenlik istihbaratını Devlet çapında oluşturmak ve bu

nci maddesinde belirtilen temel niteliklere ve demokratik hukuk devletine yönelik ciddi bir tehlikenin varlığı halinde Devlet güvenliğinin sağlanması, casusluk faaliyetlerinin ortaya çıkarılması, Devlet sırrının ifşasının tespiti ve terörist faaliyetlerin önlenmesine ilişkin olarak, telekomünikasyon yoluyla yapılan iletişim tespit edilebilir, dinlenebilir, sinyal bilgileri değerlendirilebilir ve kayda alınabilir.

Önleme amaçlı iletişimin denetlenmesi tedbirinin hakkında uygulanabileceği suçlar açısından 2559 sayılı Kanun ve 2803 sayılı Kanun CMK'nın 250. maddesine atıf yapmıştır. Ancak, 6352 sayılı Kanunun[418] 105. maddesi ile CMK'nın 250. maddesi yürürlükten kaldırılmıştır. Yürürlükten kaldırılan 250. maddenin birinci fıkrası şu şekildeydi:

"(1) Türk Ceza Kanununda yer alan;

a) Örgüt faaliyeti çerçevesinde işlenen uyuşturucu veya uyarıcı madde imal ve ticareti suçu,

b) Haksız ekonomik çıkar sağlamak amacıyla kurulmuş bir örgütün faaliyeti çerçevesinde cebir ve tehdit uygulanarak işlenen suçlar,

c) İkinci Kitap Dördüncü Kısmın Dört, Beş, Altı ve Yedinci Bölümünde tanımlanan suçlar (305, 318, 319, 323, 324, 325 ve 332 nci maddeler hariç),

---

istihbaratı Cumhurbaşkanı, Başbakan, Genelkurmay Başkanı, Milli Güvenlik Kurulu Genel Sekreteri ile gerekli kuruluşlara ulaştırmak.
b) Devletin milli güvenlik siyasetiyle ilgili planların hazırlanması ve yürütülmesinde; Cumhurbaşkanı, Başbakan, Genelkurmay Başkanı, Milli Güvenlik Kurulu Genel Sekreteri ile ilgili bakanlıkların istihbarat istek ve ihtiyaçlarını karşılamak.
c) Kamu kurum ve kuruluşlarının istihbarat faaliyetlerinin yönlendirilmesi için Milli Güvenlik Kurulu ve Başbakana tekliflerde bulunmak.
d) Kamu kurum ve kuruluşlarının istihbarat ve istihbarata karşı koyma faaliyetlerine teknik konularda müşavirlik yapmak ve koordinasyonun sağlanmasında yardımcı olmak.
e) Genelkurmay Başkanlığınca Silahlı Kuvvetler için lüzum görülecek haber ve istihbaratı, yapılacak protokole göre Genelkurmay Başkanlığına ulaştırmak.
f) Milli Güvenlik Kurulunda belirlenecek diğer görevleri yapmak.
g) İstihbarata karşı koymak.
Milli İstihbarat Teşkilatına bu görevler dışında görev verilemez ve bu teşkilat Devletin güvenliği ile ilgili istihbarat hizmetlerinden başka hizmet istikametlerine yöneltilemez. Milli İstihbarat Teşkilatı birimlerinin görev, yetki ve sorumlulukları Başbakanca onaylanacak bir yönetmelikte belirtilir".

[418] Yargı Hizmetlerinin Etkinleştirilmesi Amacıyla Bazı Kanunlarda Değişiklik Yapılması ve Basın Yayın Yoluyla İşlenen Suçlara İlişkin Dava ve Cezaların Ertelenmesi Hakkında Kanun. RG. 05.07.2012, 28344.

Dolayısıyla açılan davalar; Adalet Bakanlığının teklifi üzerine Hâkimler ve Savcılar Yüksek Kurulunca yargı çevresi birden çok ili kapsayacak şekilde belirlenecek illerde görevlendirilecek ağır ceza mahkemelerinde görülür".

6352 sayılı Kanunun geçici 2. maddesinin yedinci fıkrasında, *"Mevzuatta Ceza Muhakemesi Kanununun 250 nci maddesinin birinci fıkrasına göre kurulan ağır ceza mahkemelerine yapılmış olan atıflar, Terörle Mücadele Kanununun 10 uncu maddesinin birinci fıkrasında belirtilen ağır ceza mahkemelerine yapılmış sayılır"* hükmüne yer verilmiş; anılan suçlar Terörle Mücadele Kanununun 10. maddesinin dördüncü fıkrasında tekrar düzenlenmiş ve suçtan kaynaklanan malvarlığı değerini aklama suçu da bu suçlar arasına eklenmiştir. Bu çerçevede, 6352 sayılı Kanunun geçici 2. maddesinde yer alan atfın, mülga 250. maddede yer alan suçlar açısından da Terörle Mücadele Kanununun 10. maddesinin dördüncü fıkrasında yer alan suçlara yapılmış olduğunun kabulü gerekir. Bu çerçevede polis ve jandarma, önleme amaçlı iletişimin denetlenmesini ancak Terörle Mücadele Kanununun 10. maddesinin dördüncü fıkrasında yer alan suçlar açısından gerçekleştirebilecektir.

Adli amaçlı iletişimin denetlenmesi tedbirinin uygulanabilmesi için kanunda belirlenen suçların işlendiğine ilişkin kuvvetli şüphe sebeplerinin varlığı ve başka suretle delil elde edilmesi imkanının bulunmaması gerekir. Önleme amaçlı iletişimin denetlenmesi durumunda ise bir suçtan dolayı iletişim denetlenmediği için suç işlendiğine ilişkin kuvvetli şüphe sebeplerinin aranması da söz konusu olamaz[419]. Ancak, önleme amaçlı iletişimin denetlenmesinin nedenini oluşturan gerekçelerin yeterli açıklıkta olması gerekir. Basit tahminlere dayalı olarak önleme amaçlı iletişim denetlenememelidir[420]. Başka suretle delil elde edilmesi imkanının bulunmamasına ilişkin şart ise önleme amaçlı iletişimin denetlenmesi açısından öngörülmemiştir. Bu nedenle bu şartın önleme amaçlı iletişimin denetlenmesi tedbiri açısından da aranması gerektiği söylenemez.

---

[419] Taşkın, **a.g.e.**, s. 206.
[420] Yüksel, **a.g.e.**, s. 175. Yokuş Sevük, **a.g.m.**, s. 55.

3. Denetlemenin Hakim Kararı İle Yapılması

Önleme amaçlı iletişimin denetlenmesinin yapılabilmesi hakim kararını gerektirmektedir. Kural olarak, hakim kararı olmaksızın iletişiminin önleme amaçlı denetlenmesi mümkün değildir. İstisnaen gecikmesinde sakınca bulunan hallerde kanunla yetkili kılınmış merciin yazılı emri ile internet iletişimi denetlenebilir. Polisin denetim yetkisi açısından Emniyet Genel Müdürü veya İstihbarat Dairesi Başkanının; jandarmanın yetkisi açısından Jandarma Genel Komutanı veya istihbarat başkanının; Milli İstihbarat Teşkilatı açısından ise MİT Müsteşarı veya yardımcısının yazılı emri gerekir. Gecikmesinde sakınca bulunan hallerde verilen yazılı emir, yirmidört saat içinde yetkili ve görevli hakimin onayına sunulur. Hakim, kararını en geç yirmidört saat içinde verir. Sürenin dolması veya hakim tarafından aksine karar verilmesi halinde tedbir derhal kaldırılır. Bu halde dinlemenin içeriğine ilişkin kayıtlar en geç on gün içinde yok edilir; durum bir tutanakla tespit olunur ve bu tutanak denetimde ibraz edilmek üzere muhafaza edilir.

İletişimin Tespiti Yönetmeliğine göre "*gecikmesinde sakınca bulunan hal"*, derhal işlem yapılmadığı takdirde suçun iz, eser, emare ve delillerinin kaybolması veya şüphelinin kaçması veya kimliğinin saptanamaması olasılığının ortaya çıkması hali olarak tanımlanmıştır.

Önleme amaçlı iletişimin denetlenmesi konusunda yetkili ve görevli hakim, ilgili kurumların talepte bulunan biriminin bulunduğu yer itibariyle yetkili olan ve Terörle Mücadele Kanununun 10. maddesine göre kurulan ağır ceza mahkemesinin üyesidir.

İletişimin tespiti, dinlenmesi, sinyal bilgilerinin değerlendirilmesi ve kayda alınmasına dair hakim kararında ve yetkili merciler tarafından verilen yazılı emirlerde; hakkında tedbir uygulanacak kişinin kimliği, iletişim aracının türü, kullandığı telefon numaraları veya iletişim bağlantısını tespite imkan veren kodundan belirlenebilenler, tedbirin türü, kapsamı ve süresi, tedbire başvurulmasını gerektiren nedenler, yazılı emrin verildiği tarih ve saate ilişkin bilgilerin bulunması gerekir. Jandarmanın sorumluluk alanına ilişkin olarak verilen kararlar ile yazılı emirlerde sorumluluk alanına ilişkin bilgi ve belgelerin de yer alması gerekir.

4. Denetim Kapsamında Elde Edilen Bilgilerin Başka Amaç İçin Kullanılamayacağı, Gizliliği ve Yok Edilmesi

Önleme amaçlı iletişimin denetlenmesi tedbirinin uygulanması ile birlikte elde edilen kayıt ve bilgiler, 2559 sayılı Polis Vazife ve Selahiyet Kanununun ek 7 nci maddesi, 2803 sayılı Jandarma Teşkilat, Görev ve Yetkileri Kanununun ek 5 inci maddesi ve 2937 sayılı Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanununun 6 ncı maddesinde belirtilen amaçlar dışında kullanılamaz. Söz konusu Kanunlarda internet iletişiminin denetlenmesinin önleme amaçlı yerine getirilmesi düzenlenmiştir. Bu nedenle, önleme amaçlı denetim sonucu elde edilen kayıt ve bilgilerin delil olarak adli amaçlı kullanılması da mümkün gözükmemektedir[421].

Önleme amaçlı iletişimin denetlenmesinde bir diğer önemli ilke, elde edilen bilgi, belge ve kayıtların saklanmasında ve korunmasında gizlilik ilkesinin esas olmasıdır. Gizlilik ilkesine uyulmaması cezai sorumluluk doğurur.

Tedbir sonucu elde edilen kayıt ve bilgilerin başka bir amaç için kullanılmasının önüne geçilmesi amacıyla belli bir süre içerisinde yok edilmesi gerekir. Bu esastan hareketle İletişimin Tespiti Yönetmeliğinde, uygulanan tedbirin sona ermesi, gecikmesinde sakınca bulunan hallerde verilen yazılı emir hakkında hakim tarafından aksine karar verilmesi ya da yazılı emir hakkında yirmidört saat içinde hakim onayının alınamaması hallerinde, kararın veya yazılı emrin uygulanmasına Başkanlık tarafından derhal son verileceği öngörülmüştür. Ayrıca, dinlemenin içeriğine ilişkin kayıtların ilgili kurumların en üst amirinin ve bu kayıtların TİB'de de tutulması halinde Başkanın denetimi altında en geç on gün içinde yok edilmesi gerekir. Durum bir tutanakla tespit olunur ve bu tutanak denetimlerde ibraz edilmek üzere muhafaza edilir.

---

[421] Yüksel, **a.g.e.**, s. 197.

5. Önleme Amaçlı İletişimin Denetlenmesinde Yetkili Kurumlar

Önleme amaçlı iletişimin önlenmesi tedbirine ilişkin hakim kararları ve yazılı emirlerin yerine getirilmesinde Emniyet Genel Müdürlüğü, Jandarma Genel Komutanlığı ve Milli İstihbarat Teşkilatı yetkili kılınmıştır. Ancak her bir kuruma kendi başına önleme amaçlı denetim yapma yetkisi verilmemiştir. Bu tedbirin tek elden yürütülmesi ve denetiminin sağlanabilmesi amacıyla Telekomünikasyoın İletişim Başkanlığı yetkili kılınmıştır[422]. Şu halde, önleme amaçlı iletişimin önlenmesi tedbirinin uygulanmasında tek yetkili Kurum TİB'dir. Başkanlık, bir Başkan ile daire başkanlıklarından oluşmaktadır. Başkanlıkta; Milli İstihbarat Teşkilatı, Emniyet Genel Müdürlüğü ve Jandarma Genel Komutanlığının ilgili birimlerinden birer temsilci bulundurulmaktadır.

İletişimin denetlenmesine ilişkin hakim kararları ve yazılı emirler işletmecilere gönderilemez. Kararlar ve yazılı emirler ile bunların içeriği Başkanlığın belirleyeceği şekilde elektronik ortamda ilgili kurumlar tarafından Başkanlığa gönderilir. Kararlar ile, yapılan inceleme sonucunda İletişimin Tespiti Yönetmeliğine uygun olduğu tespit edilen yazılı emirler, ilgili kurum görevlilerince Başkanlığın koordine ve nezaretinde yerine getirilir. İşlemin başlatıldığı ve bitirildiği tarih ve saat ile işlemi yapanın kimliği bir tutanakla saptanır. İletişimin Tespiti Yönetmeliğine aykırı biçimde verilen yazılı emirler TİB tarafından yerine getirilmez.

Tedbir hakkında Emniyet Genel Müdürlüğü, Jandarma Genel Komutanlığı ve Milli İstihbarat Teşkilatının yaptığı iş ve işlemlere ilişkin bir denetim mekanizması öngörülmüştür. Emniyet Genel Müdürlüğünün, İletişimin Tespiti Yönetmeliğinde yer alan faaliyetlerle alakalı kendi birimlerindeki işlemlerine ilişkin denetimi, sıralı kurum amirleri ile Emniyet Genel Müdürlüğü ve İçişleri Bakanlığının teftiş elemanları tarafından; Jandarma Genel Komutanlığının denetimi, sıralı kurum amirleri ile Jandarma Genel Komutanlığı ve İçişleri Bakanlığının teftiş elemanları tarafından; Milli İstihbarat Teşkilatı Müsteşarlığının denetimi sıralı kurum amirleri ve Başbakanlık teftiş elemanları tarafından yapılmaktadır. Başbakanın özel

[422] Taşkın, **a.g.e.**, s. 66-67. Meran, **a.g.e.**, s. 37.

olarak yetkilendireceği kişi veya komisyon tarafından denetim yapılabilmesine ilişkin 5397 sayılı Bazı Kanunlarda Değişiklik Yapılmasına İlişkin Kanunda yer alan hükümler Anayasa Mahkemesi tarafından iptal edilmiştir[423].

6. Denetimin Uygulanabileceği Süre, Yer ve Kişi Sınırı

Önleme amaçlı iletişimin denetlenmesine ilişkin kararlar en fazla üç ay için verilebilir. Bu süre, aynı usulle üçer ayı geçmeyecek şekilde en fazla üç defa uzatılabilir. Ancak, terör örgütlerinin faaliyeti çerçevesinde devam eden tehlikelere ilişkin olarak gerekli görülmesi halinde, hakim tarafından üç aydan fazla olmamak üzere sürenin müteaddit defalar uzatılmasına karar verilebilir.

Tedbirin uygulanması yer açısından da sınırlıdır. Tüm ülkeyi kapsayacak şekilde iletişimin denetlenmesi tedbirinin uygulanması mümkün değildir. Önleme amaçlı iletişimin denetlenmesi konusunda yetkili hakim, ancak kendi yetki alanına ilişkin tedbir uygulayabilir. Hakimin yetki alanı dışında iletişimin denetlenmesi tedbirini uygulaması, yetki alanını aşma olarak değerlendirilmektedir[424].

Adli amaçlı iletişimin denetlenmesi tedbiri açısından bazı kişiler arasındaki iletişimin kayıt altına alınması mümkün değildir[425]. Örneğin, şüpheli veya sanığın tanıklıktan çekinebilecek kişilerle arasındaki iletişimi kayda alınamaz. Kayda alma gerçekleştikten sonra bu durumun anlaşılması hâlinde, alınan kayıtlar derhal yok edilir. Bu tür sınırlandırmalar, önleme amaçlı iletişimin denetlenmesi tedbiri açısından öngörülmemiştir. Bu nedenle önleme amaçlı olarak herkesin iletişimi, kişiler arası bir sınırlandırma da bulunmaksızın denetlenebilir[426]. Milletvekili, hakim - savcı, vali veya bürokrat, asker ya da sivil farketmeksizin herkesin internet iletişimi önleme amaçlı denetlenebilir[427].

---

[423] AYM, 29.01.2009, E. 2005/85, K. 2009/15, RG. 03.04.2009, 27189.
[424] Yüksel, **a.g.e.**, s. 177. Aksi yönde görüş belirten yazarlar da bulunmaktadır. Bkz. Meran, **a.g.e.**, s. 19-20.
[425] Meran, **a.g.e.**, s. 123.
[426] Yüksel, **a.g.e.**, s. 166.
[427] Taşkın, **a.g.e.**, s. 198.

Kişi açısından öngörülen bir diğer sınırlandırma, önlenmesi öngörülen suçu işleme şüphesi bulunan kişilerin iletişiminin denetlenebileceğidir. Bir diğer deyişle, kişiler açısından genel nitelikli veya geniş kitleleri kapsayan bir iletişimin denetlenmesi kararı verilemez[428].

7. Cezai Sorumluluk

2559 sayılı Kanun, 2803 sayılı Kanun ve 2937 sayılı Kanunda yer alan usul ve esaslara aykırı bir şekilde iletişimin denetlenmesi cezai yaptırıma bağlanmıştır. TCK'da haberleşmenin gizliliğini ihlal (md. 132), kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması (md. 133), özel hayatın gizliliğini ihlal (md. 134), kişisel verilerin kaydedilmesi (md. 135), verileri hukuka aykırı olarak verme veya ele geçirme (md. 136) ve verileri yok etmeme (md. 138) birer suç olarak düzenlenmiştir.

Önleme amaçlı iletişimin denetlenmesi tedbiri sonucunda elde edilen kayıtların görev sırasında veya görevden dolayı işlenmiş olsa bile kanunda öngörülen amaçlar dışında kullanılması veya elde edilen bilgi ve kayıtların saklanmasında ve korunmasında gizlilik ilkesine uyulmaması durumunda Cumhuriyet savcılarınca doğrudan soruşturma yapılacaktır.

Ç. 5651 Sayılı Kanun Çerçevesinde internet İletişiminin İzlenmesi

TİB tarafında internet üzerinde yapılacak izleme, 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunun 10. maddesinin dördüncü fıkrasında düzenlenmiştir. Buna göre TİB, internet ortamında yapılan yayınların içeriklerini izleyerek, bu Kanun kapsamına giren suçların işlendiğinin tespiti halinde, bu yayınlara erişimin engellenmesine yönelik olarak bu Kanunda öngörülen tedbirleri alma (b bendi), internet ortamında yapılan yayınların içeriklerinin izlenmesinin hangi seviye, zaman ve şekilde yapılacağını belirleme (c bendi), internet ortamındaki yayınların izlenmesi suretiyle Kanunun 8. maddesinin birinci fıkrasında sayılan suçların

[428] Taşkın, **a.g.e.**, s. 190.

işlenmesini önlemek için izleme ve bilgi ihbar merkezi dahil, gerekli her türlü teknik altyapıyı kurma veya kurdurma, bu altyapıyı işletme veya işletilmesini sağlama (d bendi) ve internet ortamında herkese açık çeşitli servislerde yapılacak filtreleme, perdeleme ve izleme esaslarına göre donanım üretilmesi veya yazılım yapılmasına ilişkin asgari kriterleri belirleme (e bendi) yetkisini haiz kılınmıştır.

Bu düzenlemeler TİB'e geniş bir çerçevede internet iletişimini izleme yetkisi vermektedir. TİB'in, bu düzenlemelere dayanarak kişisel haberleşme niteliğindeki "*e-posta"* ve "*Facebook"* gibi sosyal paylaşım siteleri üzerinden yapılan iletişimi de izleyebileceği ileri sürülmekte ve bu husus eleştirilmektedir[429]. Ancak, TİB'e internet iletişiminin izlenmesi açısından verilen bu yetki kişisel iletişimin izlenmesine ilişkin bir yetki değildir. 5651 sayılı Kanunda "*internet ortamı"* kavramı tanımlanırken "*haberleşme"*, kavramın kapsamı dışında bırakılmıştır. Haberleşme kavramı, hem internet dışında kalan hem de internet ortamında yapılan kişisel haberleşmeyi kapsamaktadır. Bu durumda örneğin, "*msn"* üzerinden yapılan bir görüşme veya *e-mail* ile yapılan haberleşme, 5651 sayılı Kanun kapsamında internet ortamını ifade etmeyeceği için bu tür kişisel haberleşmeler üzerinde izleme yapılması 5651 sayılı Kanun kapsamında mümkün değildir. 5651 sayılı Kanun kapsamında TİB'in internet iletişimini izlemesi kişisel haberleşme dışında kalan herkese açık internet ortamında gerçekleştirilebileceği için bu izlemenin, önleme amaçlı internet iletişiminin denetlenmesi olarak düşünülmesi mümkün değildir. Zaten bu alan herkese açıktır ve kişisel haberleşme niteliğinde değildir. Bu nedenle TİB, suçların tespiti ve takibi açısından herkese açık olan internet iletişimini izleyebilir; hatta izlemesi gerekir.

---

[429] Murat Volkan Dülger, "İnternet İletişiminin Engellenmesinin Hukuki Açıdan Değerlendirilmesi ve 5651 Sayılı Yasayla Getirilen Düzenleme", **İstanbul Barosu Dergisi**, Cilt. 81, Sayı. 2007/4, 2007, http://www.dulger.av.tr/assets/pdf/interneterisimininengellenmesi.pdf, 14.12.2012, s. 25.

IV. ULUSAL SİBER GÜVENLİĞİN SAĞLANMASI

Ulusal siber güvenlik, 21. Yüzyıl dünyasında ulusal güvenliğin önemli alt bileşenlerinden biri haline gelmiştir. Artık, neredeyse ulusal siber güvenliğin önemli bir unsur olarak ele alınmadığı ulusal güvenlik belgesi kalmamıştır. Ayrıca, her geçen gün ulusal siber güvenlik kavramı biçim değiştirmektedir. Günümüzde ulusal siber güvenlik, sadece siber saldırılara karşı koyma yaklaşımı olarak ele alınmamakta; internetin devletlerin siyasi sistemlerine, ulusal menfaat, değer ve bütünlüklerine karşı kullanılmasının önlenmesine yönelik politika ve stratejiler de geliştirilmektedir. Bu bölümde konu, devletlerin siber saldırılara karşı koyma ve ulus-devlet bütünlüğünü sağlama bakış açıları açısından siber güvenlik olmak üzere iki ayrı ana başlık altında ele alınmıştır.

Her devletin ulusal güvenlik ve ulusal siber güvenlik algısı farklıdır. Bu farklılıklar aşağıda yeri geldikçe incelenecektir. Devletlerin bu konuya yaklaşımı farklılık göstermekle birlikte özellikle ABD, NATO, Çin, Rusya, AB ve Avrupa ülkelerinin ulusal siber güvenlik politika ve stratejilerinin oldukça geniş, etkili ve müdahale içerikli bir nitelik gösterdiği söylenebilir[430].

A. Ulusal Siber Güvenlik

Siber tehditler ulusal güvenliğe risk oluşturma boyutuna göre "*siber güvenlik" (cyber security)* veya "*ulusal siber güvenlik" (national cyber security)* kavramları çerçevesinde ele alınabilir. Her siber tehdit, saldırı veya suç ulusal siber güvenlik tehdit unsuru olarak ele alınamaz. Siber güvenlik, siber ortamda kişi, kurum ve kuruluşların varlığını korumak amacıyla geliştirilen plan, program, strateji ve uygulamalar bütünlüğü[431]; ulusal siber güvenlik ise bir devletin, her ne şekilde olursa olsun bilişim sistemleri kullanılarak ulusal güvenliğine tehdit oluşturan faaliyetlere karşı geliştirdiği politika, strateji ve uygulamalar bütünlüğü olarak tanımlanabilir. Siber

---

[430] Muharrem Gürkaynak, Adem Ali İren, "Reel Dünyada Sanal Açmaz: Siber Alanda Uluslararası İlişkiler", **Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi**, C. 16, S. 2, 2011, s. 264.

[431] Mustafa Ünver, Cafer Canbay, Hüseyin Burhan Özkan, **Kritik Altyapıların Korunması**, BTK, Mayıs 2010, s. 1-2.

güvenlik kavramı, teknik anlamda (technical computer security) ele alındığında ise bir bilişim sisteminin erişilebilirlik (availability), bütünlük (integrity) ve gizlilik (confidentiality) özelliklerini ifade etmektedir[432].

Ulusal siber güvenlik konusunun incelendiği çalışmalarda genellikle bu alanda kullanılan kavramların tanımlanması yoluna gidilmektedir. Ancak, tanımlamadaki zorluk nedeniyle kavramlar arasındaki ilişki net bir şekilde ortaya konulamamaktadır. Burada da aynı yöntem izlenmiş; ancak kavramlar arasındaki belirsizlik olabildiğince netleştirilmeye çalışılmıştır. Ayrıca, mümkün olduğunca hukuksal tahlil yöntemine başvurulacaktır.

1. Siber Saldırı

"Siber saldırı" (cyber attack), öz bir ifade ile amacı her ne olursa olsun bilişim sistemlerinin işleyişini engelleme, bozma veya sistemdeki verileri edinme veya kullanmaya yönelik siber ortamda yapılan saldırılar olarak tanımlanabilir. Bir siber saldırı, bir bilgi sisteminin erişilebilirlik, bütünlük ve gizlilik özelliklerine etki etmeyi amaçlar. Siber saldırı hukukta karşılığını "*siber suç" (cyber crime)* kavramında bulmaktadır. Ulusal güvenliği tehdit boyutuyla siber saldırı ise kamusal düzenin işleyişini bozmak amacıyla, sistematize bir şekilde ve ideolojik, ekonomik, sosyal, kültürel veya siyasi gerekçelerle bir devletin kamu kurumlarının, özel sektör kuruluşlarının veya kişilerin ciddi bir zarar ortaya çıkarabilecek şekilde bilişim sistemlerinin engellenmesi, bozulması veya verilerin edinilmesi ya da kullanılmasını sağlamaya yönelik faaliyetler olarak ele alınabilir. Ulusal güvenliği tehdit eden saldırılar da siber suç kavramına girmektedir. Hatta bu tür siber suçların yaptırımları diğer siber suçlara göre daha ağır olabilmektedir.

Siber saldırılar kişilerden, organize suç örgütleri ve terör örgütlerinden veya devletlerden[433] gelebilmektedir[434]. Siber saldırılar, "*siber silah" (cyber weapon)* olarak adlandırılan araçlar aracılığıyla işlenmektedir. DoS (Denial of

---

[432] Helen Nissenbaum, "Where Computer Securtiy Meets National Security", **Ethics and Information Technology**, 7, 2005, s. 63.
[433] Jamal Henry, **Reducing the Threat of State-to-State Cyber Attack Against Critical Infrastructure Through International Norms and Agreements**, CISSM Working Paper, 2010, s. 2.
[434] Wilson, **a.g.e.**, s. 1.

Service) veya DDoS (Distributed Denial of Service) saldırıları[435], trojan, worm, spam, virus ve yazılım bombası (logic bomb) gibi kötü amaçlı yazılımlar (malicious code) siber silah olarak kullanılabilir[436]. Teknolojinin gelişimi ile birlikte her geçen gün yeni ve daha etkili siber silahlar üretilmektedir.

Bir siber saldırı, bilgisayarların donanım veya yazılım güvenliğine zarar verme, sistemin işleyişini değiştirme veya veri çalma ya da veriye zarar verme şeklinde gerçekleştirilebilmektedir[437]. Bilişim sistemlerine sadece sanal ortamda yapılan saldırıları değil; aynı zamanda fiziksel ortamda yapılan saldırıları da siber saldırı olarak değerlendirmek gerekir. Elektromagnetik enerji gücü ile yapılan saldırılar da buna dahildir.

Günümüzde ulusal güvenliği tehdit edebilecek siber saldırılar kamu kurumlarının internet sitelerini, banka hizmetlerini, enerji ve su şebekelerini, ulaşım altyapısını ve hizmetlerini, hava trafik sistemlerini, iletişim altyapısını ve askeri silah sistemlerini, kısaca ülkenin politik, askeri ve ekonomik varlığını ciddi derecede tehlikeye sokabilecek niteliğe sahip bir boyuta gelmiştir. Siber saldırıların gerçekleştirilmesinde internetin katkısı ise küçümsenemeyecek derecededir. Siber saldırılar, kritik bilişim altyapılarını (critical information infrastructure) da hedef alabilir. USA Patriot Act'da "kritik altyapı", zarar görmesi halinde güvenlik, ulusal ekonomik güvenlik, ulusal kamu sağlığı veya güvenliği üzerinde olumsuz etki doğurabilecek Birleşik Devletler için kritik derecede önem taşıyan fiziksel veya sanal sistem ve varlıklar olarak tanımlanmıştır[438].

---

[435] DDoS, bir bilişim sistemine zarar vermek amacıyla yönlendirilmiş bilgisayarlarla organize bir şekilde bir bilişim sistemine yoğun bir internet trafik akışı sağlayarak sistemin etkisiz hale getirilmesi olarak tanımlanabilir. Saldırıda kullanılan bilgisayarlar botnet ve zombie içerisinde yer alan bilgisayarlar olabileceği gibi kişiler gönüllü olarak bilgisayarlarına zararlı yazılımları da yükleyerek saldırıya katılabilirler. Örneğin, organize bir şekilde kişilerin hedef aldıkları bir internet sitesini birlikte ve aynı anda yenilemeleri basit bir DDoS saldırısı olarak değerlendirilebilir. Jose Nazario, "Politically Motivated Denial of Service Attacks", http://static.ow.ly/docs/12_NAZARIO%20Politically%20Motivated%20DDoS_iWO.pdf, s. 1.

[436] Gürkaynak / İren, **a.g.m.**, s. 269-275.

[437] Wilson, **a.g.e.**, s. 3.

[438] Henry, **a.g.e.**, s. 1.

2. Siber Savaş

a. Tanım

Genel olarak savaş kavramının tanımlanması ve savaşın ortaya çıkardığı uluslararası hukuksal sorunlar siber savaş kavramı söz konusu olduğunda da karşımıza çıkmaktadır. Ancak, siber savaş kavramının genel olarak savaş kavramından farklı yönleri ve özellikleri bulunmaktadır. Bu nedenle, siber savaş kavramı tanımlanmaya ve hukuksal bir çerçeveye oturtulmaya ihtiyaç duymaktadır. Doktrinde "*siber savaş" (cyber warfare),* devletlerin bilişim sistemlerini korumak için siber ortamda yaptıkları savunma ve saldırı faaliyetlerinin bütünü olarak tanımlanmaktadır[439]. Siber savaş, devletler arasında siber ortamda yürütülen mücadele olarak da tanımlanıp, devlet dışı aktörlerin siber saldırıları siber savaş kavramı dışında tutulabilir. Bu tanımlamalar siber savaş kavramını oldukça geniş bir çerçeveye oturtmaktadır. Bu tanımlamalar siber saldırı içermeyen propaganda ve istihbarat toplama gibi eylemleri de siber savaş kavramı altında ele almaktadır. Ancak, bu tür eylemler fiziksel bir saldırı içermediğinden savaş kavramı altında ele alınmaya yatkın değildir.

Devletler arasında fiziksel bir savaş sürerken aynı zamanda siber ortamda da savaş yürütülmesi doğrudan savaş ve siber savaş ile ilgili bir konudur. Böyle bir durumda ortaya çıkan çatışma tereddütsüz aynı zamanda siber savaş olarak nitelendirilebilir. Fiziksel ortamda savaş yokken sadece siber ortamda mücadele yürütülmesi durumu ise siber savaş kavramı altında ele alınmaya çok uygun değildir. Ancak, bu durumda siber ortamda yürütülen mücadele siber saldırıları da içeriyorsa ve bu saldırılar ciddi fiziksel zararlar ortaya çıkarıyorsa, bu durumun bir savaş nedeni oluşturması veya bir savaş hali olarak kabulü mümkün gözükmektedir. Devletler arasında fiziksel veya siber savaşın ortaya çıkması durumunda uluslararası savaş hukuku ve insancıl hukuk (international humanitarian law) kuralları devreye gireceği için,

[439] Gürkaynak / İren, **a.g.m.**, s. 268.

bu kurallar bu süreçte yapılan siber saldırılar için de uygulama imkanı bulacaktır[440].

Devletlerin siber ortamda yürüttükleri mücadelenin siber savaş mı yoksa siber terörizm mi oluşturacağı konusu çoğu zaman oldukça muğlaktır. Bu nedenle, "savaş" ile "terörizm" kavramlarında olduğu gibi "siber savaş" ile "siber terörizm" kavramları arasındaki farkın da net bir şekilde ortaya konulması oldukça zordur[441]. Bazı siber saldırıların niteliği, devletler tarafından yapılsa bile yapılan siber saldırıların siber savaş kavramı altında ele alınmasını engellemekte; bu tür saldırıları siber terörizm niteliğine büründürmektedir. Özellikle örneğin, uçak bilişim sistemlerine yapılan siber saldırılar ile masum insanların öldürülmesi; ambulans, polis ve itfaiye gibi hizmetlerin çağrı merkezlerine yapılan siber saldırılar ile insanların acil yardım hizmetlerinden mahrum bırakılması; elektrik, su, iletişim veya doğalgaz gibi hizmetlerin bilişim sistemlerine yapılan saldırılar ile insanların temel ihtiyaçlarından mahrum bırakılması, metro ve tren gibi ulaşım sistemlerine yapılan siber saldırılar ile insanların seyehat özgürlüklerinin engellenmesi gibi siber saldırıların kaynağı her ne olursa olsun siber terörizm kavramı altında ele alınması gerekir.

Devletlerin bilişim sistemlerine yapılan saldırıların devlet destekli olmaması durumu karşımıza ayrı bir tablo çıkarmaktadır. Bu olasılıkta bir savaş olgususundan bahsetmek mümkün değildir. Bu tür saldırıların siber terörizm kavramı altında ele alınması daha kolaydır. Ancak, siber saldırıların niteliği gereği kaynağını tespit etmekteki güçlük, saldırının devlet destekli olup olmadığını çoğu zaman belirsiz kılmaktadır[442].

b. Siber Savaşlar

Devletler arasında 1990'lı yıllardan günümüze siber savaş olarak nitelendirilebilecek bazı siber çatışmalar ortaya çıkmıştır. Kosova'da

---

[440] Heli Tiirmaa-Klaar, "Cyber Security Threats and Responses at Global, Nation-State, Industry and Individual Levels", Mart 2011, http://www.sciencespo.fr/ceri/sites/sciencespo.fr.ceri/files/art_htk.pdf, s. 4-5.
[441] Gürkaynak / İren, **a.g.m.**, s. 268.
[442] Wilson, **a.g.e.**, s. 1.

1990'larda savaş yıllarında internet önemli bir propaganda ve siber saldırı aracı olarak kullanılmış; bu mücadele ilk siber savaş olarak nitelendirilmiştir[443]. 1999 yılında NATO güçleri, Yugoslavya'da internet servis sağlayıcılarını kontrol altına almış ve propaganda amacıyla ülkenin internet bağlantısını kesmemiştir. Siber savaş olarak da nitelendirilebilecek bir diğer çatışma South Ossetia ve Abkhazia ile ilgili olarak 2008 yılında Rusya / Gürcistan arasında ortaya çıkan savaştır. Bu savaş, siber savaşı da beraberinde getirmiştir. Savaşta, fiziksel savaş ile siber savaş aynı anda gerçekleşmiştir. DDoS saldırıları ile Gürcistan Devlet Başkanlığı, Savunma Bakanlığı, Dışişleri Bakanlığı gibi kamu kurumlarının internet siteleri, haber siteleri ve bazı özel sektör kuruluşlarının siteleri hedef alınmıştır. Saldırılarda Rus organize suç örgütlerinin ve siber milislerinin de çok önemli etkisi olmuştur. Gürcistan, saldırılara etkin bir şekilde karşılık verememiş; Başkanın internet sitesi ABD'de yer alan Google Blog hizmet sunucularından, Savunma ve Dışişleri Bakanlığı gibi kimi bakanlıkların internet siteleri ise Estonya ve Polonya'daki kuruluşların hizmet sunucularından yayın yapabilmiştir.

ABD, Çin, İsrail, Kuzey Kore, kimi Avrupa devletleri ve Rusya gibi devletler gelişmiş siber savaş kapasitesine sahiptir[444] ve uluslararası alanda yürütülen güç mücadelesi bu alanda da kendisini göstermektedir. ABD gibi askeri sistemleri teknolojiye bağımlı devletler açısından askeri sistemlerine gelebilecek siber saldırılara karşı siber savunma kapasitesi daha fazla önem taşımaktadır[445]. Geleceğin siber dünyasında devletlerin siber savaş kapasitelerini artırmaya yönelik daha etkili politikalar geliştirecekleri ve savaşların siber savaşlardaki üstünlük ile şekilleneceğini şimdiden öngörmek mümkündür.

---

[443] Denning, **a.g.m.**, s. 239.

[444] Stephen Herzog, "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses", **Journal of Strategic Security**, Volume IV, Issue 2, 2011, s. 52.

[445] Aviv Cohen, "Cyberterrorism: Are We Legally Ready?", **The Journal of International Business & Law**, http://law.hofstra.edu/pdf/academics/journals/jibl/jibl_vol9no1_cohen_cyberterrorism.pdf, 2010, s. 9.

Aşağıdaki tabloda 1998'den günümüze kadar gerçekleşen siber savaşların bir listesi verilmiştir[446].

Tablo 9. Seçilmiş Bölgesel Siber Çatışmalar

1998	Zapatista sympathizers vs. Mexico Zapatista sympathizers vs. DOD, Frankfurt Stock Exchange Pakistan vs. India (after nuclear tests)
1999	NATO (in Kosovo) vs. Serbians (and Russians) China vs. US (bombing of Chinese Embassy in Belgrade) China vs. Taiwan India vs. Pakistan (during conflict in Kashmir) Hamas vs. Israel
2000	Azerbaijan and Turkey vs. Armenia Hezbollah vs. Israel
2001	China vs. US (after downing of US Navy EP-3 aircraft)
2005	Indonesia vs. Malaysia (dispute over Celebes Sea) China and South Korea vs. Japan (dispute over Japan war crimes) German Neo-Nazis vs. the World
2006	Muslims vs. Denmark (during furor over Muhammad cartoon)
2007	Russia vs. Estonia Israel vs. Syria (supporting air attack)
2008	Russia vs. Lithuania Russia vs. Georgia (during invasion by Russian troops)
2009	Russia vs. Kazakhstan (news agencies) North Korea vs. South Korea and US Russia vs. Kyrgyzstan
2010	WikiLeaks' US opponents (and others) vs. WikiLeaks' supporters

Tablo'da yer alan siber çatışmaların çoğunluğunun yerel nitelikli, ağırlıklı olarak sivil kaynaklı veya örtülü bir şekilde devlet destekli ve etnik çatışmalardan[447] kaynaklandığı görülmektedir[448].

Bir devlet tarafından yapılan siber saldırıların silahlı bir saldırı ve dolayısıyla bir savaş sebebi olarak kabul edilip edilemeyeceği doktrinde

---

[446] Robert S. Dudney, "Rise of the Cyber Militias", **Air Force Magazine**, 2011, http://www.airforce-magazine.com/MagazineArchive/Documents/2011/February%202011/0211cyber.pdf, 6.12.2012, s. 89.

[447] Robert Faris, Jonathan Zittrain, "Web Tactics", **Index on Censorship**, http://ioc.sagepub.com/content/38/4/90, 18.03.2013, s. 94.

[448] Yazar, siber saldırı içerisinde yer alan sivilleri *siber milis (cyber militia)* olarak nitelendirmektedir. Dudney, **a.g.m.**, s. 88. Sivillerin vatansever duygularla siber saldırı gerçekleştirmesi (patriotic hacking), siber savaş olgusunun önemli bir özelliği haline gelmiştir. Deibert / Rohozinski, **a.g.m.**, s. 54. Konu ile ilgili Batı kaynaklı eserlerin neredeyse tamamında sivillerin siber savaş içerisinde yer almasının Çin, Rusya, bazı Arap ülkeleri ve İran gibi bazı devletler tarafından teşvik edildiği her seferinde ileri sürülse de çoğu Batı devletinin sivil vatansever hackerlarının bulunduğu da bir gerçektir.

tartışılmaktadır. ABD, ülkesine karşı yapılacak bir siber saldırının savaş sebebi olacağını ilan etmiştir[449].

3. Siber Terörizm

a. Tanım

Terörizm kavramını tanımlamak oldukça güçtür. Her devletin farklı bir terörizm algısı vardır ve doktrinde ortaya konulan tanımlamalar oldukça birbirinden farklı ve geniş bir yelpaze oluşturmaktadır. Aynı güçlük siber terörizm kavramında da kendisini göstermektedir. Siber terörizm konusunda birbirinden oldukça farklı tanımlamalar yapılmaktadır. Doktrinde yapılan tanımlamalara bakıldığında "*amaç", "kullanılan araç", "politik güdü", "saldırının yöneldiği hedef", "saldırıyı düzenleyen kişi veya organizasyon", "saldırının yoğunluğu", "saldırının etkisi"* gibi unsurların etkin olduğu görülmektedir. Bir görüş, siber terörizm kavramını, klasik terörizm faaliyetlerinin bilişim sistemleri kullanılarak işlenmesi olarak tanımlamıştır[450]. Bir diğer görüşe göre siber terörizm, siyasi, ideolojik, askeri, ekonomik, sosyal veya kültürel bir amacı gerçekleştirmek için sistematik bir şekilde şiddet, tehdit, korkutma ve yıldırma yöntemi kullanarak bir toplum ve devlet üzerinde baskı kurmaya yönelik siber saldırı faaliyetleridir[451]. Bir başka tanımlamaya göre siber terörizm, bilişim teknolojileri kullanılarak topluma zarar verme veya toplumu paniğe sürükleme faaliyetleridir[452]. Denning, ayrıştırmadaki zorluğu belirtmekle birlikte "*activism", "hacktivism"* ve "*cyberterrorism"* arasında bir ayrım yapmakta ve "activismi", bir amacın gerçekleştirilmesi için internet siteleri oluşturma, yayınları e-mail ile gönderme, forum, tartışma ve sosyal paylaşım sitelerini aktif olarak kullanma, interneti takip etme gibi internetin normal ve zararsız kullanımı; "hacktivismi",

---

[449] Gürkaynak / İren, **a.g.m.**, s. 272.
[450] Mehmet Özcan, "Siber Terörizm ve Ulusal Güvenliğe Tehdit Oluşturma Boyutu", http://www.ozhankalac.info/dokumanlar/siber.pdf, 06.12.2012, s. 6.
[451] Wilson, **a.g.e.**, s. 4.
[452] Gürkaynak / İren, **a.g.m.**, s. 266.

ağır zararlar ortaya çıkarmayacak şekilde siber saldırılarda bulunulması[453]; "cyberterrorismi" ise hava trafik kontrol sistemlerine yapılan siber saldırılar ile uçakların çarpışmasının sağlanmasında olduğu gibi politik bir saik ile ölüm ve ağır ekonomik zararlar ortaya çıkarmayı amaçlayan siber saldırılarda bulunulması olarak tanımlamaktadır[454]. Bir başka görüşe göre ise siber terörizm, bilgisayar ağları kullanılarak bir devletin kritik derecede önem taşıyan elektronik sistemlerine karşı yapılan saldırılardır[455].

Yapılan tanımlamalar siber terörizmin birçok yönüne ışık tutmaktadır. Burada ayrı bir tanımlama yöntemi izlenmeden ne tür siber saldırıların "siber terörizm" faaliyeti oluşturabileceği belirlenmeye çalışılmıştır. Bu çerçevede herşeyden önce her siber saldırı, siber terörizm faaliyeti olarak değerlendirilemez. Saldırının amacı açısından, politik bir güdü içermeyen saldırılar siber terörizm kavramı dışında kalmaktadır. Ancak, saldırı politik bir güdü içermemekle birlikte kimlik hırsızlığı veya kredi kartı dolandırıcılığı gibi faaliyetlerin terör örgütleri tarafından finansal kaynak sağlama gibi bir niyetle gerçekleştirilmesi durumu bu kabulün dışında kalmaktadır. Terör örgütlerinin amaçları doğrultusunda gerçekleştirdikleri her türlü siber saldırıyı, siber terörizm kavramı altında ele almak gerekir. Diğer taraftan ortaya çıkarabileceği ağır sonuçlar göz önünde bulundurularak kritik bilişim altyapılarına yapılan saldırıları da amacını, sonucunu ve gerçekleştirenini göz önünde bulundurmaksızın siber terörizm faaliyeti kabul etmek gerekir.

Devletlerin gerçekleştirdiği siber saldırılarda, savaş hukuku kurallarının da göz önünde bulundurulması gerekir. Ancak, devletler arasında savaş yokken veya savaş olsa bile devletler tarafından siber terör saldırılarının gerçekleştirilmesi de mümkündür. Bir devlete karşı açık bir siber saldırı savaş ortaya çıkarabileceğinden veya bu saldırı uluslararası hukuk kurallarına aykırılık oluşturabileceğinden devletlerin diğer devletlere karşı açık siber saldırılar yerine gizli bir şekilde ve genellikle terör ya da organize suç örgütleri ya da siber milisleri ile birlikte siber saldırılarda bulundukları

---

[453] Örneğin, *web sit-in*. Web sit-in, aynı anda binlerce activistin bir internet sitesini ziyaret etmesi ve trafik yoğunluğundan dolayı diğer kişilerin internet sitesine erişememesi olarak tanımlanmaktadır.
[454] Denning, **a.g.m.**, s. 241. Siber terörizmin aynı yöndeki tanımlaması için bkz. Cohen, **a.g.m.**, s. 7.
[455] Herzog, **a.g.m.**, s. 52.

görülmektedir. Amacı her ne olursa olsun devletlerin bu tür saldırılarını siber terörizm kavramı altında ele almak gerekir. Diğer taraftan, devletlerin savaş halinde olması durumunda bile kritik bilişim altyapılarına siber saldırı düzenlenerek masum insanlara zarar verilmesi durumunda da siber terörizmden bahsedilecektir.

Terör örgütleri tarafından siber saldırı içermeyen, ancak faaliyetlerinin gerçekleştirilmesi için internetin kullanılmasının siber terörizm kavramı altında ele alınıp alınamayacağı tartışılabilir. Aslında bu tartışma belli bir noktaya kadar anlam kazanabilir. İster fiziksel ortamda isterse sanal ortamda olsun sonuçta terör örgütlerinin faaliyetleri terörizm faaliyetleridir. Ancak, terör örgütlerinin siber saldırı içermeyen sanal ortamdaki faaliyetlerinin de ayrıca siber terörizm kavramı altında ele alınması, terör örgütlerinin sanal ortamı kullanarak faaliyetlerini yürüttükleri alana vurgu yapması ve buna karşı da mücadele yöntemleri geliştirilmesi açısından faydalı olacaktır[456].

b. Bir Suç Olarak Siber Terörizm

Siber terör saldırılarının gerçekleştirilmesine yönelik birçok fiil siber suç tanımlamalarına girmektedir. Ancak, diğer suçlardan bağımsız bir "s*iber terörizm suçu"* tanımlamasına ihtiyaç bulunup bulunmadığı tartışılabilir. Benzer şekilde, siber terör suçlarının, terör suçları kapsamına da girebilmesi nedeniyle terör suçu kavramı dışında ayrıca bir de siber terör suçu öngörmeye gerek var mıdır? Bilişim teknolojilerindeki gelişim, siber terör tehdidinin her geçen gün artması ve ağır sonuçlar ortaya çıkarmaya başlaması ve siber terörizm kavramındaki belirsizliğin giderilebilmesi açısından ayrı bir siber terörizm suçunun tanımlanmasına ihtiyaç bulunduğu söylenebilir. İngiliz hukukunda Terörizm Kanunu (Terrorism Act 2000) ile terörizm suçu tanımlanırken aynı zamanda siber terörizm suçu da tanımlanmıştır (md. 1/2, e). Buna göre, politik, dini veya ideolojik bir amaç için elektronik sistemlere ciddi şekilde zarar verilmesi siber terörizm suçu

[456] Clive Walker, "Cyber-Terrorism: Legal Principle and Law in the United Kingdom", **Penn State Law Review**, Vol. 110: 3, s. 634.

kabul edilmiştir[457]. Benzer şekilde ülkemizde 3713 sayılı Terörle Mücadele Kanununda terör; "*cebir ve şiddet kullanarak; baskı, korkutma, yıldırma, sindirme veya tehdit yöntemlerinden biriyle, Anayasada belirtilen Cumhuriyetin niteliklerini, siyasî, hukukî, sosyal, laik, ekonomik düzeni değiştirmek, Devletin ülkesi ve milletiyle bölünmez bütünlüğünü bozmak, Türk Devletinin ve Cumhuriyetin varlığını tehlikeye düşürmek, Devlet otoritesini zaafa uğratmak veya yıkmak veya ele geçirmek, temel hak ve hürriyetleri yok etmek, Devletin iç ve dış güvenliğini, kamu düzenini veya genel sağlığı bozmak amacıyla bir örgüte mensup kişi veya kişiler tarafından girişilecek her türlü suç teşkil eden eylemler"* olarak tanımlanmış; *terör suçları* ile *terör amacı ile işlenen suçlar* ayrımı yapılarak bu tür suçlar tek tek belirlenmiştir. Bu çerçevede siber terörizm konusu olabilecek saldırılar ve internette terörizmin propagandası gibi fiiller cezai yaptırım altına alınmıştır. Örneğin, Terörle Mücadele Kanununda yapılan tanımlama çerçevesinde TCK'da yer alan "*bilişim sistemine girme" (md. 243)* ve *"sistemi engelleme, bozma, verileri yok etme veya değiştirme" (244*) suçlarının terör amacı ile işlenmesi terör suçu sayılmıştır.

Uluslararası hukuk kaynaklarına bakldığında Avrupa Konseyi Siber Suç Sözleşmesinde bir siber terörizm suçu öngörülmemiştir. Ancak, siber terörizm oluşturabilecek birçok fiil bu Sözleşme kapsamında siber suç kapsamına girebilir. Terörizm ve siber terörizm, Uluslararası Ceza Mahkemesini kuran Roma Şartı (Rome Statute)'nın kapsamı dışında bırakılmıştır. Bu nedenle siber terörizm faillerinin Uluslararası Ceza Mahkemesince yargılanması imkanı bulunmamaktadır[458].

c. Siber Terör Saldırıları

Siber terörizmin önemli bir özelliği siber saldırıların genellikle asimetrik bir yapıda tek bir ülke kaynaklı olmaması, başka ülkelerdeki bilişim

[457] Walker, **a.g.m.**, s. 632.
[458] Cohen, **a.g.m.**, s. 37.

kaynaklarından da önemli ölçüde yararlanılmasıdır[459]. Siber terör saldırılarının bir diğer özelliği bu saldırıların kaynağını bulmaktaki zorluktur. Bu zorluk, bazı devletlerin arka planda kalarak ve iz bırakmayarak siber saldırı organize etmelerini sağlayabilmektedir. Örneğin, Estonya hükümeti, Sovyetlerin Nazilerden kurtuluşunu sembolize eden bir anıtı başkent Tallinn'de mevcut yerinden bir başka yere taşımış, bu girişim Estonya'da yaşayan Rus etnik azınlığın büyük bir tepkisiyle karşılaşmıştır. Bunun üzerine patlak veren gösteriler ile birlikte 2007'nin Nisan ayında Estonya kamu kuruluşlarının, siyasi partilerin, bazı bankaların, internet servis sağlayıcıların ve parlamentonun web sitelerine yoğun bir siber saldırıda bulunulmuştur[460]. Her ne kadar saldırıların Rusya'dan geldiği yönünde açık bir delil elde edilememişse de çoğu kaynakta saldırıların Rusya ve Rus diasporasından geldiği ileri sürülmüştür[461]. Saldırılar karşısından zor durumda kalan Estonya'ya NATO ve ABD'nin verdiği teknik destek ile saldırı ciddi bir boyuta gelmeden atlatılabilmiştir[462]. Bu saldırı, ulusal siber güvenlik alanında devletler ile NATO ve AB gibi uluslararası kuruluşları ciddi önlemler almaya itmiştir.

Estonya'ya karşı yapılan siber saldırıların, siber terörizm mi yoksa siber savaş olarak mı nitelendirilmesi konusu oldukça güçtür. Saldırıların Rusya devletinden geldiğine yönelik açık delillerin ortaya konulamaması dolayısıyla devletler arası bir siber savaşın varlığından söz etmek mümkün gözükmemektedir. Yapılan saldırıların politik hedefi, yoğunluğu ve kritik bilgi

---

[459] Örneğin, 2007 yılında Estonya'ya yapılan siber saldırılarda uzaktan kontrol edilen bilgisayarlar 76 farklı ülkeden yönlendirilmiştir. Henry, **a.g.e.**, s. 1.

[460] Christian Czossek, Rain Ottis and Anna-Maria Taliharm, "Estonia After the 2007 Cyber Attacks: Legal, Strategic and Organisational Cahnges in Cyber Security", http://www.securitydefenceagenda.org/Contentnavigation/CyberInitiative/Cyberreferencelibrary/tabid/1333/Default.aspx, 10.04.2013, s. 57. Bu saldırılarda, distributed denial of service (DDoS) yöntemi kullanılmıştır. Saldırıya maruz kalan kamu internet siteleri normalde günde 1.000 ziyaretçi alırken, saldırıların başlaması ile birlikte saniyede 2.000 ziyaretçi almaya başlamıştır. Wilson, **a.g.e.**, s. 7. 1990'lardan günümüze politik içerikli yapılmış DDoS saldırılarına ilişkin bir liste için bkz. Nazario, **a.g.m.**, s. 3 vd.

[461] Herzog, **a.g.m.**, s. 53.

[462] Estonya'da söz konusu saldırıların gerçekleştiği 2007 yılında bankacılık işlemlerinin % 99'u elektronik ortamda yapılmakta ve 100'ün üzerinde e-devlet hizmeti sunulmaktaydı. Dünyada parlamento seçimlerini elektronik ortamda yapan ilk ülke olarak Estonya, Avrupa'nın bilgi ve iletişim teknolojilerinin kullanımında en önde gelen ülkelerinden biriydi. Czossek / Ottis / Taliharm, **a.g.m.**, s. 57.

sistemlerini hedef alma unsurları göz önünde bulundurularak bir siber terörizm varlığından bahsedilebilir.

İnternet, terör örgütlerine de faaliyetlerini gerçekleştirmeleri açısından muazzam imkanlar sunmuştur[463]. Terör örgütleri interneti, faaliyetlerini gerçekleştirmede dolaylı bir araç veya doğrudan bir siber silah olarak kullanabilir. İnternette propaganda, iletişim, eğitim, örgütlenme, istihbarat, silah ve bomba yapım bilgileri sunma, militan kazandırma, finansal kaynak toplama, kredi kartı dolandırıcılığı, kimlik hırsızlığı gibi ekonomik amaçlı siber suçları işleme, terör eylemleri gerçekleştirmeye yönelik talimat ve bilgiler sunma gibi faaliyetler internetin dolaylı olarak kullanımı ile[464]; devletlerin kritik öneme sahip bilgi sistemlerine ve itibarını zedelemeye yönelik siber saldırılar ise internetin doğrudan bir siber silah olarak kullanımı ile gerçekleştirilebilecek faaliyetlerdir[465].

ABD, İngiltere ve diğer batı devletleri El-Kaide ve Jihadist internet sitelerini terör örgütü propagandası yapan internet siteleri olarak değerlendirmekte[466] ve internetin terör örgütleri tarafından kullanılmasını engellemeye yönelik ciddi önlemler almaktadır[467]. Sri Lanka'da The Liberation Tigers of Tamil Ealam'ın ayrı bir Tamil Devleti kurmak ve Hizbullah'ın faaliyetlerini etkinleştirmek için interneti aktif bir şekilde kullandıklarına dikkat çekilmektedir[468]. 11 Eylül saldırılarında internetin önemli bir iletişim aracı olarak kullanıldığı Batı doktrininde devamlı vurgulanmaktadır[469]. Ülkemizde özellikle PKK, siyasallaşma sürecine girmiş bir terör örgütü olarak internette Türk Devletine karşı ciddi bir propaganda faaliyeti yürütmektedir[470]. DHKP/C gibi sol eğilimli terör örgütleri de interneti faaliyetlerinde bir araç olarak kullanmaktadır. Bu terör örgütleri hacker grupları ile birlikte hareket ederek kamu kurumlarının bilişim sistemlerine

---

[463] Gürkaynak / İren, **a.g.m.**, s. 267.
[464] Walker, **a.g.m.**, s. 635 vd.
[465] Wilson, **a.g.e.**, s. 2. Özcan, **a.g.m.**, s. 4. Cohen, **a.g.m.**, s. 6.
[466] Walker, **a.g.m.**, s. 638-639. Deibert / Rohozinski, **a.g.m.**, s. 48.
[467] Catherine A. Theohary, John Rollins, **Terrorist Use of the Internet: Information Operations in Cyberspace**, Congressional Research Service Report for Congress, March 2011, s. 1.
[468] Walker, **a.g.m.**, s. 640.
[469] Wilson, **a.g.e.**, s. 19.
[470] Özcan, **a.g.m.**, s. 11. Walker, **a.g.m.**, s. 640.

siber saldırılarda bulunabilmektedir. Örneğin *RedHack*, ülkemizde Başbakanlık, TÜBİTAK, Emniyet Genel Müdürlüğü, Kara, Deniz ve Hava Kuvvetleri Komutanlıkları, Milli İstihbarat Teşkilatı gibi birçok kamu kurumunun bilişim sistemine saldırıda bulunmuştur[471]. RedHack Hacker Grubu, çoğu zaman PKK ve DHKP/C ile işbirliği halinde Türkiye'ye saldırmaktadır. Ülkemizin bütünlüğü aleyhine faaliyet gösteren çoğu yurt dışı kaynaklı 7000 civarında internet sitesinin bulunduğu ileri sürülmüştür[472].

Terör örgütlerinin her geçen gün siber saldırı imkanı gelişmektedir. Özellikle, terör örgütlerinin siber suçlular (cyber criminal) ile birlikte hareket ederek siber saldırı düzenlemeleri mümkün hale gelmiştir[473]. Terör örgütleri, interneti uyuşturucu ticareti gibi faaaliyetlerde de kullanabilmektedir. Terör örgütlerini destekleyen devletler, terör örgütlerine siber terörizm faaliyetlerinde de destek verebilmektedir.

B. İnternet ve Ulus-Devlet

1. İnternetin Ulus-Devlet Egemenliğini Tehdit Etmesi

Küreselleşmenin ulus-devlet üzerinde ortaya çıkardığı olumsuz etkiler doktrinde genellikle internet konusu ile birlikte ele alınmakta ve geleneksel bir görüş olarak internetin ulus-devlet varlığına karşı tehdit oluşturduğu ileri sürülmektedir[474]. Bu görüşe göre internet, ulus-devletin sınırlarını ortadan kaldırmakta, ulusal kimlik ve ideolojilere karşı olan düşünce ve akımlar internet ile birlikte daha etkin hale gelmekte ve devletin internet üzerindeki kontrol imkanlarının sınırlılığı nedeniyle devlet, ulus üzerinde de egemenliğini kaybetmeye başlamaktadır.

---

[471] http://afasam.org/tr/savunma-guvenlik/turkiyenin-yeni-guvenlik-sorunu-siber-terorizm/, 03.12.2012. http://www.haberalfa.com/haber/teknoloji/mit-ve-emniyete-darbe/833.html, 03.12.2012.
[472] Özcan, **a.g.m.**, s. 12.
[473] Wilson, **a.g.e.**, s. 2.
[474] Banu Akdenizli, "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, 26.11.2012, s. 40.

İnternet, devletlerin güç ve etkinliğine göre ulus-devlet egemenliği üzerinde farklı etkiler doğurmaktadır[475].

2. Yeni Ulus İnşasında internet

İnternet, günümüzde ulus inşasında (nation building) önemli bir faktör haline gelmiştir. Sosyal paylaşım siteleri, sohbet odaları, e-mail grupları, online ansiklopediler, internet siteleri, tartışma forumları, bloglar ve haber siteleri ulusal sembol ve karakterlerin yayılmasını kolaylaştırarak yeni bir ulusal kimlik oluşturmayı hedeflemiş toplumlara daha kolay, ucuz ve hızlı hareket edebilme ve organize olabilme imkanlarını sunmuştur[476]. Bu tür toplumlar internetin getirmiş olduğu söz konusu imkanları kullanarak uluslararası düzeyde farkındalık, etkinlik ve haklılık kazanmaya yönelik çalışmaları etkin bir şekilde yürütmekte; ulus bilinci taşıyan ve dünyanın herhangi bir köşesinde yaşayan bireylerini bir araya getirerek uluslararası düzeyde ulusal bir güç haline gelebilmektedir.

Günümüzde ulus inşasında internet diğer medya araçlarına göre çok daha fazla önem kazanmıştır. İnternetin evrensel bir karakter taşıması, devlet tarafından kontrolünün diğer medya araçlarına göre daha zor olması, düşüncelerin hızlı bir şekilde yayılmasını sağlaması, hitap ettiği kesimin uluslararası boyutta olması gibi nedenler yeni bir ulusal kimlik oluşturmayı hedeflemiş toplumlar için interneti vazgeçilmez bir araç haline getirmiştir.

Ulusal kimlik oluşturmada önemli fonksiyon taşıyan bayrak ve işaret gibi semboller, haritalar, başkentler, oluşturulmaya çalışılan ulusal kahramanlar, mitler, ortak bir geçmiş ve gelecek oluşturmayı amaçlayan dil, müzik, edebiyat, kültür ve tarih düşünce ve çalışmaları internette söz konusu toplumlar tarafından aktif bir şekilde işlenebilmektedir. Online imza kampanyaları ve oylamalar, internet aracılığıyla organize edilen konferanslar, gösteriler ve kampanyalar ile bu süreç daha da aktif hale getirilebilmektedir. Örneğin, Almanya'da kurulmuş Kürt kökenli internet siteleri üzerinde yapılan

---

[475] Akdenizli, **a.g.m.**, s. 36.
[476] Menderes Candan, Uwe Hunger, "Nation Building Online: A Case Study of Kurdish Migrants in Germany", **German Policy Studies**, Volume Four, Number 4, 2008, s. 125.

bir araştırmada ele alınan 103 internet sitesinin tamamında ulusal kimlik oluşturmaya yönelik düşünce, sembol veya karakterlerin bulunduğu tespit edilmiştir. Anılan araştırmada, söz konusu internet sitelerinin büyük çoğunluğunun verilen linkler ile birbiri ile bağlantılı halde faaliyet gösterdiği; Almanca, Kürtçe, İngilizce, Fransızca, İspanyolca, İtalyanca, İsveççe, Arapça, Farsça ve Türkçe gibi birçok dilde yayın yaptığı, ortak bir ulusal hafıza, arşiv ve uluslararası düzeyde bir Kürt diasporası oluşturma amacı taşıdığı belirtilmiştir[477].

Çeşitli etnik, dinsel, kültürel veya mezhepsel toplumların bu şekilde ulus inşasına girişmesi ulus-devlet için ciddi bir tehdit oluşturmakta ve ulus devletler bu tür girişimlere karşı geliştirdiği hukuksal ve teknolojik yöntemlerle internet üzerinden mücadele sürdürmektedir.

3. İnternetin Ulus-Devlet Egemenliğini Güçlendirmesi

İnternetin ulus-devlet egemenliği üzerinde ortaya çıkardığı tehditler, tehdidin niteliğine göre ulus-devletin ulusal güvenlik algısını, hizmet sunum biçimlerini, hukuksal düzenlemelerini, organizasyonel yapılarını değiştirmektedir. Ulus-devlet, gelişen internet teknolojisi ile toplum üzerinde daha fazla gözetim ve kontrol imkanı sağlayabilmekte, siber suçlarla mücadele için yeni hukuksal argümanlar geliştirebilmekte, ulusal kimliğin ve meşruiyetin güçlendirilmesi için faaliyetlerde bulunabilmekte ve bu gelişim internetin getirmiş olduğu tehditlere karşı ulus-devletin geliştirdiği mücadele yöntemlerine toplum nezdinde haklılık kazandırabilmektedir. Örneğin, Avrupa'da 2011 yılında faaliyete geçen Vise Bilgi Sistemi (Visa Information System) ile Avrupa'ya girecek kişilerin takibi oldukça kolaylaşmıştır. Ülkemizde interneti Geliştirme Kuruluna Türk Kültürü, Türk Tarihi ve Türk Dünyasıyla ilgili bilgilerin internet ortamında daha fazla yer alması ve bunların tanıtılması hususunda çalışmalar yapma gibi görevler verilerek internet, ulusal kimliği güçlendirmede araç olarak öngörülmüştür. ABD'de USA Patriot

[477] Candan / Hunger, **a.g.m.**, s. 133, 140.

Act ile kamu kuruluşlarına, internet servis sağlayıcılarından bir mahkeme kararı olmaksızın kişisel bilgi talep etme hakkı verilmiştir[478].

İnternet, ulus-devlet tarafından tehdit unsuru olarak algılanabileceği gibi kalkınma ve gelişmenin aracı olarak da algılanabilmektedir[479]. İnternet özellikle gelişmekte olan ülkeler için yeni fırsatlar sunabilmekte ve gelişmiş ülkeler açısından küresel ekonomide devletlerin rekabet gücünü artırabilmektedir[480].

C. Devletlerin Ulusal Siber Güvenliği Sağlama Çabaları ve Uluslararası Hukuk

1. Devletlerin Ulusal Siber Güvenliği Sağlama Çabaları

Batı ülkeleri siber terörizmi çok ciddi bir tehdit olarak ele almaktadır. Amerika'da siber saldırıların, gelecekte ABD'nin ulusal güvenliği açısından tehlike oluşturan unsurların en başında geleceği öngörülmektedir[481]. ABD, devlet dışı aktörlerin siber saldırına karşı kendisini hazırladığı gibi Çin, Rusya ve İran gibi devletleri de kendisine karşı siber saldırı yürütebilecek aktörler olarak görmekte ve siber güvenlik politikasını buna göre şekillendirmektedir. ABD, ulusal güvenlik açısından internet sitelerini takip etmekte, değerlendirmekte ve tehdit boyutunu analiz etmekte; ulusal güvenliğe tehdit oluşturan internet sitelerine erişimi engellemekte; karşı propaganda faaliyetleri yürütmektedir. Bu işlevin yerine getirilmesinde, Central Intelligence Agency (CIA), National Security Agency (NSA), Department of Defense (DOD), Department of Justice (DOJ), Federal Bureau of Investigation (FBI) ve Department of Homeland Security[482] (DHS) değişik roller üstlenmiştir[483].

Estonya'da 2007 siber saldırılarından sonra siber güvenlik, bir ulusal güvenlik konusu olarak ele alınmış, ulusal siber güvenlik stratejisi (National

---

[478] Nissenbaum, **a.g.m.**, s. 70.
[479] Uçkan, **a.g.e.**, s. 57-58.
[480] Akdenizli, **a.g.m.**, s. 35.
[481] http://www.informationweek.com/government/security/cyber-attacks-becoming-top-terror-, threat/232600046 10.9.2012. Ulusal siber güvenliğin sağlanması konusunda en sert ve etkili tedbirleri alan ülkelerin başında ABD gelmektedir. Deibert / Rohozinski, **a.g.m.**, s. 49.
[482] DHS bünyesinde National Cyber Security Division oluşturulmuştur.
[483] Theohary / Rollins, **a.g.m.**, s. 6-8.

Cyber Security Strategy 2008) oluşturulmuş, siber güvenlik kültürünün geliştirilmesine yönelik eylemler belirlenmiş, başta ceza kanunu olmak üzere hukukun birçok alanında siber güvenliği sağlamaya yönelik değişikliklere gidilmiş[484], kritik bilgi sistemleri ve altyapılarının, acil ve olağanüstü durumlarda da işlevini yerine getirebilmesine (critical information infrastructure protection) yönelik kurumsal[485] ve hukuksal düzenlemeler yapılmış, Hükümet Güvenlik Komitesine (Government Security Committee) bağlı Siber Güvenlik Kurulu (Cyber Security Council) oluşturulmuştur[486].

İtalya'da Ulusal Güvenlik Konseyi (National Security Committee), internet ile ilgili ulusal güvenliği sağlama görevine de sahiptir[487].

Devletler ulusal siber savunma ve siber savaş kapasitelerini artırmak için "*siber kuvvetler"* veya *"siber ordularını"* oluşturmaya çalışmaktadır[488].

2. Uluslararası Hukuk

Uluslararası hukukta genel kabul görmüş bir "terörizm" ve "siber terörizm" tanımı bulunmamaktadır. Bununla birlikte bazı uluslararası sözleşmelerde terörizm tanımlamasına rastlanmaktadır. Örneğin, Terörizmin Finansmanının Önlenmesine Dair Sözleşmede terörizm, doğası veya içeriği gereği bir hareketin amacı toplumu korkutmak veya hükümeti ya da uluslararası kuruluşları bir şey yapmaya veya bir şey yapmaktan vazgeçirmeye yönelik olarak sivillerin veya silahlı bir çatışma içerisinde düşman tarafın yanında aktif bir pozisyonda yer almayan diğer kişilerin öldürülmesi veya ciddi bir şekilde yaralanmasına neden olan fiiller olarak ele alınmıştır[489]. Bu sözleşmede ve ilgili diğer uluslararası sözleşmelerde

---

[484] Örneğin, kritik bilgi sistemlerine yapılan saldırılar ile sıradan bilişim suçları birbirinden ayrıştırılmış ve farklı cezalara tabi kılınmış, 2009 yılında kabul edilen Emergency Act ile siber saldırılar karşısından kriz yönetimine ilişkin hükümler getirilmiştir. Czossek / Ottis / Taliharm, **a.g.m.**, s. 60.

[485] Örneğin, Estonya Bilişim Merkezine (Estonian Informatics Centre) bağlı Kritik Bilgi Altyapısını Koruma Departmanı (Department of Critical Information Infrastructure Protection) kurulmuştur. Czossek / Ottis / Taliharm, **a.g.m.**, s. 61.

[486] Czossek / Ottis / Taliharm, **a.g.m.**, s. 58-61.

[487] https://opennet.net/research/profiles/italy, 14.03.2013.

[488] Gürkaynak / İren, **a.g.m.**, s. 264. Deibert / Rohozinski, **a.g.m.**, s. 49.

[489] United Nation International Convention for the Suppression of the Financing of Terrorism, 1999, http://treaties.un.org/doc/db/Terrorism/english-18-11.pdf, 07.12.2012.

terörizm tanımlaması açısından ortak olan nokta terörizmin, siviller veya silahlı bir çatışma içerisinde düşman tarafın yanında aktif bir pozisyonda yer almayan diğer kişiler üzerinde fiziksel bir zarar ortaya çıkarması ve saldırının toplumu korkutmak veya hükümeti ya da uluslararası kuruluşları bir şey yapmaya veya bir şey yapmaktan vazgeçirmeye yönelik olmasıdır[490]. BM'in terörizmle mücadele bakış açısı "genel" ve "özel" olmak üzere iki farklı yaklaşım göstermektedir[491]. Genel bakış açısı, terörizmi bir bütün olarak ele almakta ve genel olarak terörizmle mücadele yöntemlerini; özel bakış açısı ise terörizmin çeşitli şekilllerini tek tek ele almakta ve her biri için ayrı ayrı mücadele yöntemlerini içermektedir. BM bünyesinde bugüne kadar terörizmle mücadeleyi içeren birçok uluslararası sözleşme kabul edilmiştir[492]. Ancak, bu güne kadar henüz spesifik olarak siber terörizmle mücadeleyi içeren bir uluslararası sözleşme kabul edilmemiştir[493]. Doktrinde söz konusu uluslararası terörizmle mücadele sözleşmelerinin siber terörizmle mücadelede de uygulanabilir nitelikte olduğu ileri sürülmektedir[494].

Uluslararası kuruluşlar, siber terörizmle mücadeleyi içeren bazı çalışmalar yürütmektedir. BM, 2006 yılında Küresel Terörle Mücadele Stratejisi ve buna ek Eylem Planını kabul etmiştir. BM Güvenlik Konseyi aldığı kararlar ile terörle mücadelede etkinlik sağlamaya çalışmaktadır. NATO 2010 yılında stratejik bir model kabul etmiş; 2007 yılında yapılan siber saldırılardan sonra Estonya'da Siber Savunma Mükemmeliyet Merkezini kurmuştur.

AB'nin 2005 tarihinde yürürlüğe konulan Terörizmle Mücadele Stratejisi ve 2010 tarihli Stockholm Programında internetin terör örgütlerine sunduğu imkanlarla mücadele yöntemleri de belirlenmiştir[495].

---

[490] Cohen, **a.g.m.**, s. 3.
[491] Cohen, **a.g.m.**, s. 4.
[492] Sözleşmeler için bkz. www.un.org/terrorism/instruments.html, 10.04.2013.
[493] Cohen, **a.g.m.**, s. 10.
[494] Cohen, **a.g.m.**, s. 29.
[495] Burak Tangör, Sevinç Sayın, "Avrupa Birliği'nin Terörizmle Mücadele Stratejisi: Yeni Bir Bütünleşme Alanı mı?", **Ankara Avrupa Çalışmaları Dergisi**, Cilt: 11, No: 1, 2012, s. 94.

Ç. Türkiye'de İnternet ve Ulusal Siber Güvenlik

Ülkemizde ulusal siber güvenliğin sağlanmasına yönelik bazı çalışmalar ve hukuksal düzenlemeler yapılmıştır. Bilgi Toplumu Stratesinin eki Eylem Planında 10 nolu eylem (internet güvenliği), 26 nolu eylem (e-ticaret güvenlik altyapısı), 76 nolu eylem (bilgi sistemleri olağanüstü durum yönetim merkezi), 87 nolu eylem (bilgi güvenliği ile ilgili yasal düzenlemeler) ve 88 nolu eylem (ulusal bilgi sistemleri güvenlik programı) ile siber güvenlik alanında yapılması gereken bazı eylemler tespit edilmiştir[496]. Ayrıca siber tehdit, 2012 yılında Milli Güvenlik Siyaset Belgesine ulusal bir tehdit unsuru olarak girmiştir.

Bakanlar Kurulu'nun 11.6.2012 tarihli ve 2012/3842 sayılı Kararı ile Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar yürürlüğe konulmuştur[497]. Bu karar ile kamu kurum ve kuruluşlarınca bilgi teknolojileri üzerinden sağlanan her türlü hizmet, işlem ve veri ile bunların sunumunda yer alan sistemlerin güvenliğinin sağlanmasına ve gizliliğinin korunmasına yönelik tedbirlerin alınması ve bilgi ve iletişim teknolojilerine ilişkin kritik altyapıların işletiminde yer alan gerçek ve tüzel kişilerce uyulması gerekli usul ve esaslar belirlenmiştir (md.1). Karar ile ulusal siber güvenlikten Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, Bilgi Teknolojişleri ve İletişim Kurumu ve bu karar ile ilk defa oluşturulan Siber Güvenlik Kurulu sorumlu kılınmıştır. Siber Güvenlik Kurulu, esasen siber güvenlikle ilgili olarak alınacak önlemleri belirlemek, hazırlanan strateji ve planları onaylamak ve bunların uygulanmasını ve koordinasyonunu sağlamakla; Ulaştırma, Denizcilik ve Haberleşme Bakanlığı ve BTK ise Siber Güvenlik Kurulu tarafından belirlenen tedbirlerin veya onaylanan strateji ve planların uygulanması ile görevli kılınmıştır. Siber Güvenlik Kurulu, Ulaştırma, Denizcilik ve Haberleşme Bakanının başkanlığında, Dışişleri, İçişleri, Milli Savunma, Ulaştırma, Denizcilik ve Haberleşme bakanlıkları müsteşarları, Kamu Düzeni ve Güvenliği Müsteşarı, Milli İstihbarat Teşkilatı Müsteşarı,

---

[496] http://www.bilgitoplumu.gov.tr/Documents/1/BT_Strateji/Diger/060700_EylemPlani.pdf, 10.04.2013.
[497] RG. 20.10.2012, 28447.

Genelkurmay Başkanlığı Muhabere Elektronik ve Bilgi Sistemleri Başkanı, BTK Başkanı, TÜBİTAK Başkanı, MASAK Başkanı, TİB Başkanı ile Ulaştırma, Denizcilik ve Haberleşme Bakanınca belirlenecek bakanlık ve kamu kurumlarının üst düzey yöneticilerinden oluşan bir kurul olarak organize edilmiştir (md. 4)[498].

Siber Güvenlik Kurulunun en önemli fonksiyonunun strateji belirleme ve koordinasyon sağlama olduğu göz önüne alındığında, bu Kurulun bizce Başbakanlık bünyesinde ve koordinasyonunda oluşturulması daha doğru olacaktır[499]. Ayrıca, Siber Güvenlik Kurulu yanısıra özel sektör ve kamu kurumu niteliğindeki meslek kuruluşlarının üyelerinin de katılımını sağlayan Siber Güvenlik Danışma Kurulu ve Türk Ulusal Siber Olaylara Müdahale Ekibinin oluşturulmasına ihtiyaç duyulmaktadır[500].

Bu olumlu gelişmeler yanında Türkiye'nin ulusal siber güvenlik konusunda eksiklikleri de bulunmaktadır. Örneğin, Türkiye, ulusal siber güvenlik stratejisi belgesine sahip değildir[501]. Ulusal siber güvenlik, AB Terörizmle Mücadele Stratejisinin terörle mücadele örneğinde olduğu gibi önleme, koruma, izleme ve karşılık verme stratejileri çerçevesinde ele alınmalıdır[502]. Ayrıca, internetin terör örgütleri ve devletler tarafından Türk devletinin ulusal güvenliği ve menfaatlerine tehdit oluşturan unsurlarına karşı internet iletişim stratejisi geliştirilmelidir. Ulusal güvenliği tehdit eden unsurlara karşı istihbarat, karşı propaganda ve psikolojik savunma yöntemleri

---

[498] Kurulun bir Bakanlar Kurulu Kararı ile oluşturulması, 27.9.1984 tarihli ve 3046 sayılı Kanunun 39. maddesi ve 655 sayılı Ulaştırma, Denizcilik ve Haberleşme Bakanlığının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararnamenin 29. maddesine aykırı düşmektedir. 3046 sayılı Kanunun 39. maddesine göre, "*Bakanlıklarda ve bağlı kuruluşlarda hizmetin kurul biçiminde yürütülmesi gerektiğinde, görevleri ve teşekkül tarzı kuruluş kanunlarında veya diğer kanunlarda gösterilmek kaydıyla sürekli kurullar kurulabilir".* 655 sayılı Kanun Hükmünde Kararnamenin 29. maddesinde ise oluşturulan sürekli kurullar arasında Siber Güvenlik Kurulu yer almamaktadır. Bu nedenle Kurulun oluşumunun bir an önce çıkarılması gereken Ulusal Siber Güvenlik Kanunu ile düzenlenmesi gerekir.

[499] Bilgi Güvenliği Derneği, **Ulusal Siber Güvenlik Stratejisi**, Haziran 2012, http://www.bilgiguvenligi.org.tr/index_files/pdf/Ulusal_Siber_Guvenlik_Stratejisi.pdf, 27.11.2012, s. 18.

[500] Bilgi Güvenliği Derneği, **Ulusal Siber Güvenlik Stratejisi**, Haziran 2012, http://www.bilgiguvenligi.org.tr/index_files/pdf/Ulusal_Siber_Guvenlik_Stratejisi.pdf, 27.11.2012, s. 16, 21.

[501] Bilgi Güvenliği Derneği, **Ulusal Siber Güvenlik Stratejisi**, Haziran 2012, http://www.bilgiguvenligi.org.tr/index_files/pdf/Ulusal_Siber_Guvenlik_Stratejisi.pdf, 27.11.2012, s. 29-30.

[502] Tangör / Sayın, **a.g.m.**, s. 93.

ile karşı konulmalıdır. PKK terör örgütü ile mücadele ve Ermeni Meselesi gibi ulusal güvenlik konularında, internette Türkiye'nin mücadelesinin haklılığını ortaya koyan çalışmalar yapılmalıdır. Ulusal siber güvenliğin sağlanmasında kamu-özel sektör işbirliğinin geliştirilmesi[503], milli işletim sistemi ve milli arama motoru gibi yazılımların üretilmesi, ulusal güvenliği tehdit eden siber saldırılara karşı ulusal güvenliğin sağlanması ve saldırılara karşı saldırıda bulunulması[504] amacıyla bir siber ordu oluşturulması ve bunun hukuksal altyapısının düzenlenmesine yönelik çalışmalara ihtiyaç duyulmaktadır. Aynı ihtiyaç, interaktif bankacılık altyapısı, e-ticaret siteleri, kamu kurumlarının siteleri ile internet servis sağlayıcılarının bilişim altyapısının korunmasına yönelik strateji ve işbirliğinin geliştirilmesi[505] ve siber güvenlik kültürünün oluşturulması açısından da kendisini göstermektedir.

[503] Tiirmaa-Klaar, **a.g.m.**, s. 9.
[504] Örneğin, Amerikan hukukuna göre ulusal güvenliğe karşı yapılan siber saldırılara devlet, orantılı bir şekilde denial-of-service (DoS) karşı saldırısı ile cevap verebilir. Denning, **a.g.m.**, s. 267.
[505] Tiirmaa-Klaar, **a.g.m.**, s. 6.

DÖRDÜNCÜ BÖLÜM
DEVLETİN İNTERNETİ DÜZENLEME ARAÇLARI

Devlet, bir yandan interneti düzenlerken diğer yandan da bu düzenlemelerin hayata geçirilebilmesi için bazı hukuksal araçlar geliştirmektedir. Esasen bu hukuksal araçlar; cezai, idari ve hukuksal sorumluluk olarak karşımıza çıkmaktadır. Hukuksal sorumluluk, bu çalışmanın kapsamı dışında bırakılmıştır. Bu bölümde, devlet tarafından cezai ve idari sorumluluk araçlarının internet alanında ne şekilde kullanıldığı incelenmiştir.

I. YÜKÜMLÜLÜK ÖNGÖRÜLEN SUJELER

Devletin internet üzerinde düzenleme yaparken düzenleme araçlarını üzerinde uygulayabileceği üç suje bulunmaktadır. Bunlar, içeriği üretenler, aracılar (intermediaries) ve kullanıcılardır[506].

Bilgi Toplumu Hizmetlerinin Bazı Hukuki Yönleri ve Özellikle İç Pazarda Elektronik Ticaret Konusunda 8 Haziran 2000 tarihli 2000/31/AT sayılı Avrupa Parlamentosu ve Konsey Direktifinde (e-Ticaret Direktifi)[507] "*hizmet sağlayıcı"* kavramı, bir bilgi toplumu hizmeti sağlayan her türlü gerçek veya tüzel kişi olarak (md. 2/1, b); "*bilgi toplu hizmeti"* kavramı ise Direktifin 98/34/EC sayılı AB Direktifine (Teknik Standartlar ve Düzenlemeler ile Bilgi Toplumu Hizmetleri Konusunda Bilgi Teminine İlişkin Direktif)[508] yaptığı atıf nedeniyle bu Direktifte, bir ücret karşılığı olarak belli bir mesafeden elektronik araçlar vasıtasıyla ve hizmet alıcısının bireysel bir talebi üzerine sunulan hizmet olarak tanımlanmıştır. Bu çerçevede, Direktifte yer alan hizmet

---

[506] Goldsmith / Wu, **a.g.e.**, s. 69.

[507] 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:HTML, 23/10/2012.

[508] Directive 98/34/EC of The European Parliament And of The Council of 22 June 1998 aying down a procedure for the provision of information in the field of technical standards and regulations and of rules on Information Society services, http://eur-lex.europa.eu/LexUriServ/site/en/consleg/1998/L/01998L0034-20070101-en.pdf, 23/10/2012.

sağlayıcı kavramı çok geniş bir çerçeveye oturtulmuştur. Direktifte ayrıca, aracı hizmet sağlayıcılarının (intermediary service providers) sorumlulukları da düzenlenmiştir (md. 12-15). Direktifte yer alan söz konusu düzenlemeler AB üyesi ülkelerin düzenlemelerini bu doğrultuda şekillendirmiş ve internet süjeleri ile bunların sorumluluk ve yükümlülükleri tek tek belirlenmiştir. Ülkemiz düzenlemesine yön vermesi itibariyle önem taşıyan Alman Telemedya Kanununda (Telemedia Act-TMG) da e-Ticaret Direktifine paralel şekilde internet süjelerinin sorumluluk ve yükümlülükleri belirlenmiştir. Ülkemizde 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun ile e-Ticaret Direktifi ve Alman Telemedya Kanununda yer alan düzenlemelere benzer düzenlemeler yapılmıştır.

5651 sayılı Kanunda içerik sağlayıcı, erişim sağlayıcı, yer sağlayıcı, toplu kullanım sağlayıcı ve kullanıcı tek tek tanımlanmıştır. Bu tanımlama internet alanında faaliyet gösteren veya interneti kullanan kişilerin sorumluluklarının belirlenmesi açısından faydalı olmuştur[509].

İnternetin düzenlenmesi konusunda her suje açısından farklı yükümlülükler öngörülmekle birlikte bazı durumlarda söz konusu süjelerin içiçe geçmesi söz konusu olabilmektedir. Bir diğer deyişle, bir sujenin birden fazla kimliği bünyesinde taşıması mümkündür. Örneğin, içerik sağlayıcı aynı zamanda yer sağlayıcı olabileceği gibi, yer sağlayıcı aynı zamanda erişim sağlayıcı da olabilir. Böyle durumlarda, birden fazla kimliği bünyesinde bulunduran internet süjesinin bünyesinde taşıdığı her kimlik açısından öngörülen yükümlülükleri yerine getirmesi gerekir.

Bu bölümde sadece internetin düzenlenmesinde yükümlülük ve sorumluluk öngörülen taraflar incelenmiştir. Bunların yükümlülük ve sorumlulukları aşağıda ayrı bir bölüm başlığı altında ayrıca incelenmiştir.

---

[509] İçel, **a.g.m.**, s. 27.

A. İçerik Sağlayıcı

İçerik sağlayıcı, internet ortamında kendisine ait içeriği yayına sunan kişi olarak tanımlanabilir. 5651 sayılı Kanuna göre içerik sağlayıcı, "*internet ortamı üzerinden kullanıcılara sunulan her türlü bilgi veya veriyi üreten, değiştiren ve sağlayan gerçek veya tüzel kişi"*dir. Yerinde bir düzenleme olarak bu tanımlama ile içerik sağlayıcı kavramı oldukça geniş bir çerçeveye oturtulmuştur. Ancak, tanımlama lafzen ele alındığı zaman *"ve"* sözcüğünden dolayı sanki içerik sağlayıcının bilgi veya veriyi üretme, değiştirme ve sağlama faaliyetlerini birlikte yerine getirmesi gibi bir anlam ortaya çıkmaktadır. Halbuki, internet ortamında bu faaliyetlerin her birinin farklı kişiler tarafından yerine getirilmesi mümkündür[510]. Hatta internetin yapısı, bunu gerekli kılmaktadır. Aksini düşünmek, internet ortamında sadece bilgi veya veri üreten veya sadece değiştiren ya da sadece sağlayan kişileri içerik sağlayıcı konumunda olmaktan çıkarmaktadır. Yasa koyucunun amacının bu yönde olmadığı kuşkusuzdur. Bu nedenle, internet ortamında herhangi bir bilgi veya veriyi tek başına üreten, değiştiren veya sağlayan kişiyi içerik sağlayıcı olarak kabul etmek gerekir.

Doktrinde 5651 sayılı Kanunda yer alan içerik sağlayıcı tanımlamasının açık olmadığı[511] ve birçok hukuksal sorunu beraberinde getirdiği ileri sürülmüştür[512]. Özellikle arama motorları ve Web 2.0 teknolojisini kullanan internet siteleri açısından Kanunda yer alan tanımlamanın yetersiz olduğu ifade edilmiştir.

Arama motorları açısından konuya yaklaştığımız zaman, arama motorlarının içerik sağlayıcı konumunda olup olmadıkları ve bu çerçevede tabi olacakları yükümlülük ve sorumluluklar tartışmalıdır[513]. Bir görüş, arama

---

[510] Yasemin Durnagöl, "5651 Sayılı Kanun Kapsamında İnternet Aktörlerine Getirilen Yükümlülükler ile İdari ve Cezai Yaptırımlar", **TAAD**, Cilt. 2, Yıl. 2, Sayı. 4, 20 Ocak 2011, s. 400-401.

[511] Durnagöl, **a.g.m.**, s. 401.

[512] Günaydın, **a.g.e.**, s. 134. E-Ticaret Direktifi ve Alman Telemedya Kanunu açısından benzer bir görüş için bkz. Thomas Hoeren, "Liability for Online Services in Germany", **German Law Journal**, Vol. 10, No. 05, s. 583.

[513] Gönenç Gürkaynak, İlay Yıldız, Pınar Kara, "Türk İnternet Hukuku Uygulamasının ve Mevzuatının Evriminin İlk Dönemini Tamamlaması İçin Öneriler ve Gözlemler", http://www.elig.com/docs/Turk_internet_Hukuku_Uygulamasinin_ve_Mevzuatinin_Evriminin_Ilk_Donemini_Tamamlamasi_Icin_Oneriler_ve_Gozlemler.pdf, 10.04.2013, s. 3.

motorlarının içerik sağlayıcı konumunda olmadığını ileri sürmektedir. Bu görüşe göre arama motorları herhangi bir içerik üretmemekte, üçüncü kişiler tarafından üretilmiş içeriğe sadece erişim sağlamaktadır[514]. Diğer görüşe göre ise arama motorları içerik sağlayıcı konumundadır. Bu görüşe göre, arama motorları belki doğrudan bir içerik sağlamaz; ama diğer internet sitelerinde yayınlanan içeriği belli bir sistem ve bütünlük içerisinde bir araya getirir. 5651 sayılı Kanun açısından ise esasında içerik sağlayıcı kavramı tanımlanırken, arama motorları açısından bir ayrım yapılmamış; hem içeriği üretenler hem arama motorları içerik sağlayıcı kabul edilmiştir.

Konuya Web 2.0 teknolojisini kullanan internet siteleri açısından yaklaştığımız zaman ise 5651 sayılı Kanun çerçevesinde örneğin, bir forum sayfasına kullanıcı tarafından bir yorum yazılması durumunda, hem bu yorumu yazan kişi[515] hem de sitenin sahibi içerik sağlayıcı konumunda olacaktır. Benzer durum, blog siteleri, video paylaşım siteleri[516], sosyal paylaşım siteleri, e-ticaret siteleri gibi sitelere kullanıcılar tarafından içerik yüklenmesi durumunda da karşımıza çıkmaktadır. Aynen arama motorlarında olduğu gibi bu tür teknoloji kullanan internet siteleri açısından da 5651 sayılı Kanunun içerik sağlayıcı tanımlamasında bir ayrım yapılmamıştır.

Arama motorları ve Web 2.0 teknolojisi kullanan internet siteleri açısından yapılan bu değerlendirme, bunların sorumluluk esaslarının, bizzat içeriği üreten diğer içerik sağlayıcıları ile aynı sorumluluk esaslarına tabi kılındığı anlamına gelmemektedir. Arama motorları ve Web 2.0 teknolojisi kullanan internet siteleri içerik sağlayıcıdırlar; ancak, bunların sorumluluk esasları aşağıda görüleceği üzere ayrıca düzenlenmiştir.

Benzer bir yaklaşım Alman Telemedya Kanununda öngörülmüştür[517]. Ancak, Kanunda içerik sağlayıcı tanımlaması ayrıca yapılmamış; hizmet

---

[514] Özbek, **a.g.m.**, s. 111. Gürkaynak / Yıldız / Kara, **a.g.m.**, s. 3.

[515] Durnagöl, **a.g.m.**, s. 401.

[516] Bir görüş, Youtube'a video yüklenmesi olayında video yükleyen kişinin içerik sağlayıcı, Youtube'un ise yer sağlayıcı olduğunu ileri sürmektedir. Savaş Bozbel, "5651 Sayılı Kanuna İstinaden Bazı İnternet Sitelerine Erişimin Engellenmesi Tedbirlerine Eleştirel Bir Yaklaşım", **e-Akademi**, S. 72, Şubat 2008, http://www.e-akademi.org/makaleler/sbozbel-5.htm, 10.04.2013, s. 3.

[517] Almanya'da Telemedia Act'ın sorumluluk başlıklı üçüncü bölümünde servis sağlayıcıların sorumlulukları düzenlenmiştir. Bu bölümde genel ilkeler (md. 7), bilgi iletimi faaliyeti (md. 8), bilginin hızlı iletimi için geçici depolama (md. 9) ve bilginin depolanmasına (md. 10) ilişkin

sağlayıcı (service provider) kavramı, içerik sağlayıcıları (content provider) da kapsar şekilde kendi veya başkasının içeriğini kullanıma sunan veya buna erişim sağlayan gerçek veya tüzel kişi olarak tanımlanmış (md 2) ve hizmet sağlayıcıların, kullanıma hazır bulundurdukları kendilerine ait bilgiden genel hükümlere göre sorumlu oldukları hüküm altına alınmıştır (md. 7). Şu halde, bu düzenlemeler gereği kendisine ait bir bilgiyi kullanıma hazır bulunduran hizmet sağlayıcı, içerik sağlayıcı kabul edilecektir[518].

B. Erişim Sağlayıcı

Erişim sağlayıcı, kullanıcıların internete erişimine abone ile yaptıkları sözleşme çerçevesinde imkan sağlayan firmaları ifade etmek üzere kullanılan bir kavramdır. Erişim sağlayıcı, internet ortamında herhangi bir içerik üretmemekte; başkaları tarafından üretilen içeriğe erişimi sağlamaktadır[519]. internet alanında, erişim sağlayıcıların hukuksal konumu belirlenirken internette üretilen içerik üzerinde bunların bir etkisinin bulunup bulunamayacağı tartışılmış ve "*yayıncı" (publisher)* ile "*dağıtıcı" (distributer)* arasında yapılan ayırım, bu alana da uygulanmıştır. Bunun sonucunda erişim sağlayıcıların yayıncı konumunda değil, dağıtıcı konumunda oldukları kabul edilmiştir.

e-Ticaret Direktifinde, erişim sağlayıcı kavramı doğrudan tanımlanmamıştır. Ancak, Direktifin dördüncü bölümünde "*aracı hizmet sağlayıcıların"* sorumlulukları belirlenirken erişim sağlayıcı, bir iletişim ağına erişim sağlayan olarak ifade edilmiştir (md. 12/1).

Türk hukuk sisteminde "*internet servis sağlayıcı" (İSS)* ile "*erişim sağlayıcı"* kavramlarına farklı anlamlar yüklenmiştir. İnternet servis sağlayıcısı, sadece internet erişim hizmeti sunmakla yetkilendirilen işletmeleri; erişim sağlayıcı kavramı ise, internet servis sağlayıcılar da dahil olmak üzere internete erişim imkanı sağlayan her türlü işletmeciyi ifade

---

hükümlere yer verilmiştir[517]. Söz konusu hükümlerde internetin süjesi olarak içerik sağlayıcı, erişim sağlayıcı ve yer sağlayıcı ele alınmış ve bunların sorumlulukları düzenlenmiştir. Hoeren, **a.g.m.**, s. 562.

[518] Hoeren, **a.g.m.**, s. 562.

[519] Soysal, "İnternet Servis Sağlayıcılarının", s. 308.

etmektedir. 5651 sayılı Kanunda erişim sağlayıcı," *kullanıcılarına internet ortamına erişim sağlayan her türlü gerçek veya tüzel kişi"* olarak tanımlanmıştır[520]. Bu tanım ile erişim sağlayıcılık hizmeti geniş bir çerçeveye oturtulmuş, herhangi bir şekilde kullanıcılarına internet ortamına erişim imkanı sağlayan her türlü kişi erişim sağlayıcısı kabul edilmiştir. Bu çerçevede İSS, GSM, GMPCS, IMT–2000/UMTS, SMŞH, HT-GSM 1800 MTH işletmecisi ile uydu ve kablo hizmetlerine ilişkin görev sözleşmesi sahibi işletmeciler erişim sağlayıcı olabilecektir[521]. Erişim sağlayıcı kavramının bu şekilde geniş bir çerçevede tanımlanması, tanımlamanın teknolojik gelişmelere açıklığı nedeniyle doktrinde olumlu değerlendirilmektedir[522]. Ülkemizde erişim sağlayıcı olarak faaliyet gösteren işletmeci listesi TİB'in internet sitesinde güncel olarak yayınlanmaktadır[523].

Alman Telemedya Kanununda, "içerik sağlayıcı" kavramında olduğu gibi "erişim sağlayıcı" kavramı da ayrıca tanımlanmamıştır. Ancak, erişim sağlayıcıların sorumlulukları belirlenirken üçüncü kişilere ait bilginin bir iletişim ağı içerisinde iletilmesi veya buna erişim sağlanması, erişim sağlayıcı faaliyeti olarak ele alınmıştır (md. 8 ve 9).

C. Yer Sağlayıcı

"*Hosting"*, başkaları tarafından üretilen içeriğe yer sağlanması ve internet ortamında yayına sunulması faaliyeti olarak tanımlanabilir[524]. Kişinin ürettiği içeriğe bizzat kendisinin de yer sağlaması mümkündür. Bu durumda içerik sağlayıcı aynı zamanda yer sağlayıcı konumundadır. Ancak,

---

[520] Bu tanımın kapsamı, Telekomünikasyon Kurumu Tarafından Erişim Sağlayıcılara ve Yer Sağlayıcılara Faaliyet Belgesi Verilmesine İlişkin Usul ve Esaslar Hakkında Yönetmelik ile erişim sağlayıcılığı sadece sermaye şirketlerine özgülenerek sınırlandırılmıştır (md. 4).

[521] Bkz. Elektronik Haberleşme Sektörüne İlişkin Yetkilendirme Yönetmeliği md. 19/1, (s) bendi. Anılan maddede erişim sağlayıcı olabilecek işletmeciler sınırlı sayıda sayılmamıştır.

[522] Durnagöl, **a.g.m.**, s. 384-385.

[523] Liste için bkz. http://www.btk.gov.tr/elektronik_haberlesme_sektoru/yetkilendirme/isletmeciler/isletmeci.php?yetkitipi=ISS_B, 19.10.2012. Sektörde en yüksek oranda pazar payına sahip olan TTNet'in abone oranı 2011 yılında % 81 olarak gerçekleşmiştir. Bilgi Teknolojileri ve İletişim Kurumu, **Faaliyet Raporu 2011**, http://www.tk.gov.tr/kutuphane_ve_veribankasi/raporlar/faaliyet_raporlari/index.php, 05.10.2012, s. 30.

[524] Soysal, "İnternet Servis Sağlayıcılarının", s. 318.

uygulamada genellikle yer sağlama hizmeti bu işi ticari bir faaliyet olarak yürüten firmalardan ücret karşılığında alınmaktadır. Bu tür durumlarda, hosting firmaları sadece başkaları tarafından üretilen içeriği barındırır.

e-Ticaret Direktifinde, erişim sağlayıcı kavramı gibi yer sağlayıcı kavramı da doğrudan tanımlanmamıştır. Ancak, Direktifin "*hosting"* başlıklı 14. maddesinde yer sağlayıcı, hizmetin alıcısı tarafından sağlanan bilginin saklanması olarak ifade edilmiştir.

5651 sayılı Kanunda "*yer sağlayıcı"* kavramı, hizmet ve içerikleri barındıran sistemleri sağlayan veya işleten gerçek veya tüzel kişi olarak tanımlanmıştır (md. 2/1, m). Kanunda yer alan bu tanımlama, ticari bir faaliyet olarak yer sağlama hizmeti veren hosting firmalarını veya gerçek kişileri kapsadığı gibi kişisel yayınlarını kendi sistemlerinde barındıran kişileri de kapsamaktadır[525]. Yer sağlayıcı tanımlaması yapılırken ve bunların uymaları gereken yükümlülükler belirlenirken bu farklılığın gözetilmemesi, fiiliyatta bu hükmün uygulanmasının mümkün olmadığı ve kişisel yayınlarını kendi sistemlerinde barındıranlar için aşırı yükümlülükler içerdiği gerekçesiyle eleştirilmekte ve son sıradakilerin ayrıca tanımlanması ve yükümlülüklerinin belirlenmesi gerektiği ileri sürülmektedir[526].

Ülkemizde faaliyet gösteren yer sağlayıcı listesi, TİB'in internet sitesinde güncel bir şekilde yayınlanmaktadır[527].

Alman Telemedya Kanununda, açıkça tanımlama yapılmamakla birlikte üçüncü kişilere ait bilginin hizmetin alıcısı için depolanması, yer sağlama faaliyet olarak ele alınmıştır (md. 10).

Ç. Toplu Kullanım Sağlayıcı

"Toplu kullanım sağlayıcı" kavramı, Türk hukukunda özellikle *"internet kafelerin"* hukuksal konumunu belirlemek amacıyla kullanılmıştır. Toplu kullanım sağlayıcılar, kullanıcıların internete erişimine imkan sağlamakla birlikte internete erişim sağlayan firmalardan farklıdır. 5651 sayılı Kanunda

---

[525] Durnagöl, **a.g.m.**, s. 393.
[526] Durnagöl, **a.g.m.**, s. 393, 395.
[527] http://www.tib.gov.tr/tr/tr-menu-57-yer_saglayicilar_listesi.html, 23.10.2012.

toplu kullanım sağlayıcı, "*kişilere belli bir yerde ve belli bir süre internet ortamı kullanım olanağı sağlayan"* olarak tanımlanmış (md. 2/1, i); "*ticari amaçla toplu kullanım sağlayıcılar"* ile "*ticari amaçlı olmayan toplu kullanım sağlayıcılar"* arasında bir ayrım yapılarak, bunlar açısından farklı yükümlülük ve sorumluluklar öngörülmüştür (md. 7). Ticari amaç taşıyan toplu kullanım sağlayıcılar ile böyle bir amaç taşımayan toplu kullanım sağlayıcılar açısından bu şekilde bir ayırım yapılması yerinde bir yaklaşım olmuştur.

İnternet Toplu Kullanım Sağlayıcıları Hakkında Yönetmelikte "*ticari amaçla internet toplu kullanım sağlayıcı"* kavramı, internet 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 imkan sağlayan gerçek ve tüzel kişi olarak tanımlanmıştır (md. 3/1, l). Bu çerçevede internet kafeler, ticari amaç taşıyan toplu kullanım sağlayıcı; çalışanlarına internet kullanım olanağı sağlayan işyerleri ile kamu kurum ve kuruluşları, okullar, kütüphaneler ve üniversiteler gibi yerler ise ticari amaç taşımayan toplu kullanım sağlayıcı kabul edilecektir[528].

Toplu kullanım sağlayıcıların hangi durumlarda ticari amaç taşıyacakları hususu özellikle, müşterilerine asıl olarak sundukları diğer hizmetler yanında ücretsiz ek hizmet olarak toplu internet kullanım hizmeti sağlayan işyerleri açısından bir belirsizlik yaratabilir[529]. Söz konusu işyerlerinin, toplu internet kullanım hizmetini müşterilerine ücretsiz olarak sunmaları nedeniyle Yönetmeliğin anılan hükmü gereğince bu işyerlerini ticari amaç taşıyan toplu kullanım sağlayıcı olarak kabul etmek mümkün gözükmemektedir.

D. Kullanıcı

"Kullanıcı" (user), interneti kullanan kişidir. Abone (subscriber) ise bir sözleşme ile erişim sağlayıcılardan internete bağlanma hizmeti alan kişidir. Kullanıcı kavramı, abone kavramından farklıdır. Bir kişi, internet abonesi

[528] Durnagöl, **a.g.m.**, s. 404, 407.
[529] Durnagöl, **a.g.m.**, s. 407.

olmamasına rağmen internet kullanıcısı olabilir. Her internet abonesi de kullanıcı konumunda olmayabilir. Kullanıcı ve abone, gerçek kişi olabileceği gibi tüzel kişi de olabilir. İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelikte kullanıcı, aboneliği olup olmamasına bakılmaksızın internet ortamından yararlanan gerçek veya tüzel kişiler; abone ise herhangi bir sözleşme ile erişim sağlayıcılarından internet ortamına bağlanma hizmeti alan gerçek veya tüzel kişiler olarak tanımlanmıştır (md. 3). Aynı tanımlama 5809 sayılı Elektronik Haberleşme Kanununda da yapılmıştır (md. 3). Kamu hukuku açısından öngörülen yükümlülükler kullanıcıya yöneliktir.

Kullanıcı, internette içerik üretmeye başladığı anda "*içerik sağlayıcı"* konumuna gelir. Örneğin, bir forum sitesinde yazılanları takip eden kişi kullanıcıdır. Ancak, forum sitesine bir yorum yazıldığında kullanıcı artık içerik sağlayıcı konumuna gelmektedir.

II. SORUMLULUK

İnternet alanında öngörülen sorumluluk sistemi, sektörün gelişimi ve bilgi toplumunun gerçekleştirilmesinde destekleyici bir rol üstlenebileceği gibi aksi yönde gelişimi tersine de çevirebilir[530]. Bu nedenle bu alanda öngörülecek sorumluluk sisteminin hassasiyetle belirlenmesi ve bu bağlamda sektör ile bilgi toplumunun gelişimi yönünde bir politika izlenmesi gerekir. Ceza hukuku kurallarına son çare olarak başvurulması ilkesi bu anlamda özellikle önem taşımaktadır[531].

Cezai sorumluluk, ceza normlarının uygulanmasını gerektirir. İdari sorumluluk, idari para cezası, faaliyet belgesinin iptali, internette yer alan içeriğe erişimin engellenmesi gibi idari yaptırım uygulamalarını beraberinde getirmektedir. Hukuksal sorumluluk ise kişi haklarını ihlal eden bir içeriğin yayından çıkarılması, hakkı ihlal edilen kişiye cevap hakkının tanınması ve tazminat öngörülmesi gibi hukuksal müesseseleri karşımıza çıkarmaktadır. Bu çalışmada, hukuksal sorumluluk müessesesi ve bu çerçevede kişilik

---

[530] Soysal, "internet Servis Sağlayıcılarının", s. 305.
[531] Özen / Baştürk, **a.g.e.**, s. 4. Özbek, **a.g.m.**, s. 105. Uçkan / Beceni, **a.g.m.**, s. 367.

haklarının ihlalinden dolayı ortaya çıkan hukuksal uyuşmazlıklar incelenmeyecektir.

e-Ticaret Direktifinde aracı hizmet sağlayıcılar açısından getirilen tanımlamalar ve sorumluluk sistemi sadece hukuksal sorumluluğu kapsamamakta; aynı zamanda cezai ve idari sorumluluğu da kapsamaktadır[532]. Bu nedenle burada cezai ve idari sorumluluk açısından yapılan değerlendirmelerde e-Ticaret Direktifi göz önünde bulundurulacaktır. Aynı değerlendirme, 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunda yer alan düzenlemeler açısından da yapılabilir. 5651 sayılı Kanunda, internet ortamında yer alan içerikten dolayı içerik, yer ve erişim sağlayıcılar için belirlenen sorumluluk sistemi (md. 4, 5, ve 6) cezai, idari ve hukuksal sorumluluk açısından uygulanabilir niteliktedir.

A. Cezai Sorumluluk

İnternet ortamında yer alan içerikten dolayı cezai açıdan kural olarak içerik sahibinin sorumlu olması gerekir. İçerik bizzat onun tarafından üretilmiş ve internet ortamında yayına sunulmuştur. Herkes kendi fiilinin sonuçlarına katlanmalıdır.

Yer sağlayıcı, erişim sağlayıcı ve toplu kullanım sağlayıcı gibi aracılar ise kural olarak cezai sorumluluğa tabi tutulmamalıdır. Bunların işlevi başkalarına ait içeriğe kullanıcıların erişimini sağlamaktır. İçeriğin üretiminde herhangi bir katkıları bulunmamaktadır. Bu yaklaşım, bunların hukuka aykırı internet yayınının doğrudan sahibi olmamaları ve yayınlanan içeriği her seferinde kontrol etmelerinin imkansız olduğu düşüncesinden kaynaklanmıştır[533]. Bu yaklaşım genel olarak doktrinde olumlu değerlendirilmiştir[534].

---

[532] Gerald Spindler, **Study On The Liability of Internet Intermediaries**, 2007, http://ec.europa.eu/internal_market/e-commerce/docs/study/liability/final_report_en.pdf, 23.10.2012, s. 4.
[533] Uçkan / Beceni, **a.g.m.**, s. 411-412.
[534] İçel, **a.g.m.**, s. 20.

Kullanıcıların sorumluluğu ise internet ortamından başkalarına ait içeriğin indirilmesi durumunda söz konusu olur.

1. İçerik Sağlayıcıların Cezai Sorumluluğu

5651 sayılı Kanun ile cezai hükümlerin uygulanması bakımından kural olarak içerik sağlayıcılar muhatap alınmış; erişim sağlayıcılar, yer sağlayıcılar ve toplu kullanım sağlayıcılar açısından ise bazı kabahat türünden fiiller ve bu fiillerin işlenmesi durumunda idari yaptırımlar öngörülmüştür[535].

5651 sayılı Kanun ile içerik sağlayıcı, internet ortamında kullanıma sunduğu her türlü içerikten sorumlu tutulmuş (md. 4/1)[536]; 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 sorumlu tutulabilecektir (md. 4/2).

5651 sayılı Kanunun söz konusu düzenlemesi aslında içerik sağlayıcıları iki gruba ayırmaktadır. Birinci grup, kendisine ait içeriği internet ortamında kullanıma sunan gruptur. İkinci grup ise bağlantı sağlanan başkasına ait içeriği internet ortamında kullanıma sunan gruptur. Birinci grup, internet ortamında kullanıma sunduğu her türlü içerikten her hangi bir sınırlandırılmaya tabi olmaksızın her halde sorumlu tutulmuştur. Kanunun bu yaklaşımı, herkesin kendi fiilinden sorumlu olması gerektiği düşüncesine dayandığından yerinde bir düzenleme olmştur. İkinci grup ise kural olarak bağlantı sağladığı başkasına ait içerikten sorumlu tutulmamıştır. Bu noktada *bağlantı sağlama* kavramı önem kazanmaktadır[537]. Doktrinde bağlantı sağlama kavramını, "*link verme"* veya "*banner"* olarak yorumlayan yazarlar vardır[538]. Ancak, bizce bağlantı sağlama kavramı bu derece dar bir çerçevede ele alınamaz. Bu kavram, "link verme" veya "banner" şeklinde bağlantı sağlamanın yanısıra bir içerik sağlayıcının bizzat kendisine ait

---

[535] İçel, **a.g.m.**, s. 23-24.
[536] Bu sorumluluk, hukuki bir sorumluluk gerektirebileceği gibi cezai veya idari bir sorumluluk da gerektirebilir.
[537] Akdeniz / Altıparmak, **a.g.e.**, s. 34. Günaydın, **a.g.e.**, s. 126.
[538] Dülger, **a.g.m.**, s. 8.

olmayan her türlü içeriğe kendi yayınında yer vermesini veya bu tür içeriğin kendi yayınında yer almasını kapsayacak şekilde geniş bir anlama sahiptir. Örneğin, bir blog, sosyal paylaşım, forum, video paylaşım veya sohbet sitesini işleten veya arama motoru[539] hizmeti sunanlar başkasına ait içerikten kural olarak sorumlu değildir[540]. Bir blog sitesinde blog açıp içerik üreten, bir sosyal paylaşım, forum veya sohbet sitesinde görüşlerini yazan, bir video paylaşım sitesinde video paylaşan veya bir web sitesi aracılığıyla doğrudan yayın yapan kişiler ise doğrudan içeriğin sahibi olduklarından söz konusu içerikten sorumludur.

Diğer taraftan, Kanunun 4. maddesinin ikinci fıkrası ile söz konusu ikinci grubun istisnaen başkasına ait içerikten sorumlu tutulması öngörülmüştür. Doktrinde söz konusu düzenleme, belirsizlik içerdiği ve birçok hukuksal sorunu bünyesinde taşıdığı gerekçesiyle eleştirilmiştir[541]. Eleştirilen ilk husus, yayıncının sunuş biçiminden bağlantı sağladığı içeriği benimsediğinin ve kullanıcının söz konusu içeriğe ulaşmasını amaçladığının açıkça belli olduğu durumların belirsizlik içerdiği yönündedir. Bu görüş birçok yönden haklılık payı içermektedir. Ancak, bağlantı sağlanan başkasına ait içerikten dolayı içerik sağlayıcının hiçbir şekilde sorumlu tutulmaması gibi bir yaklaşım da birçok sakıncayı bünyesinde barındırmaktadır. Böyle bir yaklaşımın kabul edilmesi durumunda, bağlantı sağlanan hukuka aykırı içerikle mücadele etmek oldukça güç bir hal alabilir[542]. Ayrıca, bir kişinin bağlantı sağladığı başkasına ait içerikten sorumlu tutulması o kadar kolay değildir. Kanun, bunun için birçok şart öngörmüştür. Bu şartları, *yayının sunuş biçimi*, *bağlantı sağlanan içeriği benimseme ve kullanıcının söz konusu içeriğe ulaşmasını amaçlama* ve *bunun açıkça belli olması* başlıkları altında ele alabiliriz. İlk olarak internet sitesinin "*sunuş biçimi"*, bağlantı sağlanan içeriğin benimsendiği ve kullanıcının söz konusu içeriğe ulaşmasının amaçlandığını ortaya koymalıdır. Bu husus, sunuş biçiminden

---

[539] Dülger, **a.g.m.**, s. 8.
[540] Alman hukukunda web 2.0 destekli internet sitelerinin sorumlulukları hakkında bkz. Hoeren, **a.g.m.**, s. 576 vd.
[541] Mehmet Bedii Kaya, **Teknik ve Hukuki Boyutlarıyla İnternete Erişimin Engellenmesi**, XII Levha, 1. Baskı, İstanbul, Şubat 2010, s. 127-130.
[542] Durnagöl, **a.g.m.**, s. 401.

de "*açıkça"* anlaşılmalıdır. Nihayet, internet sitesinin sunuş biçiminden hem bağlantı sağlanan içeriğin benimsendiğinin hem de kullanıcının söz konusu içeriğe ulaşmasının amaçladığı anlaşılmalıdır. Sadece benimseme ya da sadece içeriğe ulaşılmasını amaçlama tek başına yeterli olmamaktadır. Bu noktada örneğin arama motorlarının ücret karşılığında bazı linkleri üst sıralara taşıması fiili, kullanıcının söz konusu içeriğe ulaşmasını amaçlayan bir kast içermekle birlikte, bağlantı sağlanan içeriği benimseme gibi bir kast içermemektedir[543]. Arama motorları bu işi ticari bir faaliyet olarak yürütmektedir. Bu nedenle, Kanunun 4. maddesi çerçevesinde arama motorlarına bizzat kendisinin ürettiği içerik dışında bağlantı sağladığı başkasına ait içerikten dolayı cezai sorumluluk yüklenmesi mümkün gözükmemektedir[544].

Eleştirilen ikinci husus ise genel hükümlere atıf yapılmasının belirsizlik içerdiğidir. Belirsizlik, atıf yapılan genel hükümlerden kastın TCK'da yer alan iştirak hükümleri mi yoksa Kanunun genel hükümleri mi olduğu yönündedir. Atfın iştirak hükümlerine göre ele alınması durumunda bağlantı sağlayan internet sitesi sorumlularının bağlantı sağlama fiillerinin TCK'da yer alan iştirak hükümleri kapsamına girmediği belirtilmektedir[545]. Aslında burada sorunun çözümü, suç oluşturan bir içeriğe bağlantı sağlamanın ayrı bir suç oluşturup oluşturmadığının belirlenmesinde yatmaktadır. Suç oluşturan içeriğe bağlantı sağlamanın ayrı bir suç oluşturduğu kabul edildiğinde ise iştirak hükümlerine başvurulması söz konusu olmayacaktır. Ayrıca, burada genel hükümlere yapılan atıf, özel olarak iştirak hükümlerine veya genel olarak TCK'ya değil; sorumluluk öngören hukukun genel hükümlerine yapılan atıf mahiyetindedir. Alman Telemedya Kanununa göre de hizmet sağlayıcılar, kullanıma hazır bulundurdukları kendilerine ait bilgiden "*genel hükümlere"* göre sorumludur (md. 7). Alman hukukunda genel hükümlerden anlaşılan genel hukuk kurallarıdır[546].

---

[543] Arama motorlarının ücret karşılığında bazı linkleri üst sıralara taşımasının sorumluluk gerektirebileceği hakkında bkz. Mehmet Bedii Kaya, **a.g.e.**, s. 129.
[544] Özbek, **a.g.m.**, s. 111.
[545] Mehmet Bedii Kaya, **a.g.e.**, s. 129.
[546] Hoeren, **a.g.m.**, s. 562-564.

Doktrinde, 5651 sayılı Kanunda yer alan "*içerik sağlayıcı, internet ortamında kullanıma sunduğu her türlü içerikten sorumludur*" hükmünün interaktif siteler açısından objektif bir sorumluluk şekli içerdiği ileri sürülmüştür[547]. İleri sürülen görüşlere göre, 5651 sayılı Kanunun söz konusu hükmü çerçevesinde arama motorları, forum, blog, video paylaşım, sosyal paylaşım gibi sitelerin sorumluları, sitelerinde yayınlanan başkalarına ait içerikten dolayı herhangi bir kusurları bulunmamasına rağmen sorumlu tutulmaktadır[548]. Bu görüş, bağlantı sağlama kavramının dar yorumundan kaynaklanmaktadır. Bunun sonucu olarak interaktif yayıncılık yapan sitelerde yer alan başkalarına ait içeriği de söz konusu siteler tarafından üretilen içerik olarak değerlendirmektedir. Bir an için böyle olduğu düşünülse bile yine de söz konusu sitelerin objektif sorumluluğundan bahsedilemez. 5651 sayılı Kanun, her ne kadar "içerik sağlayıcı, internet ortamında kullanıma sunduğu her türlü içerikten sorumludur" hükmünü içerse de, bu sorumluluğun şekli kural olarak 5651 sayılı Kanunda düzenlenmemiş; genel sorumluluk hükümlerine gönderme yapılmıştır ve TCK'da da söz konusu internet sitesi sorumlularının objektif sorumluluğuna ilişkin bir hükme yer verilmemiştir. Tam aksine, TCK'nın 21. maddesi gereği suçun oluşması kastın varlığına bağlı olduğu için söz konusu internet sitelerinin sorumlularının, kendi internet sitelerinde yer alsa bile başkalarına ait içerikten dolayı sorumlu tutulmaları mümkün gözükmemektedir. Kastın varlığı açısından bir an için söz konusu internet sitesi sorumlularının kontrol yükümlülüğünün bulunduğu düşünülebilir. Ancak bu düşünce, internetin doğasına uygun düşmemektedir ve çoğu zaman fiilen imkansızdır. Söz konusu internet sitesi sorumlularına böyle bir kontrol yükümlülüğünü yükleyecek hiçbir haklı gerekçe de bulunmamaktadır[549].

Aslında aksi yönde yorumların ortaya çıkmasını engellemek açısından söz konusu internet sitesi sorumlularının, başkalarına ait içerikten dolayı

---

[547] Günaydın, **a.g.e.**, s. 127.
[548] Mehmet Bedii Kaya, **a.g.e.**, s. 127.
[549] İçel / Ünver, **a.g.e.**, s. 436.

sorumlu tutulmamalarına yönelik açık bir hükmün getirilmesi daha yerinde bir yaklaşım olacaktır[550].

Nihayet, 5651 sayılı Kanunda genel olarak ve söz konusu içerik sağlayıcılar açısından istisnaen sadece bir yerde dolaylı bir sorumluluk şekli öngörülmüştür: Kanunun 9. maddesine göre, içeriğin yayından çıkarılması ve cevap hakkı açısından sulh ceza hakiminin kararını söz konusu maddede belirtilen şartlara uygun olarak süresinde yerine getirmeyen sorumlu kişi, altı aydan iki yıla kadar hapis cezası ile cezalandırılır[551]. Bu sorumluluk şeklinin ise doğrudan kişinin kendi fiil ve kastından kaynaklanan bir sorumluluk şekli olduğu kuşkusuzdur.

"Sorumlu kişi", internet içeriğini internet ortamında yayınlayan ve bunu yöneten kişidir. *"Yayın sorumlusu"* ise Kanunun 9. maddesinde, içerik sağlayıcının tüzel kişi olması halinde içeriğin yönetiminden sorumlu kişi olarak ele alınmıştır.

2. Erişim Sağlayıcıların Cezai Sorumluluğu

Erişim sağlayıcıların, sadece kişilerin internete erişim sağlamalarına aracılık etmeleri ve içeriğin üretiminde bir etkilerinin olmamasından dolayı cezai bir sorumluluğa tabi tutulmaması gerekir. Ayrıca, kendileri aracılığıyla internette erişilen bilgilerin içeriklerinin hukuka uygun olup olmadığını ve sorumluluk gerektirip gerektirmediğini kontrol yükümlülüğüne tabi tutulmaması da gerekir. Böyle bir yükümlülük internetin gelişmesini engeller ve başkalarının fiilerinden dolayı erişim sağlayıcıların sorumlu tutulması gibi adaletsiz bir uygulama ortaya çıkarır. Ayrıca, teknik olarak internette yer alan milyarlarca bilginin hukuka uygunluk açısından kontrol edilmesi mümkün değildir[552].

Erişim sağlayıcılar kendileri aracılığıyla erişim sağlanan içerikten sorumlu tutulmamalarına ve içeriği hukuka uygunluk açısından denetlemekle

---

[550] Aynı durum, e-Ticaret Direktifi ve Alman Telemedya Kanunu açısından da geçerlidir. Anılan Direktif ve Kanunda arama motorları ve web 2.0 teknolojisini kullanan internet sitelerine özgü bir düzenlemeye yer verilmemiştir. Hoeren, **a.g.m.**, s. 573.

[551] Bu hükmün arama motorları açısından uygulanamayacağı hakkında bkz. Gürkaynak / Yıldız / Kara, **a.g.m.**, s. 4.

[552] Yıldız, **a.g.e.**, s. 90.

yükümlü olmamalarına rağmen acaba erişim sağlanan içeriğin hukuka aykırı olduğu konusunda yetkili makamlarca bilgilendirilmeleri ve teknik olarak söz konusu içeriğe erişimi engellemelerinin mümkün olması durumunda bir yükümlülüğe tabi kılınabilirler mi? Bu durumda artık erişim sağlayıcılar açısından aracılık unsuru ortadan kalkmakta, erişim sağlanan hukuka aykırı içeriğe doğrudan yetkili makamlarca işaret edilmektedir. Şu halde, bu son durumda erişim sağlayıcılar açısından bazı yükümlülükler öngörülmesi söz konusu olabilmelidir[553].

e-Ticaret Direktifi erişim sağlayıcıların sorumluluğu açısından benzer bir yaklaşımı esas almıştır. Direktife göre, hizmetin alıcısı tarafından sağlanan bilginin bir iletişim ağı içerisinde iletimi veya bir iletişim ağına erişim sağlayanlar açısından üye devletler aşağıdaki koşullarda servis sağlayıcının bilgi iletiminden sorumlu tutulmamasını güvence altına alır *(basit iletim - mere conduit)*:

a. Sağlayıcı iletimi başlatmamışsa.

b. İletimin alıcısını seçmemişse ve

c. İletimin kapsadığı bilgiyi seçmemiş veya değiştirmemişsse (md. 12).

Direktifde "*ön belleğe alma" (caching)* ise ayrıca düzenlenmiştir. Buna göre hizmetin alıcısı tarafından sağlanan bilginin bir iletişim ağı içerisinde iletimi durumunda üye devletler, servis sağlayıcının, bilginin sırf istekleri üzerine diğer hizmet alıcılarına iletimini daha etkili hale getirmek amacıyla otomatik, ara ve geçici bir şekilde saklanmasından aşağıdaki koşullarda sorumlu tutulmamasını güvence altına alır (md. 13):

a. Sağlayıcı, bilgiyi değiştirmemişse.

b. Sağlayıcı, bilgiye erişim şartlarına uygun davranmışsa.

c. Sağlayıcı, özellikle sektör tarafından genel olarak tanındığı ve kullanıldığı şekilde bilginin güncellenmesine ilişkin kurallara uygun davranmışsa.

---

[553] Yana Breindl, Joss Wright, "Internet Filtering Trends in Western Liberal Democracies: French and German Regulatory Debates", http://www.academia.edu/2870660/internet_Filtering_Trends_in_Western_Liberal_Democracies_French_and_German_Regulatory_Debates, 15.03.2013, s. 2.

d. Sağlayıcı, bilginin kullanımına ilişkin veriyi elde etmek için, sektör tarafından genel olarak tanınan ve kullanılan teknolojinin hukuka uygun kullanımına müdahale etmiyorsa.

e. Sağlayıcı, ilk yayın kaynağındaki bilginin ağdan kaldırıldığına veya erişimin engellendiğine ilişkin bilgi elde ettiğinde veya erişimin engellenmesine ya da bilginin kaldırılmasına ilişkin bir mahkeme veya idari bir karar bulunduğunu öğrendiği zaman bilgiye erişimi engellemek veya çıkarmak için hemen harekete geçmişse.

Direktife göre, erişim sağlayıcıların sorumluluğu açısından getirilen güvence niteliğindeki hükümler, üye devletlerin, hukuk sistemlerine göre bir mahkeme veya idari otoritenin servis sağlayıcıdan ihlali sona erdirmesi veya önlemesini talep etme imkanını ortadan kaldırmamaktadır (md. 12/3). Erişim sağlayıcıların genel izleme ve kontrol yükümlülüğü ise bulunmamaktadır (md. 15/1). Ancak, Direktife göre üye devletler bilgi toplumu hizmet sağlayıcıları için kanuna aykırı olduğu iddia edilen faaliyetler konusunda yetkili kamu kurumlarını hemen bilgilendirme veya yetkili kamu kurumlarının talebi üzerine aralarında saklama sözleşmesi bulunan hizmet alıcılarının kimliklerine imkan tanıyan bilgiye ilişkin olarak onlarla iletişime geçilmesine yönelik zorunluluklar getirebilir (md. 15/2).

Bu esaslar Türk hukuk sisteminde de karşılığını bulmuştur. 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanuna göre cezai sorumluluk açısından erişim sağlayıcı, kendisi aracılığıyla erişilen bilgilerin içeriğinin hukuka aykırı olup olmadığını ve sorumluluk gerektirip gerektirmediğini kontrol etmekle yükümlü değildir (md. 6/2). Böyle bir yükümlülük öngörülmeyerek, erişim sağlayıcıların erişim sağladıkları içerikten sorumlu tutulmamaları amaçlanmıştır. Doktrinde Kanunun bu yaklaşımı olumlu değerlendirilmektedir[554].

Erişimine aracılık ettikleri içerikten sorumlu tutulmamakla birlikte, erişim sağlayıcıların uymaları gereken bazı yükümlülükler öngörülmüştür.

[554] Dülger, **a.g.m.**, s. 9.

5651 sayılı Kanuna göre erişim sağlayıcı, herhangi bir kullanıcısının yayınladığı hukuka aykırı içerikten, yargı mercilerinin koruma tedbiri kapsamında verdiği erişimi engelleme kararı doğrultusunda haberdar edilmesi halinde ve teknik olarak engelleme imkanı bulunduğu ölçüde erişimi engellemekle yükümlüdür (md. 6/1, a). Bu çerçevede koruma tedbiri olarak verilen erişimin engellenmesi kararının gereğini yerine getirmeyen erişim sağlayıcısının sorumlusu, fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde, altı aydan iki yıla kadar hapis cezası ile cezalandırılacaktır.

Erişim sağlayıcılar açısından her ne şekilde olursa olsun cezai bir sorumluluk öngörülmesi eleştirilebilir. Yürüttükleri ticari bir faaliyetten dolayı öngörülen regule edici düzenlemelerin yerine getirilmemesinden dolayı erişim sağlayıcıların faaliyetlerinin cezai sorumluluk sistemi yerine idari sorumluluk sistemi ile karşılanması çok daha adil ve yerinde olacaktır.

Genel olarak, 5651 sayılı Kanunun erişim sağlayıcılar açısından öngördüğü sorumluluk sisteminin e-Ticaret Direktifi ile uyumlu olduğu söylenebilir.

Erişim sağlayıcıların sorumluluğuna ilişkin 5651 sayılı Kanunda yer alan hükümler Alman Telemedya Kanununda yer alan hükümler ile benzerlik göstermektedir[555]. Alman Telemedya Kanununa göre hizmet sağlayıcılar, bir iletişim ağı içerisinde ilettikleri veya erişim sağladıkları üçüncü kişilere ait bilgiden dolayı kural olarak sorumlu tutulamaz. Ancak bu durumda hizmet sağlayıcıların,

1. iletimi başlatmaması,
2. İletilen bilginin adresini seçmemiş olması,
3. İletilen bilgiyi seçmemiş veya değiştirmemiş olması

gerekir. Servis sağlayıcının kasten kanuna aykırı bir fiilin işlenmesinde, sunduğu hizmetin alıcısı ile birlikte çalışması durumunda bu kural uygulanmaz. Erişim sağlayıcı, erişim sağlama faaliyeti yürütürken erişim

[555] İçel / Ünver, **a.g.e.**, s. 435. Genel olarak servis sağlayıcıların sorumluluğuna ilişkin benzer düzenlemeler Fransa'da Digital Ekonomide Güven Kanununda (Loi pour la Confiance dans I'Economie Numerique-LCEN) da yer almıştır. https://opennet.net/research/profiles/france, 15.03.2013.

sağladığı bilginin otomatik, ara ve geçici depolanmasından da, bu faaliyetin sadece iletişim ağı içerisinde iletimin gerçekleştirilmesi amacı ile yapılması ve bilginin iletim için gerekli olan süreden daha uzun bir süre depolanmaması kaydıyla sorumlu tutulamaz (md 8). Ayrıca, hizmet sağlayıcılar, bilginin iletiminin daha etkili bir şekilde gerçekleştirilebilmesi amacına özgü olmak üzere bilginin otomatik, ara ve geçici depolanmasından kural olarak sorumlu tutulamaz. Ancak bu durumda hizmet sağlayıcıların,

1. Bilgiyi değiştirmemesi,

2. Bilgiye erişim şartlarına uyması,

3. Özellikle sektör tarafından kabul edilen ve kullanılan, bilginin güncelleştirilmesine ilişkin kurallara uyması,

4. Bilginin kullanımı konusunda veri elde etmek için teknolojinin hukuka uygun kullanımına engel olmaması,

5. Mahkeme kararı veya idari bir kurumun kararı üzerine bilginin çıkarılması veya erişimin engellenmesi konusunda hemen harekete geçmesi,

gerekir (md. 9).

Nihayet, Alman Telemedya Kanununa göre erişim sağlayıcılar, erişim sağladıkları bilginin izlenmesi veya hukuka aykırı faaliyetlerin araştırılması konusunda bir yükümlülüğe tabi tutulamaz. Ancak bu durum, erişim sağlayıcılar açısından genel hükümlere göre bilginin çıkarılması veya engellenmesine ilişkin zorunluluğu ortadan kaldırmaz. Telekomünikasyon Kanununun 88. maddesine göre iletişimin gizliliğine ilişkin hükümler saklıdır (md 7).

Erişim sağlayıcıların sorumsuzluğuna ilişkim benzer bir hüküm ABD'de, İletişim Ahlak Kanununda (Communications Decency Act) da yer almıştır. Kanunun 230. maddesine göre, *"İnteraktif bir bilgisayar hizmetinin sağlayıcısı veya kullanıcısı, başka bir bilgi içerik sağlayıcısı tarafından sağlanan herhangi bir bilginin yayıncısı veya konuşmacısı olarak kabul edilemez. Bu bölüme aykırı herhangi bir eyalet veya yerel hukuk kuralına göre herhangi bir sorumluluk yüklenemez".*

3. Yer Sağlayıcıların Cezai Sorumluluğu

Yer sağlayıcılar erişim sağlayıcılar gibi başkaları tarafından üretilen içeriğin internette yayınlanmasında aracı konumundadır. Bu nedenle bunların da yer sağladıkları içerikten dolayı doğrudan sorumlu tutulmaması gerekir. Ayrıca, yer sağladıkları içerik konusunda bir kontrol yükümlülüğü öngörülmemelidir. Bu hem teknik açıdan hem de internetin gelişimi ve işin doğası gereği mümkün değildir[556]. Başkalarının ürettiği içerikten dolayı sorumlu tutulmamaları ceza sorumluluğuna ilişkin temel ilkelerdendir. Ancak, aynen erişim sağlayıcılar açısından olduğu gibi yer sağlayıcılar açısından da yetkili makamlarca bilgilendirilmeleri ve teknik olarak erişimi engellemelerinin mümkün olması durumunda, bunlardan hukuka aykırı içeriği engellemeleri beklenebilir.

e-Ticaret Direktifine göre, hizmetin alıcısı tarafından sağlanan bilginin saklanmasına ilişkin bilgi toplumu hizmetlerinde üye devletler şu koşulların gerçekleşmesi durumunda hizmet sağlayıcısının sorumlu tutulmamasını güvence altına alır:

a. Sağlayıcının, kanuna aykırı faaliyet veya bilgi hakkında bilgi sahibi olmaması ve zarar iddialarına ilişkin olarak kanuna aykırı faaliyet veya bilginin bulunduğuna dair durum ve koşullardan haberdar olmaması.

b. Sağlayıcının, böyle bir bilgiyi edinmesi veya fark etmesi üzerine hemen bu bilgiyi çıkarması veya bilgiye erişimi engellemesi (md. 14).

Direktife göre, yer sağlayıcıların sorumluluğu açısından getirilen güvence niteliğindeki hükümler, üye devletlerin, hukuk sistemlerine göre bir mahkeme veya idari otoritenin servis sağlayıcıdan ihlali sona erdirmesi veya önlemesini talep etme imkanını ortadan kaldırmamakta ve üye devletlerin bilgiye erişimi engellenmesi veya ortadan kaldırılmasını yöneten usullerin oluşturulması imkanını etkilememektedir (md. 12/3). Direktife göre yer sağlayıcıların genel izleme ve kontrol yükümlülüğü bulunmamaktadır (md. 15). Ancak, üye devletler bilgi toplumu hizmet sağlayıcıları için kanuna aykırı olduğu iddia edilen faaliyetler konusunda yetkili kamu kurumlarını hemen

---

[556] Yıldız, **a.g.e.**, s. 93.

bilgilendirme veya yetkili kamu kurumlarının talebi üzerine aralarında saklama sözleşmesi bulunan hizmet alıcılarının kimliklerine imkan tanıyan bilgiye ilişkin olarak onlarla iletişime geçilmesine yönelik zorunluluklar getirebilir (md. 15/2).

5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanuna göre yer sağlayıcı, yer sağladığı içeriği kontrol etmek veya hukuka aykırı bir faaliyetin söz konusu olup olmadığını araştırmakla yükümlü değildir (md. 5/1). Kanunun bu yaklaşımı oldukça yerinde olmuştur. Yer sağlayıcılar genellikle ticari faaliyet yürüten aracı işletmelerdir. Barındırdıkları içeriği kendileri üretmez; başkaları tarafından üretilen içeriği ticari bir faaliyet olarak sahip oldukları hizmet sunucuları ile barındırır. Yer sağlayıcılara, genel olarak yer sağlanan içeriği kontrol veya hukuk aykırı bir faaliyetin söz konusu olup olmadığını araştırma yükümlülüğünün getirilmesi bu sektörün faaliyet yürütemez hale gelmesine neden olur. Ayrıca, böyle bir yükümlülüğün tam anlamıyla yerine getirilmesi mümkün değildir. Ancak yer sağlayıcı, yer sağladığı hukuka aykırı içerikten, ceza sorumluluğu ile ilgili hükümler saklı kalmak kaydıyla, anılan Kanunun 8. ve 9. maddelerine göre haberdar edilmesi halinde ve teknik olarak imkan bulunduğu ölçüde hukuka aykırı içeriği yayından kaldırmakla yükümlü tutulmuştur (md. 5/2). Bu yükümlülüğün ihlali halinde, eğer bu ihlal koruma tedbiri olarak verilen erişimin engellenmesi kararının gereğinin yerine getirilmemesinden kaynaklanıyorsa, söz konusu yer sağlayıcının sorumluları hakkında, fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde altı aydan iki yıla kadar hapis cezası verilecektir (md. 8/10). İhlal, içeriğin yayından çıkarılması ve cevap hakkına ilişkin olarak sulh ceza hakiminin kararının 9. maddede belirtilen şartlara uygun olarak ve süresinde yerine getirilmemesinden kaynaklanıyorsa, sorumlu kişi hakkında altı aydan iki yıla kadar hapis cezası verilecektir. Yer sağlayıcının tüzel kişi olması halinde anılan ceza, yayın sorumlusu hakkında uygulanacaktır (md. 9).

5651 sayılı Kanunun 5. maddesinde yer alan “ceza sorumluluğu ile ilgili hükümler saklı kalmak kaydıyla” ibaresinin ifade ettiği anlam net değildir.

Hüküm sanki, yer sağlayıcının yer sağladığı hukuka aykırı içerikten dolayı cezalandırılmasına yönelik özel ceza normlarının bulunduğu yönünde bir anlam taşımaktadır. Ancak, yer sağlayıcının yer sağladığı içerikten dolayı, dolaylı bir şekilde cezalandırılabilmesine yönelik sadece 8. maddenin onuncu fıkrasında ve 9. maddede iki tane cezai hüküm öngörülmüştür. Bu nedenle, 5. maddede ceza sorumluluğu ile ilgili olarak saklı tutulan sorumluluk şeklinin 8. ve 9. maddelerde yer alan sorumluluk olduğu sonucuna varılabilir.

Yer sağlayıcılar açısından her ne şekilde olursa olsun cezai bir sorumluluk öngörülmesi doktrinde eleştirilmektedir. Bu görüşe biz de katılmaktayız. Yürüttükleri ticari bir faaliyetten dolayı öngörülen regule edici düzenlemelerin yerine getirilmemesinden dolayı yer sağlayıcıların faaliyetlerinin cezai sorumluluk sistemi yerine idari sorumluluk sistemi ile karşılanması çok daha adil ve yerinde olacaktır.

Genel olarak 5651 sayılı Kanunun yer sağlayıcılar açısından öngördüğü ceza sorumluluk sisteminin e-Ticaret Direktifi ile uyumlu olduğu söylenebilir.

Alman Telemedya Kanununa göre hizmet sağlayıcılar, bir hizmetin alıcısı için depolanan üçüncü kişilere ait bilgiden sorumlu tutulamaz. Ancak bu durumda hizmet sağlayıcıların,

1. Hukuka aykırı faaliyet veya bilgi konusunda bilgi sahibi olmaması, tazminat talepleri açısından hukuka aykırı faaliyetlerden haberdar olmaması,

2. Hukuka aykırı faaliyet veya bilginin edinilmesi durumunda, hemen hukuka aykırı bilginin çıkarılması veya erişimin engellenmesi,

yönünde hareket etmesi gerekir.

Hizmetin alıcısının, hizmet sağlayıcına bağlı olarak veya onun kontrolünde faaliyet göstermesi halinde yukarıdaki fıkra uygulanmaz (10). Ayrıca yer sağlayıcılar, yer sağladıkları bilginin izlenmesi veya hukuka aykırı faaliyetlerin araştırılması konusunda bir yükümlülüğe tabi tutulamaz. Ancak bu durum, yer sağlayıcılar açısından genel hükümlere göre bilginin çıkarılması veya engellenmesine ilişkin zorunluluğu ortadan kaldırmaz. Telekomünikasyon Kanununun 88. maddesine göre iletişimin gizliliğine ilişkin hükümler saklıdır (md 7).

4. Toplu Kullanım Sağlayıcıların Cezai Sorumluluğu

5651 sayılı Kanuna göre, ticari amaçlı olup olmadığına bakılmaksızın toplu kullanım sağlayıcılar, konusu suç oluşturan içeriğe erişimi önleyici tedbirleri almakla yükümlüdür (md. 7/2). Ancak, 5651 sayılı Kanunda toplu kullanım sağlayıcılar açısında ister ticari amaç taşıyan toplu kullanım sağlayıcı isterse ticari amaç taşımayan toplu kullanım sağlayıcı olsun, herhangi cezai bir yaptırım öngörülmemiştir. Kanunun bu yaklaşımının yerinde bir yaklaşım olduğu değerlendirilmektedir.

5. Kullanıcıların Cezai Sorumluluğu

Kural olarak, internet ortamından yararlanan ve herhangi bir içerik üretmeyen kullanıcıların cezai bir sorumluluk ile karşılaşmaması gerekir. Ancak, kullanıcılar açısından cezai sorumluluk, internet ortamında yer alan bir içeriğin indirilmesi durumunda söz konusu olabilir. Ayrıca kullanıcılar, e-posta ile yaptıkları iletişim açısından gönderdikleri e-postaların içeriğinden her durumda sorumludur.

Kullanıcı, içerik sağlayıcı konumuna geçtiği an artık ürettiği içerikten sorumlu hale gelmektedir. Özellikle web 2.0 destekli internet sitelerinin kullanılarak örneğin, bir forum sayfasında yorum yapılması durumunda artık kullanıcı konumunda olan kişi içerik sağlayıcı konumuna geçmektedir. Bu noktadan sonra söz konusu kişinin sorumluluğu kullanıcı açısından değil, içerik sağlayıcı açısından değerlendirilecektir.

B. İdari Sorumluluk

5651 sayılı Kanun yer sağlayıcılar, erişim sağlayıcılar ve toplu kullanım sağlayıcılar açısından bazı yükümlülükler ve bu yükümlülüklere uyulmaması durumunda uygulanacak para cezaları öngörmüştür. Doktrinde, Kanunun bu yaklaşımı genel olarak olumlu bulunmuş; ancak internetin

gelişimi açısından Kanun ile öngörülen yüksek idari para cezalarının engelleyici bir durum oluşturacağı ifade edilmiştir[557].

Bu bölümde içerik, erişim, yer ve toplu kullanım sağlayıcıların sorumluluğu sadece 5651 sayılı Kanun çerçevesinde idari sorumluluk açısından incelenecektir.

1. İçerik Sağlayıcıların İdari Sorumluluğu

a. Bilgilendirme Yükümlülüğü

5651 sayılı Kanun ile içerik sağlayıcılara yönetmelikle belirlenen esas ve usuller çerçevesinde tanıtıcı bilgilerini kendilerine ait internet ortamında kullanıcıların ulaşabileceği şekilde ve güncel olarak bulundurma yükümlülüğü getirilmiştir (md. 3/1). İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik ile bu yükümlülüğün kapsamı, "*ticari veya ekonomik amaçlı içerik sağlayıcılar"* olarak sınırlandırılmıştır[558]. Kanunda, bu yükümlülüğü yerine getirmeyenlere Başkanlık tarafından ikibin Türk Lirasından onbin Türk Lirasına kadar idari para cezası verileceği öngörülmüştür (md. 3/2).

Anılan düzenleme ile her türlü içerik sağlayıcıya değil, ticari veya ekonomik amaçlı içerik sağlayıcılara böyle bir yükümlülük getirilmiştir. Ancak, hangi tür içerik sağlayıcıların ticari veya ekonomik amaçlı içerik sağlayıcı olduğunun çoğu zaman anlaşılmasındaki zorluk nedeniyle, bu hükmün arzu edildiği gibi uygulanabilmesinde sorunlar ortaya çıkmaktadır.

---

[557] İçel, **a.g.m.**, s. 20-21.

[558] İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmeliğin 5. maddesine göre, *"Ticari veya ekonomik amaçlı içerik sağlayıcıları, ... aşağıda belirtilen tanıtıcı bilgilerini, kendilerine ait internet ortamında, kullanıcıların ana sayfadan doğrudan ulaşabileceği şekilde ve iletişim başlığı altında, doğru, eksiksiz ve güncel olarak bulundurmakla yükümlüdür:*

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 yapılıyor ise, yetkili denetim merciine ilişkin bilgiler.

(2) Ticari veya ekonomik amaçlı içerik sağlayıcı, birinci fıkradaki bilgilerle birlikte, yer sağlayıcıya ilişkin tanıtıcı bilgileri, doğru, eksiksiz ve güncel olarak ana sayfasında bulundurmakla yükümlüdür".

Bildirme yükümlülüğü birçok açıdan önem taşımaktadır. Örneğin, suç unsuru taşıyan içerik nedeniyle içerik sağlayıcılara ulaşılmak istenmesi durumunda[559] veya kişilerin içeriğin yayından çıkarılmasını talep ve cevap hakkını kullanılabilmeleri için haklarının ihlal edildiğini düşündükleri internet sitesi yetkililerinin iletişim bilgilerine ulaşabilmeleri gerekir. Bu düzenleme buna imkan sağlamaktadır.

e-Ticaret Direktifinin 5. maddesinde servis sağlayıcıların bilgilendirme yükümlülüğü düzenlenmiştir. Buna göre, Birlik hukuku tarafından öngörülen diğer bilgilendirme yükümlülüklerine ek olarak üye devletler asgari olarak şu bilgilerin kolayca, doğrudan ve sürekli bir şekilde hizmetin alıcıları ve yetkili kamu kurumları tarafından erişilebilir olmasını mümkün kılar:

a) Servis sağlayıcının adı,

b) Servis sağlayıcının kurulduğu yerin coğrafik adresi,

c) Elektronik posta adresi dahil, hızlı bir şekilde irtibat sağlanması ve doğrudan ve etkili bir şekilde iletişime geçilmesine imkan tanıyan servis sağlayıcı hakında ayrıntılı bilgi,

d) Servis sağlayıcının ticari kayıt yaptırdığı yer, kaydı yapan kuruluş ve kayıt numarası,

e) Yürütülen faaliyetin ruhsat rejimine tabi olduğu yer, özellikle ilgili gözetim otoritesi,

f) Düzenlenmiş meslekler (regulated professions) ile ilgili olarak,

- Servis sağlayıcının kayıt yaptırdığı mesleki veya benzer bir kuruluş,

- Mesleki unvan ve bunun hangi üye devlet tarafından verildiği,

- Üye devlet tarafından oluşturulan uygulanabilir mesleki kuralların refere edilmesi ve bunlara erişim imkanının gösterilmesi,

g) Servis sağlayıcının katma değer vergisine konu faaliyeti yüklendiği yer, vergi kimlik numarası.

Ayrıca, yine Birlik hukuku tarafından öngörülen diğer bilgilendirme yükümlülüklerine ek olarak üye devletler asgari olarak bilgi toplumu hizmetlerinin fiyatlarının geçerli olduğu yerin; fiyatların açık, belirli ve özellikle

[559] Dülger, **a.g.m.**, s. 6.

vergi ve teslimat masraflarını içerip içermediğinin gösterilmesi hususunda gerekeni yapmalıdır[560].

b. Kişisel Verileri Koruma Yükümlülüğü

Kişisel verilerin korunması yükümlülüğü açısından içerik sağlayıcılar üzerinde genellikle cezai yaptırım ve hukuksal sorumluluk mekanizmaları öngörülmekle birlikte bazı durumlarda idari yaptırım mekanizmaları da öngörülebilmektedir. Kişisel verileri hukuka aykırı işleyen kişiler hakkında idari para cezası, güvenlik önlemlerinin artırılması, verilerin açıklanmaması, veri aktarımının durdurulması ve verilerin silinmesi gibi kararların alınması mümkündür[561].

2. Erişim Sağlayıcıların İdari Sorumluluğu

5651 sayılı Kanunda, idari yükümlülük ve sorumluluk açısından erişim sağlayıcı, kendisi aracılığıyla erişilen bilgilerin içeriğinin hukuka aykırı olup olmadığını ve sorumluluk gerektirip gerektirmediğini kontrol etmekle yükümlü tutulmamıştır (md. 6/2). Bununla birlikte, erişim sağlayıcılara ilişkin bazı idari yükümlülükler ve bu yükümlülüklere uyulmaması durumunda bazı idari yaptırımlar öngörülmüştür.

a. Faaliyet Belgesi Alma Yükümlülüğü

Türkiye Cumhuriyeti sınırları içerisinde erişim sağlayıcı olmak isteyen sermaye şirketleri, hizmet vermeye başlamadan önce BTK tarafından düzenlenecek faaliyet belgesini almakla yükümlüdür[562]. Faaliyet belgesi alınmadan erişim sağlayıcı olarak faaliyette bulunulamaz.

---

[560] e-Ticaret Direktifindeki bu düzenleme, erişim ve yer sağlayıcıları da kapsamaktadır.
[561] Civelek, **a.g.e.**, s. 176.
[562] Telekomünikasyon Kurumu Tarafından Erişim Sağlayıcılara ve Yer Sağlayıcılara Faaliyet Belgesi Verilmesine İlişkin Usul ve Esaslar Hakkında Yönetmelik, md. 4. Ayrıntılı bilgi için bkz. Durnagöl, **a.g.m.**, s. 383.

b. Bilgilendirme Yükümlülüğü

İçerik sağlayıcılar açısından getirilen bilgilendirme yükümlülüğünün benzeri erişim sağlayıcılar açısından da getirilmiştir. Aynı şekilde, bu yükümlülüğü yerine getirmeyenlere Başkanlık tarafından idari para cezası verileceği öngörülmüştür[563].

c. Erişimi Engelleme Yükümlülüğü

Erişim sağlayıcı, herhangi bir kullanıcısının yayınladığı hukuka aykırı içerikten, TİB'in re'sen verdiği erişimi engelleme kararı doğrultusunda haberdar edilmesi halinde ve teknik olarak engelleme imkanı bulunduğu ölçüde erişimi engellemekle yükümlüdür (5651, md. 6/1, a). Bu çerçevede idari tedbir olarak verilen erişimin engellenmesi kararının yerine getirilmemesi halinde, TİB tarafından erişim sağlayıcısına idari para cezası verilir. İdari para cezasının verildiği andan itibaren yirmidört saat içinde kararın yerine getirilmemesi halinde ise TİB'in talebi üzerine BTK tarafından yetkilendirmenin iptaline karar verilebilir (md. 8/11). Kararı yerine getirmeyen işletmecinin kablolu ve kablosuz internet servis sağlayıcısı olması halinde, telekomünikasyon hizmeti sunumuna yönelik genel izni BTK tarafından iptal edilir. İşletmecinin, bunun dışında bir telekomünikasyon hizmeti sunumuna yönelik yetkilendirme ile erişim sağlayıcılığı hizmeti sunuyor olması halinde ise, yetkilendirilmesi kapsamındaki erişim sağlayıcılığı hizmetleri askıya alınır[564].

ç. Trafik Bilgisi Tutma Yükümlülüğü

Erişim sağlayıcı, sağladığı hizmetlere ilişkin yönetmelikte belirtilen trafik bilgilerini altı aydan az ve iki yıldan fazla olmamak üzere yönetmelikte belirlenecek süre kadar saklamakla ve bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini sağlamakla yükümlüdür (5651, md. 6/1, b). İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında

[563] Bkz. 5651 sayılı Kanun, md. 3 ve İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik, md. 5.
[564] Telekomünikasyon Kurumu Tarafından Erişim Sağlayıcılara ve Yer Sağlayıcılara Faaliyet Belgesi Verilmesine İlişkin Usul ve Esaslar Hakkında Yönetmelik, md. 19.

Yönetmelikte bu yükümlülük, erişim sağlayıcının sağladığı hizmetlere ilişkin olarak TİB'in Kanunla ve ilgili diğer mevzuatla verilen görevlerini yerine getirebilmesi için; erişim sağlayıcı trafik bilgisini[565] bir yıl saklama, bu bilgilerin doğruluğunu, bütünlüğünü oluşan verilerin dosya bütünlük değerini[566] zaman damgası[567] ile birlikte muhafaza ve gizliliğini temin etme, internet trafik izlemesinde[568] TİB'e gerekli yardım ve desteği sağlama, faaliyet belgesinde yer alan TİB'in uygun gördüğü bilgileri talep edildiğinde bildirme ve ticari amaçlı internet toplu kullanım sağlayıcılar için belirli bir IP bloğundan sabit IP planlaması yapma ve bu bloktan IP adresi verme[569] yükümlülüklerini içerecek şekilde genişletilmiştir (md. 8/1, b). Bu yükümlülüklerden herhangi birini yerine getirmeyen erişim sağlayıcısına TİB tarafından onbin Türk Lirasından ellibin Türk Lirasına kadar idari para cezası verilir (5651 sayılı Kanun md. 6/3).

Bir an için yönetmelik ile 5651 sayılı Kanunda yer alan söz konusu yükümlülüğün kapsamının genişletilemeyeceği düşünülebilir. Ancak, hem 5651 sayılı Kanun (md. 6/1, b) hem de 5326 sayılı Kabahatler Kanunu (md. 4/1) buna imkan tanımaktadır.

---

[565] 5651 sayılı Kanunda trafik bilgisi, internet ortamında gerçekleştirilen her türlü erişime ilişkin olarak taraflar, zaman, süre, yararlanılan hizmetin türü, aktarılan veri miktarı ve bağlantı noktaları gibi değerler olarak tanımlanmıştır (md. 2/1, j). İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelikte ise "*erişim sağlayıcı trafik bilgisi"*, internet ortamında yapılan her türlü erişime ilişkin olarak abonenin adı, kimlik bilgileri, adı ve soyadı, adresi, telefon numarası, sisteme bağlantı tarih ve saat bilgisi, sistemden çıkış tarih ve saat bilgisi, ilgili bağlantı için verilen IP adresi ve bağlantı noktaları gibi bilgiler olarak tanımlanmıştır (md. 3/1, g).

[566] İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelikte "*dosya bütünlük değeri"*, bir bilgisayar dosyasının içindeki bütün verilerin matematiksel işlemden geçirilmesi sonucu elde edilen ve dosyanın içerisindeki verilerde bir değişiklik yapılıp yapılmadığını kontrol için kullanılan dosyanın özünü belirten değer olarak tanımlanmıştır (md. 3/1, d.).

[567] 5070 sayılı Elektronik İmza Kanununda "*zaman damgası"*, bir elektronik verinin, üretildiği, değiştirildiği, gönderildiği, alındığı ve/veya kaydedildiği zamanın tespit edilmesi amacıyla, elektronik sertifika hizmet sağlayıcısı tarafından elektronik imzayla doğrulanan kayıt olarak tanımlanmıştır (md. 3/1, h).

[568] İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelikte "*izleme"*, internet ortamındaki verilere etki etmeksizin bilgi ve verilerin takip edilmesi olarak tanımlanmıştır (md. 3/1, j).

[569] İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelikte "*sabit IP adresi"*, belirli bir ağa bağlı cihazların birbirini tanımak, birbiriyle iletişim kurmak ve birbirlerine veri yollamak için kullandıkları, zamana ve oturuma göre değişmeyen ve sistem yöneticisi tarafından belirlenip tanımlanan ve değiştirilebilen IP adresi olarak tanımlanmıştır (md. 3/1, n)

d. Faaliyetine Son Verme Bildirim Yükümlülüğü

Erişim sağlayıcı, faaliyetine son vereceği tarihten en az üç ay önce durumu BTK'ya, içerik sağlayıcılarına ve müşterilerine bildirmek ve trafik bilgilerine ilişkin kayıtları yönetmelikte belirtilen esas ve usullere uygun olarak BTK'ya teslim etmekle yükümlüdür (5651, md. 6/1, c)[570]. Bu yükümlülüğü yerine getirmeyen erişim sağlayıcısına TİB tarafından onbin Türk Lirasından ellibin Türk Lirasına kadar idari para cezası verilir (md. 6/3).

e. Diğer Yükümlülükler

Erişim sağlayıcılar açısından yukarıda yer alan yükümlülükler dışında diğer bazı idari yükümlülükler de öngörülmüştür. İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelikte erişim sağlayıcılara, genel hatlarıyla, toptan hizmet verdiği abonelere ilişkin bilgileri TİB'e gönderme, erişimin engellenmesi kararlarının gerektiği gibi uygulanabilmesi açısından gerekli donanım ve yazılımı kurma, vekil sunucu trafik bilgisini saklama[571] ve abone bilgilerinin gizliliğini sağlama yükümlülükleri öngörülmüştür. Ancak, bu yükümlülükler için idari bir yaptırım getirilmemiştir.

3. Yer Sağlayıcıların İdari Sorumluluğu

İdari yükümlülük ve sorumluluk açısından yer sağlayıcı, yer sağladığı içeriği kontrol etmek veya hukuka aykırı bir faaliyetin söz konusu olup olmadığını araştırmakla yükümlü tutulmamıştır. (md. 5/1). Bununla birlikte 5651 sayılı Kanun, yer sağlayıcılara ilişkin bazı idari yükümlülükler ve bu yükümlülüklere uyulmaması durumunda bazı idari yaptırımlar öngörmüştür.

---

[570] Bkz. İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik, md. 8/1, c.

[571] İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelikte "*vekil sunucu trafik bilgisi"*, internet 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 saat bilgisi gibi bilgiler olarak tanımlanmıştır (md. 3/1, ö).

a. Faaliyet Belgesi Alma Yükümlülüğü

Türkiye Cumhuriyeti sınırları içerisinde yer sağlayıcı olarak faaliyet göstermek isteyen gerçek veya tüzel kişiler, hizmet vermeye başlamadan önce BTK tarafından düzenlenecek faaliyet belgesini almakla yükümlüdür. Türkiye Cumhuriyeti sınırları içerisinde, yer sağlayıcı faaliyet belgesi almaksızın yer sağlayıcılığı faaliyetinde bulunanların internet erişim hizmeti, TİB kararıyla ilgili erişim sağlayıcı tarafından durdurulur[572].

b. Bilgilendirme Yükümlülüğü

İçerik ve erişim sağlayıcılar açısından getirilen bilgilendirme yükümlülüğünün benzeri yer sağlayıcılar açısından da getirilmiştir. Aynı şekilde, bu yükümlülüğü yerine getirmeyenlere Başkanlık tarafından idari para cezası verileceği öngörülmüştür[573].

c. Trafik Bilgisi Tutma Yükümlülüğü

5651 sayılı Kanunda yer sağlayıcılar açısından böyle bir yükümlülük öngörülmemiştir. Ancak, İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelikte yer sağlayıcılar hakkında, yer sağlayıcı trafik bilgisini[574] altı ay saklama, bu bilgilerin doğruluğunu, bütünlüğünü oluşan verilerin dosya bütünlük değerini zaman damgası ile birlikte saklama ve gizliliğini temin etme yükümlülüğü getirilmiştir (md. 7/1, c).

Telekomünikasyon Kurumu Tarafından Erişim Sağlayıcılara ve Yer Sağlayıcılara Faaliyet Belgesi Verilmesine İlişkin Usul ve Esaslar Hakkında Yönetmeliğe göre Türkiye Cumhuriyeti sınırları içerisindeki yerleşik yer sağlayıcının bu Yönetmelikteki yükümlülüklerini yerine getirmemesi halinde

---

[572] Telekomünikasyon Kurumu Tarafından Erişim Sağlayıcılara ve Yer Sağlayıcılara Faaliyet Belgesi Verilmesine İlişkin Usul ve Esaslar Hakkında Yönetmelik, md. 4.

[573] Bkz. 5651 sayılı Kanun, md. 3 ve İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik, md. 5.

[574] İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelikte "*yer sağlayıcı trafik bilgisi"*, internet ortamında her türlü yer sağlamaya ilişkin olarak kayak IP adresi, hedef IP adresi, bağlantı tarih ve saat bilgisi, istenen sayfa adresi, işlem bilgisi (GET, POST komut detayları) ve sonuç bilgileri gibi bilgiler olarak tanımlanmıştır (md. 3/1, ş).

faaliyet belgesi BTK tarafından iptal edilebilir (md. 19/3)[575]. Şu durumda, trafik bilgisi saklama yükümlülüğünü yerine getirmeyen yer sağlayıcı hakkında "*faaliyet belgesinin iptali"* yaptırımı uygulanabilir. Yönetmeliğin bu hükmü ile aslında kanunda yer almayan bir yaptırım türü öngörülmüştür. 5326 sayılı Kabahatler Kanununda yer alan "*kanunilik ilkesi"* gereği, idari yaptırımların türü, süresi ve miktarı ancak kanunla düzenlenebilir (md. 4/2)[576]. Bu nedenle, anılan Yönetmelik hükmü hukuka aykırı nitelik taşımaktadır.

4. Toplu Kullanım Sağlayıcıların İdari Sorumluluğu

5651 sayılı Kanun, tabi olacakları yükümlülük ve sorumluluk bakımından ticari amaç taşımayan toplu kullanım sağlayıcılar ile ticari amaç taşıyan toplu kullanım sağlayıcıları birbirinden ayırmış ve ayrı düzenlemelere tabi tutmuştur.

a. Ticari Amaç Taşımayan Toplu Kullanım Sağlayıcıların İdari Yükümlülük ve Sorumlulukları

(1) Suç Oluşturan İçeriğe Erişimi Engelleme Yükümlülüğü

Ticari amaç taşımayan toplu kullanım sağlayıcı, konusu suç oluşturan içeriğe erişimi önleyici tedbirleri almakla yükümlüdür (5651, md. 7/2). Bu yükümlülüğe uyulmaması durumunda uygulanabilecek idari bir yaptırım öngörülmemiştir. Ticari amaç taşımayan toplu kullanım sağlayıcılar açısından söz konusu yükümlülüğün kapsamı oldukça geniş ele alınmış; suç oluşturan her türlü içeriğe erişimi engelleme yükümlülüğü getirilmiştir[577].

(2) İç IP Dağıtım Loglarını Kaydetme Yükümlülüğü

Kanunda yer almayan bu yükümlülük internet Toplu Kullanım Sağlayıcıları Hakkında Yönetmelikte yer almıştır. Yönetmeliğe göre, ticari

---

[575] Durnagöl, **a.g.m.**, s. 398.
[576] Ramazan Çağlayan, **İdari Yaptırımlar Hukuku**, Asil Yayın Dağıtım, 1. Baskı, Ankara, 2006, s. 132.
[577] Durnagöl, **a.g.m.**, s. 404.

amaç taşımayan toplu kullanım sağlayıcı, iç IP Dağıtım Loglarını[578] elektronik ortamda kendi sistemine kaydetmekle yükümlüdür (md. 4/1, b). Bu yükümlülüğe uyulmaması durumunda uygulanabilecek idari bir yaptırım öngörülmemiştir.

b. Ticari Amaç Taşıyan Toplu Kullanım Sağlayıcıların İdari Yükümlülük ve Sorumlulukları

(1) İzin Belgesi Alma Yükümlülüğü

Ticari amaç taşıyan toplu kullanım sağlayıcı, mahalli mülki amirden izin belgesi almakla yükümlüdür (5651, md. 7/1). Bu yükümlülüğe aykırı hareket eden kişiye mahalli mülki amir tarafından üç bin Türk Lirasından onbeşbin Türk Lirasına kadar idari para cezası verilir (md. 7/3).

İnternet Toplu Kullanım Sağlayıcıları Hakkında Yönetmelikte, mülki idare amirlerince izin alınmadan açıldığı tespit edilen işyerlerinin, mülki idare amirlikleri tarafından sebebi bir tutanakla belirlenmek ve mühürlenmek suretiyle re'sen kapatılacağı düzenlenmiştir (md. 7/1). Bu düzenleme idarenin re'sen icra yetkisinin bir sonucudur.

(2) Diğer Yükümlülükler

Ticari amaç taşıyan toplu kullanım sağlayıcı, konusu suç oluşturan içeriğe erişimi önleyici tedbirleri almakla yükümlüdür (5651, md. 7/2). Bu yükümlülüğün kapsamı konusu suç oluşturan her türlü içeriğe erişimi önleyici tedbirlerin alınmasına yönelik olarak oldukça geniş belirlenmiştir. Ancak, bu yükümlülük TİB tarafından belirlenen her türlü filterelemenin ticari amaç taşıyan toplu kullanım sağlayıcılar açısından uygulanması zorunluluğunu içermemektedir. Şöyle ki, ticari amaç taşıyan toplu kullanım sağlayıcılar açısından, 5651 sayılı Kanunun 10. maddesinin dördüncü fırasının (ç) bendi

---

[578] İnternet Toplu Kullanım Sağlayıcıları Hakkında Yönetmelikte "*İç IP Dağıtım Logu"*, 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 bilgiler olarak tanımlanmıştır.

çerçevesinde Başkanlık tarafından filtreleme ve bloke etmede kullanılacak sistemlere ve yapılacak düzenlemelere yönelik belirlenen esas ve usuller, sadece Kanunun 8. maddesinde sayılan suçlar açısından geçerli olacaktır. 5651 sayılı Kanunun amaç ve kapsamı, internet ortamında işlenen belirli suçlarla mücadele olarak belirlenmiş ve Kanun kapsamında belirli suçlar da 8. maddede sayılanlardan oluşmuştur. Şu halde, ticari amaç taşıyan toplu kullanım sağlayıcılar TİB tarafından belirlenen sadece 8. maddede sayılan suçlar açısından getirilen filtreleme sistemini uygulama yükümlülüğü altındadır. Bununla birlikte bu durum, ticari amaç taşıyan toplu kullanım sağlayıcıların diğer suçlar açısından da erişimi önleyici tedbirleri alma yükümlülüğünü Kanunun 7. maddesinin ikinci fıkrası kapsamında ortadan kaldırmamaktadır.

Kanunda, bu yükümlülüğe uyulmaması durumunda uygulanabilecek idari bir yaptırım öngörülmemiştir. Ancak, internet Toplu Kullanım Sağlayıcıları Hakkında Yönetmelikte, söz konusu yükümlülüğe aykırı hareket ettiği belirlenen ticari amaç taşıyan toplu kullanım sağlayıcılara, mülki idare amiri tarafından üçbin Türk Lirasından onbeşbin Türk Lirasına kadar idari para cezası verileceği düzenlenmiştir.

İnternet Toplu Kullanım Sağlayıcıları Hakkında Yönetmelik ile başka yükümlülükler de öngörülmüştür. Söz konusu Yönetmeliğe göre ticari amaç taşıyan toplu kullanım sağlayıcı, TİB tarafından onaylanan içerik filtreleme yazılımını kullanmak, erişim sağlayıcılardan sabit IP almak ve kullanmak, iç IP dağıtım loglarını elektronik ortamda kendi sistemlerine kaydetmek, TİB tarafından verilen yazılım ile kaydedilen iç IP dağıtım loglarına ilişkin bilgileri ve bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini teyit eden değeri kendi sistemlerine günlük olarak kaydetmek ve bu verileri bir yıl süre ile saklamakla yükümlüdür (md. 5/1) Yönetmeliğe göre, söz konusu yükümlülüklere aykırı hareket ettiği belirlenen ticari amaç taşıyan toplu kullanım sağlayıcılara, mülki idare amiri tarafından üçbin Türk Lirasından onbeşbin Türk Lirasına kadar idari para cezası verilir (md. 11/1).

5326 sayılı Kabahatler Kanununda yer alan "*kanunilik ilkesi*" gereği, idari yaptırımların türü, süresi ve miktarı ancak kanunla düzenlenebilir (md.

4/2). Bu nedenle, anılan Yönetmelik hükmü hukuka aykırı nitelik taşımaktadır[579]. Özellikle konusu suç oluşturan içeriğe erişimi önleyici tedbirlerin alınmasına yönelik olarak, bu tedbirleri yerine getirmeyen ticari amaç taşıyan toplu kullanım sağlayıcılara karşı kanun düzeyinde idari yaptırım sistemine ihtiyaç bulunmaktadır.

5. İdari Para Cezalarına Karşı Kanun Yolu

5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanuna göre, bu Kanunda tanımlanan kabahatler dolayısıyla Başkanlık veya Kurum tarafından verilen idari para cezalarına ilişkin kararlara karşı, 2577 sayılı İdari Yargılama Usulü Kanunu hükümlerine göre kanun yoluna başvurulabilir (md. 8/12). 5651 sayılı Kanunda böyle bir düzenleme yer almamış olsaydı bu Kanuna göre verilen idari para cezalarına karşı, 5326 sayılı Kabahatler Kanununun 3. ve 27. maddesine göre sulh ceza mahkemesine başvurmak gerekecekti. Ancak, bu düzenleme ile söz konusu kanun yolunun önü kapatılmıştır. Bu düzenleme bizce isabetli olmuştur. İdari işlemlere karşı açılan davaların uzmanlık mahkemeleri olan idari mahkemelerde görülmesi hem Anayasa gereğidir; hem de daha isabetlidir[580].

İdari Yargılama Usulü Kanunu hükümlerine göre kanun yoluna başvurulabilmesi, Kanunun geneli açısından geçerli olmakla birlikte sadece bir yerde istisnailik göstermektedir. Toplu kullanım sağlayıcıların yükümlülüklerinin düzenlendiği 7. maddeye göre alınması gereken izin belgesinin alınmaması durumunda uygulanacak idari para cezasının mahalli mülki amir tarafından yerine getirileceği düzenlenmiştir. 5651 sayılı Kanunun 8. maddesine göre İdari Yargılama Usulü Kanunu hükümleri çerçevesinde kanun yoluna başvurulabilmesi için ise idari para cezasının Başkanlık veya Kurum tarafından verilmesi gerekir. O halde, mülki idari amir tarafından

---

[579] Durnagöl, **a.g.m.**, s. 408.
[580] Yücel Oğurlu, **İdari Yaptırımlar Karşısında Yargısal Korunma**, Seçkin Yayınevi, Ankara, 2000, s. 127. Aksi yönde görüş için bkz. İçel, **a.g.m.**, s. 22.

uygulanan idari para cezalarına karşı Kabahatler Kanununun 3. ve 27. maddesi gereği ancak sulh ceza mahkemesine başvurulabilir.

C. Erişimin Engellenmesi [581]

İnternette yer alan içeriğe erişimin engellenmesi, günümüz dünyasında neredeyse her devletin başvurduğu hukuksal bir araç haline gelmiştir. Erişimin engellenmesi müessesesi, demokratik kabul edilmeyen ülkelerin düzenlemelerinde yer alabileceği gibi demokratik kabul edilen ülkelerin düzenlemelerinde de yer alabilmektedir[582]. Ancak, düzenlemenin niteliği, nedenleri, kapsamı, yöntemleri, usulü, sınırları ve sonuçları ülkeden ülkeye farklılık göstermektedir. Bu farklılıkların temel hak ve özgürlükler üzerinde ortaya çıkardığı etki ise düzenlemelerin demokratik olup olmadığının belirlenmesinde göz önünde bulundurulmaktadır.

Erişimin engellenmesi konusunda önemli bir nokta, düzenleme ile uygulamanın farklılık gösterebilmesidir. Çoğu zaman düzenlemelere aykırı uygulamalar ortaya çıkabildiği gibi filtreleme yöntemleri de düzenlemeye göre uygulama farklılığı yaratabilmektedir. Gizli veya şeffaf olmayan şekilde ya da tamamen uygulamaya dayanan erişim engellemeleri uygulama farklılığı yaratan diğer durumlardır[583]. Ayrıca, erişimin engellenmesi konusu ile ilgili düzenlemeler her zaman spesifik olarak bu alana özgü düzenlemeler olmamakta; kişilik haklarının korunması, fikri mülkiyet haklarının korunması, hakaretin önlenmesi gibi yerleşmiş hukuk kuralları da erişimin engellenmesi yaptırımının uygulanabilmesi açısından genişletilebilmektedir. Böyle durumlarda, mevcut düzenlemelerden ziyade uygulama yön gösterici olabilmektedir. Bu bölümde mümkün olduğunca devletlerin düzenlemeleri ile uygulamaları birlikte değerlendirilmeye çalışılacaktır.

---

[581] Bu başlık altında "*internet içeriğine erişimin engellenmesi"* incelenmiştir. "*İnternete erişimin kişisel olarak engellenmesi"* ise aşağıda ayrı bir başlık altında ele alınacaktır.
[582] Breindl / Wright, **a.g.m.**, s. 1. Deibert / Rohozinski, **a.g.m.**, s. 49.
[583] Doğan Kılınç, "Türk Hukukunda ve Mukayeseli Hukukta İnternet Sitelerine Erişimin Engellenmesi ve İfade Hürriyeti", **GÜHFD**, C. XIV, S. 2, 2010, s. 433.

Filtreleme, erişimin engellenmesi kavramı içerisinde yer almakla birlikte önemi ve farklılığına binaen aşağıda ayrı bir başlık altında incelenmiştir.

1. Tanımı

Erişimin engellenmesi, yetkili kamusal merciler tarafından hukuka aykırı bulunan internet içeriğine çeşitli teknik yöntemler uygulanarak kişilerin erişiminin engellenmesi olarak tanımlanabilir. Teknik ve hukuksal engelleme arasında ortaya çıkabilecek fark nedeniyle erişimin engellenmesi konusu incelenirken erişimin hukuksal olarak engellenmesi ile teknik olarak engellenmesi arasındaki farklılık göz önünde bulundurulmalıdır. Çoğu zaman hukuken engellenen içeriğe teknik olarak erişmek mümkün olabilmektedir.

"Erişimin engellenmesi" kavramı, kullanıcılara yönelik olduğundan kavramsal olarak eleştirilmektedir. Halbuki burada doğrudan kullanıcılara yönelik bir yaklaşım yerine içerik, erişim ve yer sağlayıcılara yönelik bir engelleme söz konusudur. Bu nedenle erişimin engellenmesi kavramı yerine "*iletişimin engellenmesi"* kavramının daha doğru bir kavram olduğu ileri sürülmektedir[584].

2. Yöntemleri

Erişimin engellenmesi alan adı, IP bloklaması veya nesne tabanlı (URL) engelleme şeklinde uygulanabilmektedir[585]. Alan adı engellemesinde, alan adı sunucularından ilgili alan adına erişim kapatılmaktadır. Bunun sonucu olarak ilgili alan adında yayın yapan internet sitesine erişim engellenmiş olmaktadır. IP bloklamada, ilgili internet sitesinin yayın yaptığı IP bloğuna erişim engellenmektedir. Nesne tabanlı engellemede ise internet sitesi yerine doğrudan hukuka aykırı içeriğin yer aldığı internet sayfasına (URL'ye) erişim engellenmektedir.

Alan adı engellemesi ve IP bloklaması internet sitesinin tamamına erişimi engellemektedir. Bu durum, söz konusu internet sitesinde yer alan

---

[584] Dülger, **a.g.m.**, s. 3.
[585] Kılınç, "Türk Hukukunda", s. 408-409. Breindl / Wright, **a.g.m.**, s. 2.

hukuka aykırı olmayan içeriğe de erişimin engellenmesi açısından sakıncalıdır ve temel hak ve özgürlükler üzerinde ağır müdahale oluşturmaktadır. Ayrıca, bir IP adresinde birden fazla alan adında içerik yayınlanması mümkün olduğundan IP bloklaması, hukuka aykırı içerik taşımayan internet sitelerine de erişimin engellenmesi sonucunu doğurabilir. IP bloklamasının sakıncalı yönü daha ağır basmaktadır. Nesne tabanlı engelleme, doğrudan hukuka aykırı olan internet sayfasına erişimi engelleyen bir yöntem olması nedeniyle erişimin engellenmesi açısından aslında en uygun ve doğru olan yöntemdir. Nesne tabanlı engelleme yöntemi, özellikle sosyal paylaşım siteleri veya blog siteleri gibi internet sitelerinde yer alan içerikten sadece hukuka aykırı ilgili sayfaya erişimin engellenmesi açısından oldukça uygundur[586]. Ancak, bu yöntemin uygulanması teknik olarak mümkün olmakla birlikte maliyetli olması ve internet hızını yavaşlatması nedeniyle uygulanamamaktadır[587]. Ülkemizde de nesne tabanlı engelleme yöntemi uygulanmamakta; bunun yerine alan adı veya IP bloklaması yöntemleri uygulanmaktadır.

3. Hukuksal Niteliği

Erişimin engellenmesi müessesesinin hukuksal niteliği belirlenirken erişimin engellenmesi kararının adli bir karar mı yoksa idari bir karar mı olduğu üzerinde durmak gerekir. Bu kararın adli bir karar olduğu sonucuna varılırsa kararın sadece adli merciler tarafından, idari bir karar olduğu sonucuna varılırsa idari merciler tarafından alınabilmesi söz konusu olur. Doktrinde genel olarak adli işlemler ile idari işlemler[588] arasındaki nitelik farkının belirlenmesine yönelik ciddi çabalar gösterilmiş ve tatmin edici bir sonuç ortaya konulamamıştır. Bu nedenle, genel olarak farklılığın nitelikten

---

[586] Craddock, **a.g.m.**, s. 5.
[587] Kılınç, "Türk Hukukunda", s. 409.
[588] *"İdari işlem, idare veya idare adına hareket eden özel hukuk kişilerince, kamu gücü kullanılarak yapılan; doğrudan ya da belli bir süreç içinde, rızaları olsun ya da olmasın kişi veya onlara ait nesnelerin hukuki durumlarını etkileyen, kamusal nitelikli, tek yanlı irade açıklamalarıdır"*. Akyılmaz / Sezginer / Kaya, **a.g.e.**, s. 368. "*İdari işlem, idari makamların kamu gücü ve usullerini kullanarak, tek yanlı iradeleriyle yapmış oldukları, hukuki etki ve sonuş doğuran işlemlerdir*". Ender Ethem Atay, **İdare Hukuku**, 3. Bası, Turhan Kitabevi, Ankara, 2012, s. 408.

değil, tamamen işlemi yapan organ ve işlemin şeklinden kaynaklandığı kabul edilmektedir. Buna göre, bağımsız bir yargı organı tarafından yargılama usulü uygulanarak yapılan işlemlerin adli, idare tarafından yapılan işlemlerin ise idari işlem olduğu ifade edilmektedir[589]. Genel kıstas bu olmakla birlikte, elbette yasa koyucuyu sınırlandıran Anayasal ilkeler bulunabilir. Örneğin, Anayasamızda bir tedbirin ancak hakim kararı ile alınabileceği düzenlenmişse artık bu noktadan sonra o tedbirin idari bir kararla alınabileceği söylenemez[590].

Erişimin engellenmesi tedbiri açısından konuya yaklaştığımız zaman bir görüş bu tedbirin nitelik itibariyle adli bir işlem olduğunu ileri sürmektedir[591]. Bu görüşün dayandığı gerekçe ise TİB'e verilen re'sen erişimi engelleme kararının alınmasında bu Kurumun bir suç değerlendirmesi yapacak olması; suç değerlendirmesi işlevinin ise adli nitelikte bir işlem olduğu hususudur[592]. Ayrıca bir diğer gerekçeye göre, AİHS (md. 6) ve Anayasamızda (md. 36) yer alan "*adil yargılanma hakkı"* gereği suç değerlendirilmesi ancak mahkemeler tarafından yapılabilir. Aksi durum adil yargılanma hakkına aykırılık oluşturur[593].

Bizce, bu konu tamamen kanun düzenleme tekniği ve yasa koyucunun temel hak ve özgürlüklere yaklaşımı ile ilgili bir husustur. Örneğin, kanun koyucu, "*çocukları cinsel olarak istismar eden veya müstehcen nitelikteki içeriğe erişim TİB tarafından engellenir"* şeklinde, suç değerlendirmesine atıf yapmaksızın bir düzenleme de öngörebilirdi. Yani, bu fiillerin suç oluşturmasına hiç atıf yapılmadan doğrudan bu fiiller tanımlanarak bir düzenleme de yapılabilirdi. Kanun koyucu bu yöntemi tercih etmemiş; bunun

---

[589] Feyyaz Gölcüklü, "İdari Ceza Hukuku ve Anlamı; İdarenin Cezai Müeyyide Tatbiki", **AÜSBFD**, Cilt. 18, Sayı. 2, 1963, s. 135. Turgut Tan, **İdare Hukuku**, Turhan Kitabevi, Ankara, 2011, s. 224-225. Erkut'a göre, idari işlemin kimliğinin belirlenmesinde hem organik ölçüt hem de foksiyonel ölçüt yetersiz kalmaktadır. Yapılması gereken bu iki ölçütün de göz önünde bulundurularak "idare işlevi" kavramına anlam kazandırmaktır. Bu çerçevede, idare işlevi kapsamında değerlendirilebilecek işlemler, yargı organı, yasama organı veya özel hukuk tüzel kişilerince de yapılsa aslında idari işlemdir. Celal Erkut, **İptal Davasının Konusunu Oluşturma Bakımından İdari İşlemin Kimliği**, Danıştay Yayınları, Ankara, 1990, s. 88-89.

[590] Gölcüklü, **a.g.m.**, s. 136.

[591] Akdeniz / Altıparmak, **a.g.e.**, s. 31-33. Özen / Baştürk, **a.g.e.**, s. 42-43. Dülger, **a.g.m.**, s. 25.

[592] Özen / Baştürk, **a.g.e.**, s. 42.

[593] Akdeniz / Altıparmak, **a.g.e.**, s. 31-32.

yerine mevcut düzenlemeyi tercih etmiştir. Yapılan tercihte aslında TİB'i, yapacağı değerlendirmede sınırlandırma arzusu yatmaktadır. Şöyle ki TİB tarafından erişimi engellenecek siteler hakkında yapılacak değerlendirmelerde sıkı bir kıstas olarak suç değerlendirmesinin öngörülmesi, temel hak ve özgürlükler açısından daha güvenceli bulunmuştur. Bu nedenle, erişimi engelleme kararının niteliğinin değerlendirilmesinde, suç değerlendirmesi yapılacak olmasını kıstas alarak erişimi engelleme kararının her durumda adli bir nitelik taşıyacağı ileri sürülemez. Erişimi engelleme kararının, suç değerlendirmesinden bağımsız olarak da pekala düzenlenmesi mümkündür.

TİB'in re'sen erişimi engelleme kararı almasında suç değerlendirmesi yapacak olması, re'sen erişimin engellenmesi kararı ile kişiler açısından cezai bir yaptırım öngörülmediğinden, adil yargılanma hakkına ilişkin söz konusu AİHS ve Anayasa hükümlerine de aykırılık oluşturmamaktadır. Aksini düşünmek, idarenin idari yaptırım öngören her türlü işlemini söz konusu AİHS ve Anayasa hükümlerine aykırı hale getirir[594]. Ayrıca, TİB'in re'sen erişimi engelleme kararlarına karşı idari yargı yolu her zaman açıktır. İdari yargı yolunun açık olduğu re'sen erişimi engelleme kararlarının dava açma hakkını engellediğinden de söz edilemez[595].

Şu halde, erişimin engellenmesi tedbirini nitelik itibariyle adli bir işlem olarak kabul etmenin imkanı bulunmamaktadır. Bu noktada sorunun çözümü, bu tedbirin ancak adli bir karar ile alınabileceğine yönelik Anayasal bir kuralın bulunup bulunmadığı konusunun açıklığa kavuşturulmasında yatmaktadır. Bu çerçevede karşımıza Anayasamızın haberleşme özgürlüğü (md. 22), ifade özgürlüğü (md. 26), basın özgürlüğü (md. 28) ve bilim ve sanat özgürlüğüne (md. 27) ilişkin hükümleri çıkmaktadır. Doktrinde bir kısım yazar, bir yargılama süreci olmaksızın idari mercilerin kararı ile erişimin engellenmesinin, kişi haklarını hukuk devletinin gereklerine aykırı bir şekilde

---

[594] Doktrinde hakim görüş, idari yaptırımların idari işlem niteliğinde olduğu yönündedir. Oğurlu, **İdari Yaptırımlar**, s. 121. Çağlayan, **a.g.e.**, s. 23-24. Ali Ulusoy, "İdari Ceza Hukuku'nun İşlevi ve Hukuk Düzeni İçindeki Yeri", **İdari Ceza Hukuku Sempozyumu**, Editörler: İlhan Ulusan / Funda Başaran Yavaşlar, TC İstanbul Kültür Üniversitesi, Seçkin Yayınları, Ankara, 2009, s. 48.

[595] Aksi görüş için bkz. Akdeniz / Altıparmak, **a.g.e.**, s. 33.

ihlal ettiğini ve devletin bu yolla keyfi bir uygulama yarattığını[596], bu uygulamanın TİB'e *"adli bir karar alma yetkisi"* verdiğini; idari bir kuruluşa adli bir yetkinin verilmesinin yetki gaspı anlamına geldiğini ileri sürmüştür. Aynı görüşe göre haberleşme özgürlüğü çerçevesinde erişimin engellenmesi kararı Anayasamızın 22. maddesi gereği ancak hakim kararı veya gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısının kararı ile alınabilir, aksi yöndeki uygulama söz konusu Anayasal hükümlere aykırılık oluşturur[597].

Anayasal hükümler açısından konuya yaklaştığımız zaman erişimin engellenmesi kararını sadece haberleşme özgürlüğü çerçevesinde değerlendirmek mümkün gözükmemektedir. Erişimin engellenmesi kararı haberleşme özgürlüğünü kısıtlayacağı gibi ifade özgürlüğü, basın özgürlüğü ve bilim ve sanat özgürlüğü gibi özgürlükleri de kısıtlayacak niteliktedir. Şu halde, temel hak ve özgürlükler açısından yapılacak değerlendirmelerde bu hükümlerin bir bütün olarak göz önünde bulundurulması gerekir.

Haberleşme özgürlüğü açısından Anayasamızda, herkesin haberleşme özgürlüğüne sahip ve haberleşmenin gizliliğinin esas olduğu belirtildikten sonra istisnai olarak milli güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlakın korunması veya başkalarının hak ve özgürlüklerinin korunması için bu özgürlüğün sınırlandırılabileceği; ancak bu sınırlandırmanın ancak usulüne göre verilmiş hakim kararı veya gecikmesinde sakınca bulunan hallerde kanunla yetkili kılınmış merciin yazılı emri ile yapılabileceği öngörülmüştür. Ayrıca, yetkili merciin kararının yirmidört saat içinde görevli hakimin onayına sunulması ve hakim kararının kırksekiz saat içinde açıklanması gerekmektedir. Aksi halde, bu karar kendiliğinden kalkacaktır (md. 22/1, 2).

Kural olarak haberleşme özgürlüğü ancak "*hakim kararı veya gecikmesinde sakınca bulunan hallerde kanunla yetkili kılınmış merciin yazılı emri ile"* sınırlandırılabilir. Ancak, bu kurala 22. maddenin üçüncü fıkrası ile bir istisna öngörülmüştür. Anılan fıkrada *"İstisnaların uygulanacağı kamu*

---

[596] Memiş, **a.g.m.**, s. 169.
[597] Özen / Baştürk, **a.g.e.**, s. 42-45. Dülger, **a.g.m.**, s. 35. Akdeniz / Altıparmak, **a.g.e.**, s. 127.

kurum ve kuruluşları kanunda belirtilir" hükmü yer almaktadır. Bu hüküm gereğince, istisnai olarak kanuni bir düzenleme ile bazı kamu kurum ve kuruluşlarına hakim kararı veya gecikmesinde sakınca bulunan hallerde kanunla yetkili kılınmış merciin yazılı emri olmaksızın haberleşme özgürlüğüne müdahale etme yetkisi tanınabilir[598]. 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun ile TİB'e re'sen erişimi engelleme yetkisi verilmesinin bu çerçeve içerisinde değerlendirilmesi gerekir. Ancak, söz konusu hüküm istisnai bir hüküm olduğu için TİB'e her konuda böyle bir yetki verilmesi mümkün görünmemektedir. TİB'in bu çerçevede sahip olacağı yetki mutlaka konu itibariyle sınırlı bir yetki olmak zorundadır. Nitekim, TİB'e re'sen erişimi engelleme yetkisi konu itibariyle sınırlı olarak sadece, içeriği Kanunda sayılan suçlardan en az birini oluşturduğu düşünülen suçları oluşturan yayınların içerik veya yer sağlayıcısının yurt dışında bulunması halinde veya içerik veya yer sağlayıcısı yurt içinde bulunsa bile, içeriği "*çocukların cinsel istismarı"* veya *"müstehcenlik"* suçlarını oluşturduğu düşünülen yayınlara ilişkin olarak tanınmıştır. Aksi yönde bir düzenleme getirilmiş olsa ve TİB'e her konuya ilişkin olarak veya oldukça geniş bir çerçevede re'sen erişimi engelleme yetkisi tanınmış olsaydı bu düzenlemeler Anayasamızın ilgili hükmüne aykırılık oluştururdu.

Ayrıca, haberleşme özgürlüğünün ancak hakim kararı veya *"gecikmesinde sakınca bulunan hallerde kanunla yetkili kılınmış merciin yazılı emri ile"* sınırlandırılabileceği öngörülmüş olduğundan, gecikmesinde sakınca bulunan hallerde haberleşme özgürlüğüne müdahale edilmesine kanunla, Cumhuriyet savcılığı yetkili kılınabileceği gibi başka kamusal bir mercii de

---

[598] *"... Ceza yargılaması dışında, önleyici olmak ve istihbari bilgi toplamak amacıyla iletişimin dinlenmesi yetkisinin, ancak yasayla tanınması halinde olanaklı olacağı da açıktır. Nitekim, 5397 sayılı Bazı Kanunlarda Değişiklik yapılmasına Dair Kanunla; Polis Vazife ve Selahiyetleri Kanununa, Jandarma Teşkilat Görev ve Yetkileri Kanununa, Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanununa eklenen maddelerle, bu kurumlara bu konuda yasal dayanak sağlanmıştır".* Danıştay 5. Dairesi, 28.12.2009, E. 2009/5240, http://www.danistay.gov.tr/e2009_5240.htm, 10.04.2013. Ayrıca bkz. Tezcan ve Diğerleri, **a.g.e.**, s. 296-297.

yetkili kılınabilir[599]. Ancak bu durumda, yetkili kılınan merciin kararı yirmidört saat içerisinde görevli hakimin onayına sunulmak zorundadır. Bu çerçevede TİB'in, gecikmesinde sakınca bulunan hallerde haberleşme özgürlüğüne, alınan karar yirmidört saat içerisinde hakim onayına sunulmak şartıyla müdahale edebileceği kanun ile düzenlenebilirdi.

İfade özgürlüğü açısından ise erişimin engellenmesi kararının verilmesinde Anayasamızın 26. maddesine göre hakim kararını gerektirecek bir durum bulunmamaktadır. Aynı yaklaşımı, AİHS' nin 10. maddesinde de görmek mümkündür. Basın özgürlüğü ve bilim ve sanat özgürlüğü açısından konuya yaklaşıldığında da aynı sonuca varılmaktadır. Erişimin engelleme kararlarının haberleşme özgürlüğünden ziyade ifade özgürlüğü ile ilgili bir boyutu bulunduğundan haberleşme özgürlüğüne ilişkin sınırlandırmaların erişimi engelleme kararları açısından uygulanması mümkün değildir.

Sonuç olarak bizce erişimi engelleme kararı, idari bir karar ile alınabileceği gibi adli nitelikte bir karar ile de alınabilir. Önemli olan yasa koyucunun takdir yetkisini hangi yönde kullandığı hususudur. Bir diğer deyişle, erişimin engellenmesi kararının ancak adli bir karar ile alınabileceğine yönelik yasa koyucuyu sınırlandıran Anayasal bir kural bulunmamaktadır. Yasa koyucunun takdiri, aşağıda inceleneceği üzere erişimi engelleme kararının hem adli hem de idari bir işlemle alınabilmesi yönünde olmuştur. Bu yaklaşımın, insan haklarına saygılı demokratik hukuk devleti ile çatışır bir yönü bulunmamaktadır.

4. Konusu

5651 sayılı Kanunda erişimin engellenmesi kararının "konusu", *internet ortamında yapılan yayın* olarak belirlenmiş ve bu ibare Kanunun 2. maddesinde, *"İnternet ortamında yer alan ve içeriğine belirsiz sayıda kişilerin ulaşabileceği veri"* olarak; "internet ortamı" ise *haberleşme ile kişisel veya kurumsal bilgisayar sistemleri dışında kalan ve kamuya açık olan internet üzerinde oluşturulan ortam* olarak tanımlanmıştır. Şu halde internet dışındaki

[599] Aksi yönde bir görüş için bkz. Özen / Baştürk, **a.g.e.**, s. 46.

haberleşme araçları ile yapılan "*haberleşmenin"* ve *"kişisel veya kurumsal bilgisayar sistemlerinin",* erişimin engellenmesi kararının konusunu oluşturamayacağını şüphesizdir. Bu çerçevede örneğin cep telefonu ile yapılan haberleşme ve intranet ağları üzerinden yapılan iletişim üzerinde erişimin engellenmesi tedbiri uygulanamaz.

İnternet ortamı tanımlanırken "*haberleşmenin"* kapsam dışında bırakılması internet ortamının kapsamının belirlenmesi açısından bu kavramın önemini artırmaktadır. Burada yer alan "haberleşme" kavramı sadece internet dışında yer alan iletişim araçları ile yapılan kişisel haberleşmeyi mi ifade etmekte yoksa bununla birlikte internet ortamında yapılan kişisel haberleşmeyi de kapsamakta mıdır? Kanunda böyle bir ayrım yapılmaması ve haberleşmenin kişisel bir haberleşme olarak kullanılması hem internet dışında kalan hem de internet ortamında yapılan kişisel haberleşmelerin kapsam dışında bırakılmasını sağlamıştır. Şu halde, örneğin msn üzerinden yapılan bir görüşme veya e-posta ile yapılan haberleşme 5651 sayılı Kanun kapsamında internet ortamını ifade etmeyeceği için bu tür kişisel haberleşme üzerinde erişimin engellenmesi tedbirinin uygulanması hukuken mümkün gözükmemektedir. Ayrıca, internet ortamında yapılan yayın kavramı tanımlanırken söz konusu yayının içeriğine belirsiz sayıda kişinin ulaşabilmesinden söz edilmiştir. Kişisel haberleşme niteliğindeki iletişimin içeriğine ise belirsiz sayıda kişinin ulaşması mümkün değildir. Bununla birlikte, kişisel haberleşmeye imkan tanıyan internet siteleri üzerinde bu sitelerde yer alan ve içeriğine belirsiz sayıda kişinin ulaşabildiği içerik açısından erişimin engellenmesi tedbirinin uygulanması mümkündür.

Aslında internet ortamı ve internet ortamında yapılan yayın kavramının kapsamının belirlenmesi sadece erişimin engellenmesi açısından değil, 5651 sayılı Kanunun kapsam alanının belirlenmesi açısından da önemlidir. Çünkü, Kanunun amaç ve kapsam başlıklı 1. maddesinde Kanunun kapsamı sadece internet ortamına özgülenmiştir.

5. Nedenleri

Dünya genelinde erişimin engellenmesi nedenleri oldukça geniş bir yelpaze oluşturmaktadır. Çocuk pornografisi, çocukların korunması, müstehcenlik, şiddet, ulusal güvenlik, terörizm, uyuşturucu, kumar, nefret söylemi (hate speech), din, ideoloji, siyaset, dolandırıcılık, kimlik hırsızlığı, hakaret, sağlık, fikri mülkiyet hakları gibi nedenler bunlardan bazılarıdır. Ancak, bu nedenler her devlette farklı şekilde uygulama alanı bulmakta; bazı devletler geniş bir şekilde bu nedenleri erişimi engelleme nedeni olarak kabul ederken bazı devletler erişimi engelleme nedenlerinin kapsamını daha dar tutmaktadır.

Nedenler açısından ilk ayrım demokratik kabul edilen ülkeler ile anti-demokratik ülkeler açısından yapılabilir. Birinci gruptaki ülkelerde erişimi engelleme nedenlerinin kapsam alanı daha dardır. Bu ülkelerde, müstehcenlik, çocuk pornografisi, ulusal güvenlik, terörizm, nefret söylemi, şiddet, fikri mülkiyet haklarının korunması ve uyuşturucu gibi nedenler başlıca erişim engelleme nedenleridir[600].

Erişim engelleme nedenleri açısından yapılabilecek bir diğer ayırım, suç oluşturan veya kişilik haklarını ihlal eden içeriğin engellenmesi şeklinde karşımıza çıkmaktadır. Yani, erişimin engellenmesi kararı için illaki içeriğin bir suç oluşturması gerekmemekte; içerik suç oluşturmasa da kişi haklarının ihlal edildiği kimi durumlarda içeriğe erişim yine engellenebilmektedir[601]. Ülkemizde bu ikinci durum kural olarak bir erişimi engelleme nedeni olarak kabul edilmemiştir.

Bazı erişim engelleme nedenleri hemen her ülke tarafından tartışmasız kabul edilmiştir. Örneğin, çocukların cinsel istismarı ile mücadele ve bu çerçevede erişimin engellenmesi dünya ölçeğinde tartışmasız bir konu haline gelmiştir. Her devlet, internetin çocukların cinsel istismarında bir araç olarak kullanılmasını engellemek için gerekli her türlü tedbiri almaktadır.

---

[600] Kılınç, "Türk Hukukunda", s. 433.

[601] AB, hukuka aykırı içerik ve zararlı içerik ayrımı yapmakta ve mücadele yöntemlerini bu ayrıma göre belirlemektedir. Kılınç, "Türk Hukukunda", s. 416-417.

Çoğu devlet çocukların cinsel istismarıyla mücadele konusunda kanuni bir dayanak dahi aramamaktadır[602].

İtalya, fikri mülkiyet haklarının ihlali, çocuk pornografisi ile mücadele ve sanal kumarın önlenmesi amacıyla internet sitelerine erişimi engelleyebilmektedir[603].

ABD'de ulusal güvenliğin sağlanması ve terörizm önemli bir erişimi engelleme nedeni olarak uygulanmaktadır. ABD'nin Google hizmetleri açısından uyguladığı içerik çıkarma taleplerinin nedenlerine yönelik Google Şeffaflık Raporundan (Google Transparency Report) çıkan sonuçların değerlendirilmesi, ABD'deki uygulamanın görülmesi açısından faydalı olacaktır[604]. Google'ın 2011'in ikinci dönemini kapsayan şeffaflık raporuna göre, Google hizmetlerine ilişkin olarak ABD'de 117 tanesi mahkeme kararı, 70 tanesi idari karar ile olmak üzere toplam 6.192 parça içeriğe erişimin engellenmesi talep edilmiştir[605]. Bu talep % 42 oranında Google tarafından olumlu karşılanmıştır. ABD'nin erişim engelleme talepleri web search'te iftira (defamation), özel hayatın korunması, copyright, kapsamı belirtilmeyen diğer nedenler ve kişileştirme (impersonation); Google Earth, Google Maps ve Panoramio'da özel hayatın korunması; Youtube'da iftira, özel hayatın gizliliği, pornografi, şiddet, kapsamı belirtilmeyen diğer nedenler, copyright, marka (trademark) ve ulusal güvenlik; Google AdWords'de hakaret, özel hayatın korunması, kapsamı belirtilmeyen diğer nedenler ve markaya ilişkin gerekçelere dayandırılmıştır[606]. Bu sonuçlar, söz konusu raporun geneline bakıldığında ABD'nin Google'dan 6.192 parça içerik ile en çok içerik çıkarma talep eden ülkelerden birisi olduğunu göstermektedir.

İngiltere, Terörizm Kanununa göre (Terrorism Act 2006) terörizm ile mücadele amacıyla internet sitelerine erişimi engelleyebilmektedir. Çocuk

---

[602] Memiş, **a.g.m.**, s. 164.
[603] https://opennet.net/research/profiles/italy, 14.03.2013.
[604] Diğer ülke sonuçlarını görmek için bkz. http://www.google.com/transparencyreport/map/, 15.10.2012.
[605] Bir karar ile birden fazla içeriğe erişim engelleme talep edilebildiğinden böyle bir sonuç ortaya çıkmaktadır.
[606] Bkz. http://www.google.com/transparencyreport/removals/government/US/?p=2011-12, 15.10.2012.

pornografisi ile mücadele, ırkçılık ve nefret söylemi de erişimi engelleme nedenlerindendir[607]. İngiltere'de Polis Birliği (Association of Police Officers), Google'dan 2011'in ikinci altı aylık döneminde, terörizmi desteklediklerı gerekçesiyle beş tane kullanıcı hesabının sonlandırılmasını talep etmiş; Google bu talebi olumlu karşılayarak bu hesapları iptal etmiştir. Bunun sonucunda 640 tane videoya erişim engellenmiştir[608].

Alman Telehizmetler Kanununa göre, yasal olmayan içeriğin kullanımının engellenmesini öngören genel hukuk kurallarından kaynaklanan zorunluluklar, sağlayıcının böyle bir içerik bilgisini edinmesi durumunda varlığını sürdürmektedir. Bu durumda sağlayıcının engellemeyi gerçekleştirirken Telekomünikasyon Kanununun 85. maddesi çerçevesinde telekomünikasyon mahremiyeti kurallarına uyması, engellemenin teknik olarak mümkün ve makul olması gerekir (md. 5). Almanya'da özellikle küçüklerin korunması, nefret söylemi, soykırım inkarı, aşırı sağ görüşlü içerik ve ırkçılık erişimi engelleme nedenlerindendir[609].

Fransa'da çocuk pornografisi, terörizm ve ırkçılık başlıca erişimi engelleme nedenlerindendir. Bunun yanısıra Fransa'da kamu düzeni veya güvenliği, kamu sağlığı, ulusal savunma ve kişilerin korunması gibi nedenlere dayanılarak da erişimi engelleme kararı verilebilmektedir[610].

Türk hukuk sisteminde internet sitelerine erişimin engellenmesi kararı verilebilecek durumlar çeşitli kanunlar ile düzenleme altına alınmıştır. 5651 sayılı Kanun, 7258 sayılı Futbol ve Diğer Spor Müsabakalarında Bahis ve Şans Oyunları Düzenlenmesi Hakkında Kanun, 633 sayılı Diyanet İşleri Başkanlığı Kuruluş ve Görevleri Hakkında Kanun ve 5846 sayılı Fikir ve Sanat Eserleri Kanununda erişimin engellenmesi müessesesi ve bunun nedenleri açıkça düzenlenmiştir.

---

[607] https://opennet.net/research/profiles/united-kingdom, 14.03.2013.
[608] Bkz. http://www.google.com/transparencyreport/removals/government/GB/?p=2011-12, 15.10.2012. http://www.bbc.co.uk/news/technology-18479137, 15.10.2012.
[609] https://opennet.net/research/profiles/germany, 15.03.2013. Breindl / Wright, **a.g.m.**, s. 3.
[610] http://www.indexoncensorship.org/2011/06/france-on-its-way-to-total-internet-censorship/, 15.03.2013. Breindl / Wright, **a.g.m.**, s. 3.

5651 sayılı Kanuna göre, internet ortamında yapılan ve içeriği aşağıdaki suçları oluşturduğu hususunda yeterli şüphe sebebi bulunan yayınlarla ilgili olarak erişimin engellenmesine karar verilmektedir (md. 8):

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

1) İntihara yönlendirme (madde 84),

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

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

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

5) Müstehcenlik (madde 226),

6) Fuhuş (madde 227),

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

suçları.

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

Erişimin engellenmesi kararı verilebilmesi için internet ortamında yapılan ve içeriği yukarıdaki suçlardan en az birini oluşturduğu hususunda yeterli şüphe sebebi bulunan bir yayının söz konusu olması gerekir. Hakkında yeterli şüphe bulunan, fakat yukarıda sayılmayan bir suçtan dolayı bu Kanun hükmüne göre erişimin engellenmesi kararı verilmesi mümkün değildir[611]. Ayrıca, yukarıda sayılan bir suçtan dolayı olsa bile suç içerdiği konusunda hakkında "*yeterli şüphe sebebi*"[612] bulunmayan bir yayından dolayı yine erişimin engellenmesi kararının verilemez. Avrupa İnsan Hakları Sözleşmesinin 10. maddesi ve Anayasamızın 26. maddesinde *"suçların önlenmesi"* ifade özgürlüğü üzerinde bir sınırlandırma nedeni olarak öngörülmüştür. 5651 sayılı Kanunun söz konusu hükmü de bu çerçevede suçun önlenmesini esas almıştır[613].

7258 sayılı Futbol ve Diğer Spor Müsabakalarında Bahis ve Şans Oyunları Düzenlenmesi Hakkında Kanunda bahis ve şans oyunlarının

---

[611] Dülger / Beceni, **a.g.e.**, s. 44.

[612] "*Yeterli şüphe sebebi"* kavramının "*kuvvetli şüphe"* olarak değiştirilmesi gerektiği hakkında bkz. Bozbel, **a.g.m.**, s. 2.

[613] Dülger / Beceni, **a.g.e.**, s. 14.

internet ortamında oynatılmasına yönelik olarak bazı suç ve cezalar öngörülmüş; söz konusu suçlarla ilgili olarak 5651 sayılı Kanunun erişimin engellenmesine ilişkin hükümlerinin uygulanacağını düzenlenmiştir (md. 5)[614].

633 sayılı Diyanet İşleri Başkanlığı ve Görevleri Hakkında Kanunda Mushafları İnceleme ve Kıraat Kuruluna, hatalı ve noksan olarak basılan veya yayımlanan mushaf ve cüzler ile sesli veya görüntülü Kur'an-ı Kerim yayınlarını tespit etmek görevi verildikten sonra, hatalı ve noksan olarak basıldığı veya yayımlandığı Kurul tarafından tespit edilen mushaf ve cüzler ile sesli ve görüntülü Kur'an-ı Kerim yayınlarının, Başkanlığın müracaatı üzerine, yayımın yapıldığı yer sulh hukuk mahkemesi kararı ile toplatılacağı ve imha edileceği öngörülmüştür (md. 6). Bu yayınların internet ortamında yapılması halinde ise, Başkanlığın müracaatı üzerine, sulh hukuk mahkemesinin bu yayınla ilgili olarak erişimin engellenmesi kararı vereceği düzenlenmiştir. Bu kararın bir örneği gereği yapılmak üzere Telekomünikasyon İletişim Başkanlığına gönderilecektir. Sulh hukuk mahkemesinin bu çerçevede verdiği kararlara ve Başkanlığın talebinin reddine dair kararlarına karşı tefhim veya tebliğden itibaren iki hafta içinde asliye hukuk mahkemesinde itiraz yoluna gidilebilir. 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.

633 sayılı Kanunda erişimin engellenmesi müessesesi açısından 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanuna göre ayrı esas ve usuller belirlenmiştir. Şöyle ki esas açısından, 633 sayılı Kanuna göre "*internet ortamında hatalı ve noksan olarak mushaf ve cüzler ile sesli veya görüntülü Kur'an-ı Kerim yayınlama"* fiili suç teşkil eden bir fiil olmamasına rağmen bir erişim engelleme nedenidir. Ayrıca, bu Kanun kapsamında erişim engelleme kararı bir koruma tedbirinden farklı olarak doğrudan nihai bir karar

[614] http://www.mevzuat.gov.tr/Kanunlar.aspx, 16.10.2012.

olarak verilecektir. 5651 sayılı Kanunun düzenleme yaklaşımı açısından ise erişimi engelleme nedenleri suç teşkil eden fiillerdir ve erişimi engelleme kararı bir koruma tedbiri veya idari tedbir olarak verilebilir. Usul açısından ise 633 sayılı Kanuna göre erişimin engellenmesi açısından görevli olan mahkeme, "*sulh hukuk mahkemesi"* olarak belirlenmiştir. Sulh hukuk mahkemesi kararlarına karşı asliye hukuk mahkemesine itiraz edilebilecek ve asliye hukuk mahkemesinin kararları kesin nitelik taşıyacaktır. 633 sayılı Kanunun erişimin engellenmesi açısından öngördüğü usul, 5651 sayılı Kanuna göre farklı olduğu için 633 sayılı Kanun çerçevesinde verilecek erişimin engellenmesi kararlarında, 5651 sayılı Kanunda yer alan usul uygulanmayacaktır.

Erişimin engellenmesi müessesesinin düzenlendiği bir diğer kanun, 5846 sayılı Fikir ve Sanat Eserleri Kanunudur. 5846 sayılı Fikir ve Sanat Eserleri Kanununun Ek 4. maddesinin üçüncü fıkrasında şu hüküm yer almaktadır: *"Dijital iletim de dahil olmak üzere işaret, ses ve/veya görüntü nakline yarayan araçlarla servis ve bilgi içerik sağlayıcılar tarafından eser sahipleri ile bağlantılı hak sahiplerinin bu Kanunda tanınmış haklarının ihlâli halinde, hak sahiplerinin başvuruları üzerine ihlâle konu eserler içerikten çıkarılır. Bunun için hakları haleldar olan gerçek veya tüzel kişi öncelikle bilgi içerik sağlayıcısına başvurarak üç gün içinde ihlâlin durdurulmasını ister. İhlâlin devamı halinde bu defa, Cumhuriyet savcısına yapılan başvuru üzerine, üç gün içinde servis sağlayıcıdan ihlâle devam eden bilgi içerik sağlayıcısına verilen hizmetin durdurulması istenir. İhlâlin durdurulması halinde bilgi içerik sağlayıcısına yeniden servis sağlanır. Servis sağlayıcılar, bilgi içerik sağlayıcılarının isimlerini gösterir listeyi her ayın ilk iş günü Bakanlığa bildirir. Servis sağlayıcılar ile bilgi içerik sağlayıcıları, Bakanlıkça istendiği takdirde her türlü bilgi ve belgeyi vermekle yükümlüdür. Bu maddede belirtilen hususların uygulanmasına ilişkin usul ve esaslar Bakanlık tarafından çıkarılacak bir yönetmelikle belirlenir".* 5846 sayılı Kanunun erişim engellemesi açısından öngördüğü usul de 5651 sayılı Kanunun öngördüğü usulden farklıdır. Bu madde hükmüne göre verilen erişimin engellenmesi kararı, koruma tedbiri niteliğinde bir karar değildir. Ayrıca, bu karara karşı bir

kanun yolu da öngörülmemiştir. Bizce, bu karar Cumhuriyet savcısı tarafından verilen idari bir karardır[615]. Cumhuriyet savcısı tarafından erişimin engellenmesi kararı verilirken adli bir yargılama usulü öngörülmemiş, Cumhuriyet savcısının idari bir mercinin aldığı bir karardan farksız olarak bir karar vermesi öngörülmüştür.

Doktrinde, erişimin engellenmesi nedenlerinin sadece 5651 sayılı Kanunda yer alan nedenlerle sınırlı olduğu ileri sürülmüştür. Bu görüşe göre, 5651 sayılı Kanun özel bir kanundur ve erişimin engellenmesi nedenleri bu kanunda tahdidi olarak *(katalog suçlar)* sayılmıştır[616]. Bu nedenle, diğer kanunlarda öngörülen nedenlere dayanılarak erişimin engellenmesi kararı verilemez. 5651 sayılı Kanun erişimi engelleme nedenlerini tahdidi olarak düzenlediğinden, bu görüşe katılmak mümkün gözükmemektedir. Kanuna göre Başkanlığa, bu Kanunda sayılan nedenlerle erişimi engelleme yetkisi yanında diğer kanunlarda da benzer yetkiler verilmesi mümkündür (md. 10/4)[617]. Bu hüküm göz önüne alındığında erişimin engellenmesi açısından 5651 sayılı Kanun ile başka nedenler öngören kanunlar arasında bir çatışmanın olduğu söylenemez. Aksine, erişimin engellenmesi nedenleri açısından diğer kanunlarda yer alan düzenlemeler 5651 sayılı Kanunu tamamlayıcı nitelik taşımaktadır.

Hukuk sistemimizde erişimin engellenmesi kararı verilebilecek yukarıdaki açık düzenlemeler dışında ihtiyati tedbire veya kişiliğin korunmasına yönelik düzenlemeler içeren kanunlara dayanılarak erişimin engellenmesi kararı verilip verilemeyeceği tartışılmaktadır. Örneğin, 6100 sayılı Hukuk Muhakemeleri Kanununun 389 vd. maddelerinde ihtiyati tedbir düzenlenmiştir. Mevcut durumda meydana gelebilecek bir değişme nedeniyle hakkın elde edilmesinin önemli ölçüde zorlaşacağından ya da tamamen imkansız hale geleceğinden veya gecikme sebebiyle bir sakıncanın yahut ciddi bir zararın doğacağından endişe edilmesi hallerinde, uyuşmazlık konusu hakkında ihtiyati tedbir kararı verilebilmektedir. Mahkeme, tedbire

---

[615] Dülger / Beceni, **a.g.e.**, s. 60.
[616] Bozbel, **a.g.m.**, s. 2.
[617] Özen / Baştürk, **a.g.e.**, s. 36.

konu olan mal veya hakkın muhafaza altına alınması veya bir yediemine tevdii ya da bir şeyin yapılması veya yapılmaması gibi, sakıncayı ortadan kaldıracak veya zararı engelleyecek her türlü tedbire karar verebilmektedir[618]. Yine, Türk Medeni Kanununun 24. ve 25. maddelerinde hukuka aykırı olarak kişilik hakkına saldırılan kimsenin hakimden, saldırıda bulunanlara karşı korunmasını ve bu çerçevede saldırı tehlikesinin önlenmesini, sürmekte olan saldırıya son verilmesini, sona ermiş olsa bile etkileri devam eden saldırının hukuka aykırılığının tespitini isteyebileceği; bunlarla birlikte düzeltmenin veya kararın üçüncü kişilere bildirilmesi ya da yayımlanması isteminde de bulunabileceği düzenlenmiştir. Doktrinde, söz konusu kanun hükümlerine dayanılarak erişimin engellenmesi kararı verilemeyeceği ifade edilmektedir[619]. Kişilik haklarının ihlali halinde uygulanması gereken hükümler 5651 sayılı Kanunun 9. maddesinde özel olarak düzenlenmiştir. 9. maddeye göre içerik nedeniyle hakkının ihlal edildiğini iddia eden kişi, içerik sağlayıcısına, buna ulaşamaması halinde yer sağlayıcısına başvurarak kendisine ilişkin içeriğin yayından çıkarılmasını ve yayındaki kapsamından fazla olmamak üzere hazırladığı cevabın bir hafta süreyle internet ortamında yayımlanmasını isteyebilir. Talebin iki gün içerisinde yerine getirilmemesi durumunda bu talep reddedilmiş sayılır. Talebin reddedilmiş sayılması halinde, kişi onbeş gün içinde yerleşim yeri sulh ceza mahkemesine başvurarak, içeriğin yayından çıkarılmasına ve yayındaki kapsamından fazla olmamak üzere hazırladığı cevabın bir hafta süreyle internet ortamında yayımlanmasına karar verilmesini isteyebilir[620]. Sulh ceza hakimi bu talebi üç gün içinde duruşma yapmaksızın karara bağlar. Sulh ceza hakiminin kararına karşı CMK hükümlerine göre itiraz yoluna gidilebilir. Sulh ceza hakiminin kesinleşen kararının, hakkı ihlal edilen kişi tarafından yapılan başvuruyu

---

[618] Baki Kuru, Ramazan Arslan, Ejder Yılmaz, **Medeni Usul Hukuku**, Yetkin Yayınları, 22. Baskı, Ankara, 2011, s. 582-583.

[619] Kılınç, "Türk Hukukunda", s. 410. Akdeniz / Altıparmak, **a.g.e.**, s. 43.

[620] Kişilik hakları ihlal edilen kişi sadece içeriğin yayından çıkarılmasına veya yayındaki kapsamından fazla olmamak üzere hazırladığı cevabın bir hafta süreyle internet ortamında yayımlanmasına karar verilmesini isteyebilir. Anılan kanun metninde her ne kadar "ve" bağlacı kullanılmışsa da bu kavramı "veya" olarak ele almak, Kanun ile öngörülmek istenen amaca daha uygundur. Kişilik hakkı ihlal edilen kişi içerik yayından çıkarıldıktan sonra ayrıca, bir cevap yazılmasını kişilik hakları açısından sakıncalı görebilir ve bunu istemeyebilir. İçel / Ünver, **a.g.e.**, s. 4.

yerine getirmeyen içerik veya yer sağlayıcısına tebliğinden itibaren iki gün içinde içerik yayından çıkarılarak hazırlanan cevabın yayımlanmasına başlanır. Sulh ceza hakiminin kararını bu çerçevede yerine getirmeyen sorumlu kişi, altı aydan iki yıla kadar hapis cezası ile cezalandırılır. İçerik veya yer sağlayıcının tüzel kişi olması halinde, ceza yayın sorumlusu hakkında uygulanır[621]. Görüldüğü üzere, 9. madde ile kişilik hakkı ihlallerinden dolayı erişimin engellenmesi yaptırımı öngörülmemiş; aksine, içeriğin yayından çıkarılması ve yayındaki kapsamından fazla olmamak üzere hazırlanan cevabın bir hafta süreyle internet ortamında yayınlanması ve sulh ceza hakiminin kararını yerine getirmeyen sorumlu hakkında cezai sorumluluğa ilişkin bir düzenleme getirilmiştir[622].

Gerçekten de internette kişilik haklarının ihlali nedeniyle başvurulacak hukuksal hükümler 9. madde ile özel olarak düzenlenmiştir. Bu durum karşısında kişilik haklarının korunmasına yönelik olarak diğer kanunlarda yer alan hükümlerin erişimin engellenmesi açısından uygulanması mümkün gözükmemektedir[623]. Ancak, mahkeme kararının yerine getirilmemesi durumunda cezai bir yaptırım öngörülmekle birlikte, ihlal içeren internet sitesine erişim hakkında herhangi bir karar verilip verilemeyeceği maddede düzenlenmemiştir. Bizce, mahkeme kararının yerine getirilmemesi durumunda erişimin engellenmesine ilişkin olarak bu Kanunda bir hüküm bulunmaması, kişilik haklarını koruyan diğer kanun hükümlerinin uygulanma kabiliyeti kazanmasını sağlamaktadır. Bu çerçevede hukuk mahkemeleri, Medeni Kanun veya Hukuk Muhakemeleri Kanunu kapsamında erişimin engellenmesi kararı verebilir; ancak bunun için öncelikle 5651 sayılı Kanunda yer alan içeriğin yayından çıkarılması ve cevap hakkı müessesesinin işletilmesi gerekir. Bu imkan kullanıldıktan sonra, eğer hukuka aykırı içerik

---

[621] Bu suçun, erişimin engellenmesi kararının yer ve erişim sağlayıcılarca yerine getirilmemesi durumunda işlenmiş olacak suçlar gibi 5651 sayılı Kanunun internete özgü öngördüğü bir suç olarak değerlendirilmesi gerekir.

[622] Bununla birlikte tazminat sorumluluğuna ilişkin hükümler saklıdır. Örneğin Danıştay, Serbest Muhasebeci Mali Müşavir olan davacının, davalı Odaya ait olan internet sitesinin forum sayfasına aleyhine yazılı olan ve kaldırılması istemiyle başvurmasına rağmen kaldırılmayan hakaret ve küfürler nedeniyle manevi tazminata hükmedilmesi gerektiğine karar vermiştir. Danıştay 8. Dairesi, 01.06.2011, E. 2008/6707, K. 2011/2949, http://www.danistay.gov.tr/128sayi.pdf, 24.12.2012.

[623] Akdeniz / Altıparmak, **a.g.e.**, s. 44.

çıkarılmazsa, Medeni Kanunun 25. maddesi veya HMK'nın 389 vd. maddeleri çerçevesinde erişimin engellenmesi için hukuk mahkemelerine başvurulabilmelidir. Sulh ceza mahkemesinin kararına rağmen içeriğin internet sitesinden çıkarılmaması durumunda artık 5651 sayılı Kanunun 9. maddesi ile Medeni Kanunun 25. maddesi veya HMK'nın 389 vd. maddeleri birbiri ile çatışmamakta; tam aksine birbirini tamamlamaktadır.

İnternet ortamında kişilik haklarının korunması açısından 9. madde ile öngörülen düzenleme eksik ve yetersiz bir düzenleme olmuştur. Madde ile getirilen cezai yaptırıma rağmen kişilik haklarını ihlal eden yayına devam edilmesi oldukça muhtemeldir. Hele bir de içerik ve yer sağlayıcının yurt dışında bulunduğu durumları düşündüğümüzde, cezai yaptırım da etkisini kaybetmektedir[624]. Kanunun bu yaklaşımı ile, özellikle içerik ve yer sağlayıcının yurt dışında olduğu yayınlarda vatandaşlarımızın kişilik hakları korunmasız bırakılmıştır. 9. maddenin yukarıda yapılan yorum çerçevesinde değerlendirilmesi, bu olumsuzluğu giderecektir.

Nihayet, internet bankacılığında dolandırıcılık (phishing), kimlik hırsızlığı, organ ticareti, şiddet, nefret söylemi, terörizm, bomba yapım bilgisi verme gibi suçları içeren internet sitelerine erişimin yargısal koruma tedbiri kapsamında engellenememesi eksik bir düzenleme olmuştur[625]. 5651 sayılı Kanunun kanunlaşma sürecinde Türkiye Büyük Millet Meclisinde, 8. maddede yer alan suçlara TCK'da yer alan Devletin birliği ve ülke bütünlüğü aleyhine olan suçlar ile Anayasamızın 174. maddesinde düzenlenen İnkılap Kanunlarının korunması amacıyla düzenlenen suçların da eklenmesi önerilmiş, ancak bu öneri reddedilmiştir[626]. Ülkemiz yetkili makamları PKK'nın yayın organı olan Roj TV'nin kapatılması için Danimarka makamlarına başvuruda bulunmuştur; ancak PKK'nın Roj TV'den daha etkin bir şekilde propagandasını yapan internet sitelerinin yayınını kendi topraklarında engelleyememiştir. Bu nedenle, erişimin engellenmesi nedenleri arasına bir yargısal koruma tedbiri olarak terör suçları konulmalı, ayrıca TİB'e idari bir

---

[624] Dülger, **a.g.m.**, s. 46.
[625] Dülger, **a.g.m.**, s. 36.
[626] Görüşmelerde Google Earth'ün Diyarbakır'ı sözde Kürdistanın başkenti olarak göstermesi de eleştiri konusu olmuştur. Mehmet Bedii Kaya, **a.g.e.**, s. 84. Akdeniz / Altıparmak, **a.g.e.**, s. 24.

tedbir olarak terörle mücadele çerçevesinde internet sitelerini kapatma yetkisi verilmelidir.

Google'ın 2011'in ikinci dönemini kapsayan şeffaflık raporuna göre, Google hizmetlerine ilişkin olarak ülkemizde 22 tanesi mahkeme kararı, 23 tanesi idari karar ile olmak üzere toplam 174 parça içeriğe erişimin engellenmesi talep edilmiştir. Bu talep % 56 oranında Google tarafından olumlu karşılanmıştır. Türkiye' nin erişim engelleme talepleri web search'te iftira (defamation) ve kapsamı belirtilmeyen diğer nedenler; Google Videos'da pornografi ve kapsamı belirtilmeyen diğer nedenler; Google Earth, Google Maps ve Panoramio'da hükümet eleştirisi (government criticism)[627]; Google Groups'da pornografi; Youtube'da iftira, özel hayatın gizliliği, nefret söylemi, kapsamı belirtilmeyen diğer nedenler ve hükümet eleştirisi; Blogger'da iftira, pornografi ve kapsamı belirtilmeyen diğer nedenler; Picasa Web Albums'de pornografi; Gmail'de ise kişileştirme (impersonation) gerekçelerine dayandırılmıştır[628].

6. Usul

Erişimin engellenmesi kararının nasıl bir usul dahilinde alınabileceği 5651 sayılı Kanunda ayrıntılı bir şekilde düzenlenmiştir (md. 8). Kanun, *"koruma tedbiri"* ve *"idari tedbir"* olarak iki farklı usul öngörmüştür. Birinci usulde erişimin engellenmesi kararının yargı mercileri tarafından alınması öngörülmüşken, ikinci usulde bu kararın doğrudan idari merciler tarafından alınabilmesine imkan tanınmıştır.

a. Adli Mercilerinin Kararı ile Erişimin Engellenmesi

Kural olarak erişimin engellenmesi kararı soruşturma evresinde hakim, kovuşturma evresinde ise mahkeme tarafından verilir. Soruşturma evresinde,

---

[627] Google'ın, ulusal güvenlik (national security) ile hükümet eleştirisi (government criticism) kategorisi arasındaki fark, söz konusu rapordan anlaşılamamaktadır. Aynı yöndeki taleplerin bazı ülkeler açısından ulusal güvenlik, bazı ülkeler açısından ise hükümet eleştirisi kategorisi altında değerlendirilme olasılığına karşı taleplerin içeriklerinin ve hangilerine olumlu veya olumsuz yanıt verildiği hususunun da şeffaflık ilkesi gereği açıklanması gerekir.

[628] Bkz. http://www.google.com/transparencyreport/removals/government/TR/?p=2011-12, 15.10.2012.

gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısı tarafından da erişimin engellenmesine karar verilebilir. Bu durumda Cumhuriyet savcısı kararını yirmi dört saat içinde hakimin onayına sunar ve hakim, kararını en geç yirmi dört saat içinde verir. Bu süre içinde kararın onaylanmaması halinde tedbir, Cumhuriyet savcısı tarafından derhal kaldırılır. Koruma tedbiri olarak verilen erişimin engellenmesine ilişkin karara, 5271 sayılı CMK hükümlerine göre itiraz edilebilir.

Hakim, mahkeme veya Cumhuriyet savcısı tarafından verilen erişimin engellenmesi kararının birer örneği, gereği yapılmak üzere TİB'e gönderilir (md. 8/3). Hakim, mahkeme veya Cumhuriyet savcısının, aldığı kararı doğrudan erişim sağlayıcısına gönderme yetkisi yoktur[629]. TİB tarafından erişim sağlayıcısına bildirilen hakim, mahkeme veya Cumhuriyet savcısının erişimi engelleme kararının gereği, derhal ve en geç kararın bildirilmesi anından itibaren yirmidört saat içinde yerine getirilir (md. 8/5). İşlemlerin yürütülmesi için Başkanlığa gönderilen hakim ve mahkeme kararlarına 5271 sayılı CMK hükümlerine göre TİB tarafından da itiraz edilebilir (md. 8/13)[630].

5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunda adli mercilerin kararı ile erişimin engellenmesi bir "*koruma tedbiri"* olarak düzenlenmiştir. Doktrinde koruma tedbiri, ceza muhakemesinin gecikmeksizin yürütülmesi, maddi delillerin gereği gibi tespit edilmesi ve değerlendirilmesi ve verilen kararların etkinliğini kaybetmemesi için uygulanan tedbirler olarak tanımlanmaktadır[631]. 5651 sayılı Kanunda düzenlenen koruma tedbiri, diğer koruma tedbirlerinden farklılık göstermektedir. Şöyle ki erişimin engellenmesine yönelik koruma tedbirinin ceza muhakemesinin gecikmeksizin yürütülmesi, maddi delillerin gereği gibi değerlendirilmesi veya verilen kararların etkinliğini kaybetmemesi ile bir ilgisi

---

[629] Ayrıca bkz. İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik, md. 16.

[630] Söz konusu hüküm 5651 sayılı Kanunun 8. maddesine, 2008 yılında yürürlüğe konulan 5809 sayılı Elektronik Haberleşme Kanunu ile eklenmiştir. Bizce, temel hak ve özgürlüklerin korunması açısından bu düzenleme yerinde bir yaklaşım olmuştur. Aynı yönde: Bozbel, **a.g.m.**, s. 2.

[631] Nevzat Toroslu, Metin Feyzioğlu, **Ceza Muhakemesi Hukuku**, Savaş Yayınları, Ankara, 2009, s. 214.

bulunmamaktadır. Bu açıdan 5651 sayılı Kanuna göre verilen koruma tedbiri, kendine özgü bir koruma tedbiri olarak nitelendirilebilir[632].

İstisnailik, araç olma, ölçülülük (elverişlilik, gereklilik ve orantılılık), kanunilik, önleyicilik (cezai olmama), suç şüphesinin bulunması ve geçicilik koruma tedbirlerinin özellik ve şartları olarak ifade edilmektedir[633]. Koruma tedbiri olarak verilen erişimin engellenmesi kararlarında da bu şartların yerine getirilmesi gerekir. Aksi halde, erişimin engellenmesine yönelik verilen koruma tedbiri hukuka aykırı nitelik taşıyacaktır.

İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmeliğin 15. maddesine göre koruma tedbiri olarak verilen erişimin engellenmesi kararlarında şu hususlar bulunmalıdır:

1. Kararı veren merciin adı.

2. Karar tarihi ile soruşturma numarası veya kovuşturmaya geçilmişse mahkeme esas numarası.

3. Tedbirin hangi suç için istendiği, bu suça ilişkin yeterli şüphe sebeplerinin neler olduğu.

4. "URL adresi: http://www.abcd.com/abcdefgh.htm" şeklinde örneklenen, suça ilişkin bilgilerin bulunduğu tam web adresi.

5. "www.abcd.com" şeklinde örneklenen, hakkında tedbir uygulanacak internet yayınlarının alan adı.

6. Hakkında tedbir uygulanacak internet yayınlarının bulunduğu yer sağlayıcıya ait IP adresi.

7. Alan adı veya IP adresi olarak erişim engelleme yöntemi.

b. İdari Mercilerin Kararı ile Erişimin Engellenmesi

İdari mercilerin kararı ile erişimin engellenmesine ilişkin uygulamaya birçok Avrupa ülkesinde rastlanmaktadır. Örneğin, İngiltere'de İnternet İzleme Kuruluşu (Internet Watch Foundation), İnternet Yardım Hattına suç unsuru taşıyan online içeriğin bildirilmesi amacıyla 1996 yılında internet sektörü

---

[632] Dülger / Beceni, **a.g.e.**, s. 38. 5651 sayılı Kanunun öngördüğü erişimin engellenmesi müessesesinin, hem koruma tedbiri hem idari tedbir açısından bir bütün olarak sui generis bir özellik gösterdiği görüşü için bkz. Akdeniz / Altıparmak, **a.g.e.**, s. 31.

[633] Toroslu / Feyzioğlu, **a.g.e.**, s. 215.

tarafından kurulmuştur. İnternet İzleme Kuruluşu, sektör, kamu kuruluşları, idari uygulayıcılar ve uluslararası kuruluşlar ile birlikte çalışmaktadır. Kuruluş,

1. Dünyanın herhangi bir yerinde barındırılan çocukların cinsel istismarına ilişkin içerik,

2. İngiltere'de barındırılan suç oluşturan müstehcen yetişkin içerik,

3. İngiltere'de barındırılan çocukların cinsel istismarına ilişkin fotografik olmayan görüntü içeren içerikle mücadele etmektedir[634]. Kuruluş ayrıca, Kamu Düzeni Kanununa göre (Public Order Act 1986) ırkçılık ve nefret söylemi içeren internet sitelerine de erişiminin engellenmesi konusunda girişimde bulunma yetkisini haizdir[635]. Kuruluşun aldığı kararlar, yargısal bir merciin kararını gerektirmeksizin uygulanmaktadır[636].

İngiltere'de, Terörizm Kanununun (Terrorism Act 2006) 3. maddesine göre bir internet sitesinin terörizm ile bağlantılı olduğuna dair bilgilendirme üzerine internet servis sağlayıcılar söz konusu internet sitesine erişimin engellenmesi konusunda gerekli tedbirleri almamaları durumunda söz konusu içerikten sorumludur[637].

Almanya'da örneğin, Küçükleri Medyada Yer Alan Zararlı İçeriğe Karşı Koruma Birimi (Federal Department for Media Harmful to Young Persons (BPjM)), küçüklerin zararlı içeriğe karşı korunmasına yönelik olarak müstehcen, şiddet veya suç barındıran, anti-semitik veya ırkçılık içeren içeriğe erişimi doğrudan engelleyebilmektedir. Kurumun bu kararına karşı ilgililerin dava açma hakkı vardır[638]. Almanya'da idare tarafından eyalet düzeyinde erişimi engelleme kararları da verilebilmektedir[639].

Fransa'da kamu düzeni veya güvenliği, küçüklerin korunması, kamu sağlığı, ulusal savunma ve kişilerin korunması amacıyla idare, araya bir yargı kararı girmeksizin doğrudan erişimi engelleme kararı verebilmektedir[640].

---

634 http://www.iwf.org.uk/about-iwf/remit-vision-and-mission, 30.01.2013.
635 https://opennet.net/research/profiles/united-kingdom, 14.03.2013.
636 https://opennet.net/research/profiles/united-kingdom, 14. 03.2013. McIntyre / Scott, **a.g.m.**, s. 12.
637 Bkz. http://www.legislation.gov.uk/ukpga/2006/11/section/3, 14.03.2013.
638 http://bundespruefstelle.de/bpjm/information-in-english.html, 15.03.2013.
639 https://opennet.net/research/profiles/germany, 14.03.2013.
640 http://www.indexoncensorship.org/2011/06/france-on-its-way-to-total-internet-censorship/, 15.03.2013. Breindl / Wright, **a.g.m.**, s. 4.

Digital Ekonomide Güven Kanununun (Loi pour la Confiance dans l'Economie Numerique-LCEN) 18. maddesi buna imkan tanımaktadır.

Avusturalya'da, yasaklı içerik bu ülkede barındırılır veya bu ülkeden sağlanırsa Avusturalya İletişim ve Medya Kurumu (The Australian Communications and Media Authority), içerik sağlayıcı veya servis sağlayıcıdan içeriğin çıkarılması veya içeriğe erişimin engellenmesini isteyebilir. Yasaklı içerik Avusturalya'da barındırılmaz veya Avusturalya'dan sağlanmazsa bu içerik filtrelemeyi yapacak kuruluşlara bildirilir. Avusturalya'da online içerik, Sınıflandırma Kurulu (Classification Board) tarafından sınıflandırılmaktadır. Sınıflandırma kategorisine göre cinsel içerik, çocuk pornografisi, suç unsuru taşıyan, şiddet içeren, uyuşturucu kullanımı ve terör faaliyeti içeren içerik gibi hususlar göz önünde bulundurularak sınıflandırılma yapılmaktadır. ACMA, Sınıflandırma Kurulundan bir içeriğin sınıflandırılmasını isteyebilir[641]. ACMA yetkilerini Yayın Hizmetleri Kanunundan (Broadcasting Services Act 1992) almaktadır[642].

e-Ticaret Direktifine göre, yer ve erişim sağlayıcıların sorumluluğu açısından getirilen güvence niteliğindeki hükümler, üye devletlerin, hukuk sistemlerine göre bir mahkeme veya idari otoritenin servis sağlayıcıdan ihlali sona erdirmesi veya önlemesini talep etme imkanını ortadan kaldırmamaktadır (md. 12/3, 13/2, 14/3). Bu çerçevede e-Ticaret Direktifinde yargı mercileri yanında idari mercilerin de hizmet sağlayıcılarından ihlali sona erdirmesini veya engellemesini talep edebileceği mümkün kılınmıştır.

Türkiye'de ise içeriği Kanunda sayılan suçlardan en az birini oluşturduğu hususunda yeterli şüphe sebebi bulunan yayınların içerik veya[643] yer sağlayıcısının yurt dışında bulunması halinde ya da içerik veya yer sağlayıcısı yurt içinde bulunsa bile, içeriği "*çocukların cinsel istismarı"* veya *"müstehcenlik"* suçlarını oluşturduğu hususunda yeterli şüphe sebebi bulunan yayınlara ilişkin olarak erişimin engellenmesi kararı re'sen TİB tarafından

---

[641] http://www.acma.gov.au/WEB/STANDARD/pc=INT_IND_CONTENT_ABOUT, 30.01.2013.
[642] http://www.comlaw.gov.au/Series/C2004A04401, 30.01.2013.
[643] Buradaki "veya" bağlacından dolayı, içerik veya yer sağlayıcıdan sadece birinin yurt dışında bulunması halinde de TİB tarafından re'sen erişimi engelleme kararı verilebilecektir. "Veya" bağlacının "ve" bağlacı ile değiştirilmesi gerektiği ileri sürülmektedir. Bozbel, **a.g.m.**, s. 3.

verilir. Bu karar, erişim sağlayıcısına bildirilerek gereğinin yerine getirilmesi istenir. TİB tarafından verilen erişimin engellenmesi kararının konusunu oluşturan yayını yapanların kimliklerinin belirlenmesi halinde[644] Başkanlık tarafından Cumhuriyet Başsavcılığına suç duyurusunda bulunulur. TİB tarafından verilen kararlara karşı "*zorunlu bir idari başvuru yolu*"[645] öngörülmemiştir. Bu kararlar idari davaya konu olabilecek kararlardır[646].

TİB'in re'sen erişimi engelleme kararı verebileceği nedenlerden birisi de 7258 sayılı Futbol ve Diğer Spor Müsabakalarında Bahis ve Şans Oyunları Düzenlenmesi Hakkında Kanunda yer almıştır. Bu Kanunda, bahis ve şans oyunlarının internet ortamında oynatılmasına yönelik öngörülen suçlar ile ilgili olarak 5651 sayılı Kanunun erişimin engellenmesine ilişkin hükümlerinin uygulanacağı düzenlenmiştir (md. 5) 5651 sayılı Kanunda erişimin engellemesi, koruma tedbiri ve idari tedbir olarak iki farklı şekilde öngörüldüğünden, 7258 sayılı Kanuna göre bu iki tedbir kapsamında da erişimin engellenmesi kararının verilmesi mümkün gözükmektedir. Şu durumda, TİB'in 7258 sayılı Kanunun 5. maddesinde yer alan suçlardan dolayı re'sen erişimi engelleme yetkisi bulunmaktadır. Ancak TİB, bu yetkisini 5651 sayılı Kanunun 8. maddesinin dördüncü fıkrası kapsamında kullanabileceği için bu hüküm sadece içerik veya yer sağlayıcının yurt dışında bulunması halinde uygulayabilir. Dördüncü fıkraya göre içerik veya yer sağlayıcının yurt içinde bulunması durumunda re'sen erişimin engellenmesi kararının verilebileceği haller sadece 8. maddenin birinci fıkrasının (a) bendinin (2) ve (5) numaralı alt bentlerinde yazılı suçları oluşturan yayınlar açısından öngörülmüştür.

---

[644] Doktrinde, Başkanlık tarafından verilen erişimin engellenmesi kararının konusunu oluşturan yayını yapanların kimliklerinin belirlenmesi halinde Cumhuriyet Başsavcılığına suç duyurusunda bulunulabileceğine ilişkin bu hüküm, kamu görevlileri tarafından öğrenilen her suçun, faili bilinse de bilinmese de Cumhuriyet Başsavcılığına bildirilmesi gerektiği düşüncesiyle eleştirilmektedir. Mehmet Bedii Kaya, **a.g.e.**, s. 122. Dülger, **a.g.m.**, s. 44. Akdeniz / Altıparmak, **a.g.e.**, s. 41-42.

[645] Zorunlu idari başvuru yolu, idari bir işlem hakkında dava açılmadan önce idareye başvuru yapılması zorunluluğunun kanun ile öngörülmesi halinde söz konusu olur. Bu durumda idareye başvurmadan doğrudan dava açmak, idari merci tecavüzü doğurur ve dava dilekçesi İYUK' un 15. maddesine göre, görevli idari mercie tevdi edilir. Gözübüyük, **a.g.e.**, s. 478-479.

[646] Mehmet Bedii Kaya, **a.g.e.**, s. 125. Bozbel, **a.g.m.**, s. 3.

İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelikte, çocukların cinsel istismarı veya müstehcenlik suçlarını oluşturan yayınlara ilişkin olarak içerik veya yer sağlayıcının yurt içinde bulunması durumunda TİB tarafından verilen kararın, yirmidört saat içinde hakimin onayına sunulacağı ve hakim kararının en geç yirmidört saat içinde verileceği düzenlenmiştir. Bu süre içinde kararın onaylanmaması halinde tedbir, Başkanlık tarafından derhal kaldırılacak ve erişim sağlayıcılara bildirilerek gereğinin yerine getirilmesi istenecektir. Yönetmelikle böyle bir hüküm öngörülmesi belki de doktrinde erişim engelleme kararının re'sen TİB tarafından alınmasına yönelik getirilen eleştirilerin hafifletilmesini amaçlamaktadır. Hatta doktrinde, TİB tarafından re'sen alınan diğer kararların da hakim onayına sunulması gerektiği savunulmaktadır[647]. Bizce Yönetmelikte yer alan bu hüküm 5651 sayılı Kanuna aykırılık oluşturmaktadır. Şöyle ki anılan Kanunda içeriği çocukların cinsel istismarı veya müstehcenlik suçlarını oluşturduğu düşünülen yayınlara ilişkin olarak erişimin engellenmesi kararının re'sen Başkanlık tarafından verileceği düzenlenmiştir. Bunun ötesinde bu kararın ayrıca hakim tarafından onaylanması öngörülmemiştir. Bu noktada Kanun ile yetkili kılınmış idari bir merciin görevine anılan Yönetmelik hükmü ile müdahale edilmiş ve *yetki gaspının*[648] ortaya çıkmasına zemin hazırlanmıştır.

TİB tarafından verilen re'sen erişim engelleme kararı, erişim sağlayıcısına bildirilerek gereğinin yerine getirilmesi istenir (md. 8/4). TİB tarafından erişim sağlayıcısına bildirilen erişimin engellenmesi kararının gereği, derhal ve en geç kararın bildirilmesi anından itibaren yirmidört saat içinde yerine getirilir. (md. 8/5)

TİB tarafından re'sen erişimin engellenmesi, idari tedbir olarak düzenlenmiştir. Bu tedbir geçici niteliktedir. Suç oluşturan içeriğin yayından çıkarılması durumunda re'sen erişimi engelleme tedbiri kaldırılacaktır. Bu özellik, re'sen erişimin engellenmesi tedbirini idari yaptırımdan

---

[647] Mehmet Bedii Kaya, **a.g.e.**, s. 122.

[648] Yetki gaspı, idarenin görev alanına giren bir konuda idarenin dışında yer alan kişi veya merciler tarafından karar alınması olarak tanımlanmakta ve bu kararlar *yok* hükmünde sayılmaktadır. Akyılmaz / Sezginer / Kaya, **a.g.e.**, s. 402. Günday, **a.g.e.**, s. 131.

ayırmaktadır[649]. İdari yaptırım geçici nitelikte değildir; doğrudan bir amaca yöneliktir ve kesindir. 5326 sayılı Kabahatler Kanununda ise idari yaptırım olarak iki tür yaptırım öngörülmüştür. Bunlar, "idari para cezası" ve "idari tedbir"dir[650]. İdari tedbir ise mülkiyetin kamuya geçirilmesi ve ilgili kanunlarda yer alan diğer tedbirler olarak düzenlenmiştir (md. 16). 5651 sayılı Kanunda da TİB'in erişimi engelleme kararı vermesi idari tedbir olarak ele alınmıştır (md. 8/11).

Genel olarak idari yaptırımlar[651], özel olarak ise erişimin engellenmesi tedbiri yönünden idareye, araya yargı kararı girmeksizin doğrudan yaptırım veya tedbir uygulayabilme yetkisinin verilmesi evvelden beri temel hak ve özgürlükler açısından sakıncalı bulunmuştur. Temel hak ve özgürlükler açısından bakıldığında erişimin bir yargı kararı olmaksızın idari bir merciin kararı ile engellenmesinin daha az güvence sağlayan bir sistem olduğu düşünülebilir[652]. Ancak, bazı durumlarda idareye böyle bir yetki tanınması ihtiyacı ortaya çıkabilmektedir. Bu tür durumlarda, ortaya çıkan ihtiyaca göre bir değerlendirme yapmak kaçınılmaz olmaktadır. Diğer kişilerin hak ve özgürlüklerinin korunmasının bu ihtiyacı belirleyen en önemli etken olduğu gözden kaçırılmamalıdır[653]. Bu çerçevede TİB'in re'sen erişimi engelleme kararı verebilmesi bazı sıkı şartlar altında gerçekleştirilebilmeli ve bunun hukuksal rejimi ayrıca düzenlenmelidir. İlk olarak re'sen erişimi engelleme kararları bağımsız bir kurul tarafından verilmeli; kararlar verilmeden önce içerik sağlayıcının savunmasının alınması[654], makul süreler öngörülmesi, gerekçe ilkesi, orantılılık ilkesi gibi temel hak ve özgürlükler açısından güvence niteliği taşıyan idari usul ilkeleri gözetilmelidir.

Nihayet, re'sen erişimin engellenmesinin nedenleri arasına özellikle terör suçları da konulmalıdır.

---

[649] Oğurlu, **İdari Yaptırımlar**, s. 84.
[650] Tanımlar için bkz. Oğurlu, **İdari Yaptırımlar**, s. 88.
[651] Gölcüklü, **a.g.m.**, s. 138.
[652] Bozbel, **a.g.m.**, s. 3.
[653] Çeçen, **a.g.e.**, s. 20-21.
[654] Uygulamada TİB'in 5651 sayılı Kanun kapsamında hukuka aykırı nitelik taşıyan içeriğe erişimi engelleme kararı vermeden önce ilgili içerik sahiplerini uyardığı belirtilmektedir. Akdeniz / Altıparmak, **a.g.e.**, s. 71. Ayrıca bkz. http://www.guvenliweb.org.tr/istatistikler/node/20, 24.12.2012.

7. Sonuçları

5651 sayılı Kanun, erişimi engelleme yöntemleri konusunda herhangi bir sınırlandırma içermemiştir[655]. İçeriği anılan Kanunda yer alan suçları oluşturduğu hususunda yeterli şüphe sebebi bulunan yayınlarla ilgili olarak erişimin engellenmesi, her hangi bir yöntemle alınabilir. Ancak, Kanunda erişim engelleme kararları konu itibariyle sınırlandırılmıştır. 8. maddede yer alan suçların işlenmiş olması ve bu hususta yeterli şüphe sebebinin bulunması bu sınırlandırmalardan iki tanesidir. Bunun yanısıra önemli olan bir diğer sınırlandırma da sadece 8. maddede yer alan suçları içeren içeriğe erişimin engellenebileceğine yönelik sınırlandırmadır. Bir diğer deyişle, bir internet sitesi içerisinde eğer içeriği 8. maddede yer alan suçlardan birisini oluşturan bir yayın varsa sadece bu yayına erişim engellenebilir. Yoksa, suç oluşturan bu yayından dolayı içeriği suç oluşturmayan diğer içeriğe erişimin engellenmesi mümkün değildir[656]. Bir internet sitesinin içeriğinde yer alan sadece bir kısım hukuka aykırı içerikten dolayı tüm siteye erişim engellenemez[657]. 8. maddenin bu anlamı ifade eden lafzı oldukça açıktır. Eğer yasa koyucu aksini düşünmüş olsaydı, "*suç oluşturan bir kısım içeriğe erişimin engellenememesi durumunda söz konusu internet sitesinin tamamına erişim engellenir"* şeklinde bir düzenleme içerirdi veya "*erişimin engellenmesi"* müessesesini "*internet sitelerine erişimin engellenmesi"* şeklinde düzenlerdi[658]. Aksi yönde bir yorum, içeriği hukuka uygun olan yayınlara da erişimin engellenmesi sonucunu ortaya çıkarır. İşte asıl bu durum ifade özgürlüğü ve haberleşme özgürlüğü gibi temel hak ve

---

[655] Mehmet Bedii Kaya, **a.g.e.**, s. 123.
[656] Dülger / Beceni, **a.g.e.**, s. 14.
[657] Akdeniz / Altıparmak, **a.g.e.**, s. 109.
[658] Aynı durum 633 sayılı Diyanet İşleri Başkanlığı ve Görevleri Hakkında Kanunun 6. maddesinde düzenlenen erişimin engellenmesi müessesesi açısından da geçerlidir. FSEK Ek 4. maddede ise farklı bir düzenleme yer almıştır. Ek 4. maddede, "bilgi içerik sağlayıcına verilen hizmetin durdurulması"ndan bahsedilmiştir. Şu halde Ek 4. madde kapsamında hak ihlalinde bulunan bilgi içerik sağlayıcılarının ihlal içeren içerikten dolayı internet sitelerinin tamamına yönelik erişimin engellenmesi mümkündür. Aksi yönde görüş için bkz. Dülger / Beceni, **a.g.e.**, s. 14. Bununla birlikte, Ek 4. maddenin kişi hak ve özgürlüklerini ölçüsüz bir şekilde sınırlandırdığı söylenebilir.

özgürlüklere ölçülü olmayan müdahale niteliği taşır[659]. İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmeliğin 15. maddesinde erişim engelleme yöntemi olarak sadece alan adı ve IP adresi olarak erişim engelleme yönteminin düzenlenmiş olması da bu sonucu değiştirmemektedir. Söz konusu Yönetmelik hükmünün 5651 sayılı Kanunun 8. maddesine aykırılık oluşturduğu açıktır. Erişimin engellenmesi açısından Kanunun öngördüğü sınırın çerçevesi anılan Yönetmelik hükmü ile aşılmaktadır. Bu nedenle, içeriğinin sadece bir kısmı 8. maddede yer alan suçlardan birisini oluşturan bir internet sitesinin tamamına erişimin engellenmesi yönünde hakim, mahkeme veya Cumhuriyet savcısı ya da TİB tarafından verilen kararların hukuka aykırı olduğunu belirtmemiz gerekir[660].

Ancak, bir internet sitesi örneğin, uyuşturucu veya uyarıcı madde kullanılmasını kolaylaştırma veya müstehcen içerik sunma amacıyla faaliyet gösteriyorsa ve yaptığı yayından bu açıkça anlaşılıyorsa, artık o internet sitesinin tamamına erişimi engelleme kararı verilebilmelidir. Bu durumda internet sitesi içerisinde hukuka aykırı olmayan başka yayınların da bulunmuş olması önem taşımamaktadır. İnternet sitesinin taşıdığı amacın araştırılması gerekir.

İçerisinde önemli ve hacim olarak oldukça geniş bilgiyi barındıran bir internet sitesine sadece hukuka aykırı bir içerikten dolayı erişimin engellenmesi, aslında çok yanlış ve vahim bir durumdur. Bir yazarın belirttiği gibi, bu durum zararlı bir kitaptan dolayı koskoca bir kütüphaneyi kapatmaktan farksızdır. Ancak, burada örneğin pornografik içerik taşıyan bir kitabın da bir halk kütüphanesinde bulunamayacağını veya bulunsa bile yetkili merciler tarafından bu kitabın kütüphaneden uzaklaştırılacağını göz önünde bulundurmak gerekir. Söz konusu internet olduğunda, kütüphane olayında olduğu gibi, çözümün bu kadar kolay olamayacağı görülmektedir. Fakat, bu noktada zararlı içeriği kaldırmak, o içeriği üreten kişinin

---

[659] Bozbel, **a.g.m.**, s. 4.

[660] Ülkemizde sadece hukuka aykırılık taşıyan internet sayfalarına erişimin engellenmesi yönünde de hakim veya mahkeme kararları bulunmaktadır. Akdeniz / Altıparmak, **a.g.e.**, s. 61.

sorumluluğunda olduğundan[661] bütün sorumluluğu devlete yüklemek haksız bir yaklaşım olur. Kişi bu sorumluluğu yerine getirmiyorsa, devlet gereken her türlü önlemi alacaktır ve hatta almak zorundadır. Dolayısıyla bu noktada devlete karşı ileri sürülen eleştirilerin yönünü biraz da zararlı içerik üreten kişi ve firmalara çevirmek sorunun çözümü açısından daha faydalı olacaktır. Ancak bu zorunluluk bir kısım hukuka aykırılıktan dolayı, hukuka aykırılık içermeyen içeriğe de erişimin engellenmesini yine de haklı göstermemektedir. Anılan hukuka aykırı içerik ile başka bir şekilde mücadele edilmelidir.

Erişimi engelleme kararının bir diğer sonucu, ülke dışı kaynaklı bir internet sitesine ülkede bulunan erişim sağlayıcılar aracılığıyla erişim engellendiğinde, o internet sitesine erişimin sadece o ülkeden engellenmesidir. Bu karara rağmen içerik diğer ülkelerde yayınlanmaya devam edecektir.

a. Erişimin Engellenmesi Kararının Kaldırılması

Soruşturma sonucunda kovuşturmaya yer olmadığına karar verilmesi halinde, erişimin engellenmesi kararı kendiliğinden hükümsüz kalır. Cumhuriyet savcısı, kovuşturmaya yer olmadığı kararının bir örneğini Başkanlığa gönderir (md. 8/7). Kovuşturma evresinde beraat kararı verilmesi halinde, erişimin engellenmesi kararı kendiliğinden hükümsüz kalır. Mahkemece beraat kararının bir örneği Başkanlığa gönderilir (md. 8/8). Konusu Kanunda sayılan suçları oluşturan içeriğin yayından çıkarılması halinde; erişimin engellenmesi kararı, soruşturma evresinde Cumhuriyet savcısı, kovuşturma evresinde mahkeme tarafından kaldırılır (md. 8/9).

Mahkumiyet halinde koruma tedbiri olarak verilen erişimin engellenmesi kararının durumunun ne olacağı Kanunda düzenlenmemiştir. Mahkumiyet hükmü ile birlikte koruma tedbiri niteliğindeki karar son bulacağından, erişimi engellemenin bir güvenlik tedbiri olarak ayrıca düzenlenmesi gerekirdi. Ancak, gerek TCK'da gerekse 5651 sayılı Kanunda

[661] Çeçen, **a.g.e.**, s. 107.

böyle bir güvenlik tedbiri düzenlenmemiştir. Şu halde, suç ve cezada kanunilik ilkesi gereği mahkumiyet halinde bir güvenlik tedbiri olarak erişimin engellenmesi kararının verilmesi mümkün gözükmemektedir[662]. 5651 sayılı Kanunun 10. maddesinin dördüncü fıkrasında yer alan, TİB'e re'sen erişimi engelleme yetkisi veren hükmün uygulanması dışında başka hukuksal bir imkan bulunmamaktadır. Mahkumiyet kararı, erişimin engellenmesi kararının verilmesinde TİB açısından bağlayıcı olacağı için, 10. maddenin dördüncü fıkrası çerçevesinde TİB, erişimi engelleme kararı vermek zorunda kalacaktır. Ancak, dördüncü fıkranın TİB'e her durumunda re'sen erişimi engelleme yetkisi vermediği unutulmamalıdır.

TİB tarafından re'sen verilen erişimin engellenmesi kararına konu hukuka aykırılığın giderilmesi halinde ise erişimin engellenmesi kararının kaldırılacağı 5651 sayılı Kanunda düzenlenmemiştir. Ancak, hukuka aykırılık giderildikten sonra artık erişimi engellenebilecek bir yayın bulunmayacağı için bu halde de erişimi engelleme kararının TİB tarafından kaldırılması gerekir. Bundan dolayı, re'sen erişimi engelleme kararlarının geçici nitelikte olmadığı ve süreklilik arz ettiği yönündeki görüşlere katılmamaktayız[663].

b. Erişimin Engellenmesi Kararının Yer ve Erişim Sağlayıcılarınca Yerine Getirilmemesi

Erişimin engellenmesi kararının yer ve erişim sağlayıcıları tarafından yerine getirilmemesi halinde bunlar hakkında uygulanacak bir sorumluluk rejimi öngörülmüştür. Koruma tedbiri olarak verilen erişimin engellenmesi kararının gereğini yerine getirmeyen yer sağlayıcılarının sorumluları, fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde altı aydan iki yıla kadar hapis cezası ile cezalandırılır. (5651 sayılı Kanun md. 8/10) Koruma tedbiri olarak verilen erişimin engellenmesi kararının gereğini yerine getirmeyen erişim sağlayıcılarının sorumluları ise fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde altı aydan iki yıla kadar hapis

---

[662] Dülger / Beceni, **a.g.e.**, s. 14.

[663] Re'sen erişimi engelleme kararlarının kimi zaman süresiz olacağı yönündeki bir görüş için bkz. Akdeniz / Altıparmak, **a.g.e.**, s. 30-31.

cezası ile cezalandırılır (5651 sayılı Kanun md. 8/10). İdari tedbir olarak verilen erişimin engellenmesi kararının yerine getirilmemesi halinde, Başkanlık tarafından erişim sağlayıcısına onbin Yeni Türk Lirasından yüzbin Yeni Türk Lirasına kadar idari para cezası verilir. İdari para cezasının verildiği andan itibaren yirmidört saat içinde kararın yerine getirilmemesi halinde ise Başkanlığın talebi üzerine Kurum tarafından yetkilendirmenin iptaline karar verilebilir (5651 sayılı Kanun md. 8/11).

Birinci parağrafta yer alan suçlar, 5651 sayılı Kanunun internete özgü öngördüğü suçlar olarak ele alınabilir[664]. Bu çerçevede, 5651 sayılı Kanunun diğer tanımlamalar yanı sıra ceza hükümleri öngören bir kanun olarak değerlendirilmesi gerekir. Kanunun, yer ve erişim sağlayıcılarının koruma tedbiri niteliğindeki erişimi engelleme kararlarını yerine getirmemelerinin yaptırımını cezai bir yaptırım olarak öngörmesi uygun olmamıştır. Yukarıda da belirtildiği gibi yürüttükleri ticari bir faaliyetten dolayı öngörülen regule edici düzenlemelerin yerine getirilmemesinden dolayı erişim ve yer sağlayıcıların faaliyetlerinin cezai sorumluluk yerine idari sorumluluk sistemi ile karşılanması çok daha adil ve yerinde olacaktır.

c. Erişimin Engellenmesi Tedbiri Nedeniyle Tazminat İstemi

Hakim, mahkeme veya Cumhuriyet savcısı tarafından alınan erişimin engellenmesi kararları koruma tedbiri niteliğinde kararlar olduğundan dolayı, soruşturma veya kovuşturma sonucunda söz konusu içeriğin Kanunda sayılan suçları içermediği kanaatine varıldığında bu karar kaldırılmaktadır; ancak bu kararlardan dolayı içerik sahibi kişilerin zarara uğraması oldukça muhtemeldir. Zararın devletçe karşılanması hukuk devleti olmanın bir gereğidir. Ancak, 5651 sayılı Kanunda söz konusu tazminat kuralları düzenlenmemiştir. Koruma tedbirleri nedeniyle tazminatı düzenleyen 5271 sayılı CMK'nın 141. maddesinde de erişimin engellenmesi nedeniyle tazminat kuralları düzenlenmemiştir. Bu yaklaşımın bir eksiklik oluşturduğu bir an için düşünülebilirse de Anayasamızın 40. maddesinin üçüncü fıkrası ve

[664] İçel, **a.g.m.**, s. 26.

2802 sayılı Hakimler ve Savcılar Kanununun 93/A maddesi gereğince koruma tedbiri olarak verilen erişimin engellenmesi kararlarından doğan zararlar nedeniyle Devlete karşı tazminat davası açılmasının önünde bir engel bulunmamaktadır. Anayasamızın 40. maddesine göre kişinin, resmi görevliler tarafından vaki haksız işlemler sonucu uğradığı zarar kanuna göre Devletçe tazmin edilir. Devletin sorumlu olan ilgili görevliye rücu hakkı saklıdır. Hakimler ve Savcılar Kanununun 93/A maddesine göre ise hakim ve savcıların bir soruşturma, kovuşturma veya davayla ilgili olarak yaptıkları işlem, yürüttükleri faaliyet veya verdikleri her türlü kararlar nedeniyle Devlet aleyhine tazminat davası açılabilir. Hatta bu hükme göre, hakim ve savcılarının bir soruşturma, kovuşturma veya davayla ilgili olarak yaptıkları işlem, yürüttükleri faaliyet veya verdikleri her türlü kararlar nedeniyle Devlet aleyhine açılacak tazminat davaları ile rücu davalarında bu madde hükümleri; bu maddede hüküm bulunmayan hallerde ise ilgisine göre Hukuk Usulü Muhakemeleri Kanunu ile Ceza Muhakemesi Kanunu hükümleri uygulanır[665]. 2577 sayılı İdari Yargılama Usulü Kanununa göre tam yargı davaları ancak idari eylem ve işlemler hakkında açılabileceğinden, Hakimler ve Savcılar Kanununun 93/A maddesi uyarınca Devlete karşı açılacak tazminat davalarında görevli yargı kolu adli yargıdır.

TİB tarafından verilen re'sen erişim engelleme kararlarına karşı ise idari yargıda "*tam yargı davası"* açılması her zaman mümkündür.

8. Uyar-Kaldır İlkesi

"*Uyar - kaldır ilkesi*" *(notice and takedown),* hukuka aykırı nitelik taşıyan içeriğe erişimin engellenmesinin sağlanması amacıyla internet servis sağlayıcılarının uyarılması ve bu uyarı üzerine içeriğe erişimin engellenmemesi durumunda bunların sorumluluklarına gidilmesi gerekliliğini ifade eden bir ilkedir. Bu ilke ile internet servis sağlayıcılarının başkalarına ait içerikten dolayı doğrudan sorumluluklarına gidilmesinin önü kapatılmıştır.

---

[665] Devletin sorumluluğuna ilişkin Hakimler ve Savcılar Kanununun 93/A maddesinde yer alan diğer şartlar için ilgili hükme bakılabilir. http://www.mevzuat.gov.tr/MevzuatMetin/1.5.2802.pdf, 24.12.2012.

Uyar-kaldır ilkesi, Türk hukukunda da yer bulmuştur. 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunun 8. ve 9. maddelerinde erişim ve yer sağlayıcıların hukuka aykırı içeriğe erişimi engellemeleri veya içerikten çıkarmaları konusunda uyar-kaldır ilkesi esas alınmıştır. Benzer bir yaklaşım FSEK'in Ek 4. maddesinde de öngörülmüştür. Buna göre, hakkının ihlal edildiğini ileri süren kişi öncelikle bilgi içerik sağlayıcına başvuracak, bu başvuru olumsuz sonuçlanırsa bu durumda Cumhuriyet savcısına başvuru yapacaktır.

İnternet servis sağlayıcılardan istenen erişimin engellenmesi veya hukuka aykırı içeriğin çıkarılması konusundaki talepler "gerçek bilgi" niteliğinde olmalıdır. Gerçek bilgi, herhangi bir yerden gelen rastgele bir bilgi değil; yetkili kamu kurumları veya mahkemelerden gelen bilgi olmalıdır. İngiltere ve Hollanda'da yapılan iki çalışmada rol gereği sahte bir organizasyon ismi kullanılarak hosting firmalarına kendilerine ait fikri mülkiyet hakkının ihlal edildiğine ilişkin bilgi iletilmiş ve ilgili hosting firmalarınca gerekli inceleme ve hukuksal değerlendirme yapılmaksızın anılan içeriğe erişim engellenmiştir[666].

Uyar-kaldır ilkesinin geliştirilmesine yönelik düzenlemeler yapılması, temel hak ve özgürlükler açısından daha güvenceli bir hukuk sistemi ortaya çıkaracaktır.

9. Türkiye'deki Uygulama ve Youtube'a Erişimin Engellenmesi

Türkiye'de erişim engelleme kararları 2000'li yılların başlangıcında mahkeme kararları veya idari kararlarla içeriği hukuka aykırı bulunan bazı internet siteleri hakkında uygulanmaya başlanmıştır. 2005'de Müzik Yapımcıları Derneğinin (MÜYAP), fikri mülkiyet hakkı kapsamında internetten müzik indirmeye imkan tanıyan internet sitelerine erişimin engellemesi talepleri, erişim engelleme kararlarında da artışı beraberinde getirmiştir[667]. 5651 sayılı Kanun bu dönemde yürürlükte olmadığından dolayı o dönemde

[666] Craddock, **a.g.m.**, s. 29.
[667] Akdeniz / Altıparmak, **a.g.e.**, s. 17.

verilen erişimi engelleme kararları Basın Kanunu (ör: satış yasağına ilişkin hükümler), CMK (ör: soruşturma hükümleri) veya Hukuk Usulü Muhakemeleri Kanununda (ör: ihtiyati tedbir hükümleri) yer alan bazı hükümlere ya da genel olarak cezai hükümlere (içeriğin suç oluşturmasından dolayı erişimin engellenmesi) dayandırılarak gerçekleştirilmiştir[668].

Ülkemizde erişimi engellenen veya filtrelenen internet siteleri hakkında tam bir bilgiye maalisef ulaşılamamaktadır[669]. Her ne kadar bir sorgulama sistemi[670] geliştirilmiş olsa da bu sistemin engellenen siteler hakkında yeterli bilgi verdiği söylenemez. Hangi internet sitelerinin hangi hukuksal gerekçelerle engellendiğine yönelik bilgi mutlaka kamuoyu ile paylaşılmalıdır[671]. Yönetimde şeffaflık ilkesi gereği erişimi engellenen internet sitelerinin, engelleme gerekçeleri ile birlikte yayınlanması gerekmektedir. Şeffaflık, filtrelenen internet sitelerinin açıklanmasını da gerekli kılmaktadır[672].

Diğer taraftan, engellenen internet sitelerinin sayfalarında engelleme mahkeme kararı ile gerçekleştirilmişse, "*Bu siteye erişim mahkeme kararıyla engellenmiştir"* açıklaması düşülmekte ve bu açıklamanın altına da kararı veren mahkemenin karar tarih ve sayısı ile bu karara istinaden siteye erişimin TİB tarafından engellendiği ve bunun İngilizce tercümesi yer almaktadır. Engelleme TİB tarafından gerçekleştirilmişse, *"Bu siteye erişim engellenmiştir"* notu düşülmekte ve engellemenin 5651 sayılı Kanun uyarınca katalog suçlar kapsamında yapılan teknik inceleme ve hukuksal değerlendirme sonucunda, TİB tarafından alınan kararın tarih ve sayısı ile idari tedbir niteliği de belirtilerek gerçekleştirildiği açıklamasına ve bunun İngilizce tercümesine yer verilmektedir. Ancak, söz konusu mahkeme

---

[668] Durnagöl, **a.g.m.**, s. 376. Akdeniz / Altıparmak, **a.g.e.**, s. 59-64. Bazı ülkelerde yürürlükteki genel hükümler, örneğin ulusal güvenliğin sağlanmasına ilişkin mevcut hükümler, özel bir düzenleme yapılmaksızın erişimin engellenmesine doğrudan dayanak oluşturabilmiştir. Yine çoğu ülkede, ulusal güvenlik veya kültürel değerlerin korunması gibi nedenlerle informal bir şekilde erişim veya yer sağlayıcılardan sakıncalı içeriğin çıkarılması istenebilmektedir. Deibert / Rohozinski, **a.g.m.**, s. 50-51.

[669] Bilgi Teknolojileri ve İletişim Kurumu 2011 Faaliyet Raporunda bu konuda herhangi bir veriye yer verilmemiştir. Bkz. Bilgi Teknolojileri ve İletişim Kurumu, **Faaliyet Raporu 2011,** http://www.tk.gov.tr/kutuphane_ve_veribankasi/raporlar/faaliyet_raporlari/index.php, 05.10.2012.

[670] Bkz. http://eekg.tib.gov.tr/, 12.10.2012.

[671] Erişimi engelleme veya filtreleme uygulamalarının en önemli sakıncalarından birisi şeffaflık ve hesap verilebilirliğin ihlal edilmesidir. Bkz. Breindl / Wright, **a.g.m.**, s. 2.

[672] OpenNet Initiative, **A Starting Point: Legal Implications of Internet Filtering**, 2004, http://www.opennetinitiative.org, 09.10.2012, s. 16.

kararlarının gerekçesi açıklanmamaktadır. TİB kararlarının ise sadece katalog suçlar kapsamında alındığının belirtilmesi ile yetinilmektedir[673]. Benzer bir uygulama diğer birçok Batı devleti tarafından da gerçekleştirilmektedir. Örneğin, İngiltere'de İnternet İzleme Kuruluşunun erişimi engellediği internet sitelerine ulaşılmak istendiğinde *"Page not found"* veya *"Access forbidden"* uyarıları ile karşılaşılmaktadır[674]. Bu tür uygulamalara bir an önce son verilerek hukuksal güvenliğin sağlanması, şeffaf yönetim anlayışı ve demokratik meşruiyet ilkelerinin bir gereği olarak erişimi engellenme kararlarının hukuksal gerekçesi ilgili internet sayfalarında açıklanmalıdır[675].

TİB tarafından yayınlanan ihbar istatistiklerine göre vatandaşlar tarafından internet içeriğine ilişkin olarak müstehcenlik (% 74.70), çocukların cinsel istismarı ve müstehcenlik (% 19.51), fuhuş (% 3.96), kumar (% 1.38), sabit ihtimalli ve müşterek bahis ve kumar (% 0.27) ve intihara yönlendirme (% 0. 18) suçlarından dolayı TİB'e ihbarda bulunulmuştur. TİB, erişim engelleme istatistiklerine göre ise intihara yönlendirme (% 3.70), çocukların cinsel istismarı (% 4.58), uyuşturucu veya uyarıcı madde kullanılmasını kolaylaştırma (% 0.49), sağlık için tehlikeli madde temini (% 0.66), müstehcenlik (% 46.71), fuhuş (% 9.38), kumar oynanması için yer ve imkan sağlama (% 2.88), Atatürk aleyhine işlenen suçlar (% 7.54) ve diğer (% 24.35) gerekçeler ile internet içeriğine erişim engellenmiştir[676].

Konuyu Youtube'a erişimin engellenmesi açısında ele aldığımızda ülkemizde Youtube'a erişim 2007-2008 yılları arasında ağırlıklı olarak 5816 sayılı Atatürk Aleyhine İşlenen Suçlar Hakkında Kanunda yer alan suçlar nedeniyle mahkeme kararları ile engellenmiştir[677]. Youtube'un kapatılması konusunda eleştirilen taraf hep devlet olmuştur[678]. Ancak, Youtube'un

---

[673] Ülke uygulamalarında, bir internet sitesine erişimin engellenmesi hiçbir bilgiye yer verilmeden (silent blocking), hata kaydı (error based blocking) veya bilgilendirme notu düşülerek (notification of blocking) gerçekleştirilebilmektedir. Breindl / Wright, **a.g.m.**, s. 3. McIntyre / Scott, **a.g.m.**, s. 3.
[674] Craddock, **a.g.m.**, s. 33.
[675] Akdeniz / Altıparmak, **a.g.e.**, s. 96.
[676] http://www.guvenliweb.org.tr/istatistikler/files/ihbar_istatistikleri_13.12.2012.pdf, 24.12.2012.
[677] Akdeniz / Altıparmak, **a.g.e.**, s. 55-57.
[678] Youtube yasağının Türkiye'yi totaliter devlet düzeyine getirdiği hakkında bkz. Bozbel, **a.g.m.**, s. 1.

yaklaşımının da en az devletin bu yöndeki yaklaşımı kadar eleştirilmesi gerekir. Hiçbir devlet, Youtube tarafından belirlenen ilkeler doğrultusunda hareket etmek zorunda değildir. Youtube'un ilkeleri, devletin ilkelerinden daha üstün değildir. Ulusal egemenlik teorisi, devleti Youtube'a müdahale etmeye zorunlu kılmaktadır. Ayrıca, Youtube'un kendi belirlediği ilkeler maalesef bu sitede kişilik haklarını ihlal eden, şiddet içeren, nefret söylemi yayan, terör propagandasına imkan tanıyan milyonlarca videonun yayınlanmasını engellememektedir.

Türkiye'de Youtube'un kapatılması kararının etkisiz kılınması amacıyla Google, kendisine ait bazı IP'leri Youtube'a tahsis etmiş ve Youtube bu aralıktan yayın yapmak istemiştir. BTK, bu girişimi etkisiz kılmak amacıyla, söz konusu IP aralığından yapılan yayınlara da erişimi engellemiş ve bunun sonucu olarak Google'ın Google Maps, Google Translate, Google Analytics, Google Earth ve Google Docs gibi hizmetlerine de erişim sağlanamamıştır. Bu gelişim, BTK tarafından Google'un da kapatıldığı yönünde bir kamuoyu oluşmasına neden olmuştur. Google ve Youtube'un bu girişiminin Türk devletini yasakçı ilan ettirme yönünde bir taktik olduğu da ileri sürülmüştür[679].

10. Erişimin Engellenmesinin Teknik Açıdan Etkinliği

İnternetin düzenlenmesi söz konusu olduğunda ileri sürülen veya tartışılan önemli konulardan birisi, internetin düzenlemeye uygun bir yapı oluşturup oluşturmadığı hususudur. Bu noktada internetin düzenlemeye uygun bir yapı oluşturmadığı ileri sürülebilir. Bu iddia, internetin sınır tanımayan yapısından kaynaklandığı gibi teknolojik gerekçelerden de kaynaklanabilmektedir. Teknolojik açıdan interneti düzenlemek ne kadar zorlaşırsa hukuksal açıdan da o kadar zorlaşmaktadır.

Bu noktada, "*internetin hukuksal açıdan düzenlenmesi – teknik açıdan düzenlenmesi"* ayrımı karşımıza çıkmaktadır. Ayrım özellikle internete erişimin engellenmesi kararlarının alınması durumunda söz konusu olmaktadır. Kararların hukuken alınması ile erişimin teknik olarak

[679] Medya Derneği, **Türkiye'nin internet Sansürü Sorunu**, Redaksiyon ve Güncelleme: Aslı Telli Aydemir, Temmuz 2010, s. 11.

engellenebilmesi farklılık göstermektedir. Bir diğer deyişle, internete erişimin engellenmesi hukuksal ve teknik açıdan farklı boyutlar taşımaktadır.

Hukuksal açıdan konuya yaklaşıldığı zaman bir görüş internetin hukuksal açıdan düzenlenemeyeceğini iddia etmektedir. Anılan görüşün temel dayanak noktası internetin sınır tanımayan yapısı ve evrensellik özelliğidir. Bu özellikler internetin devletler tarafından düzenlenmesini mümkün kılmamaktadır. Bir diğer görüş ise internetin düzenlenmesinde bir mükemmellik aranmaması gerektiğini, etkin bir düzenleme yapılmasının yeterli olacağını ileri sürmektedir[680]. Hatta, sırf düzenleme dahi hiçbir yaptırım içermese bile ciddi bir etkinlik düzeyine sahiptir. İnsanların büyük bir kısmı kurallara, bu kurallar yaptırım altına alındığı için değil ve fakat kural olarak belirlendiği ve dolayısıyla meşruiyet taşıdığı için uymaktadır[681].

Teknik açıdan ise her ne kadar interneti etkin bir şekilde düzenlemenin bazı zorlukları bulunsa da teknolojinin devletin elini kolunu bağladığı her koşulda söylenemez. Tam aksine, bilgi ve iletişim teknolojilerindeki gelişmeler teknolojik açıdan düzenlemenin etkinliğini artırıcı bir seyir izlemektedir[682]. Gelecekte bu etkinliğin teknolojik açıdan güçleneceği ifade edilmektedir[683].

Öte yandan, devlet tarafından erişimin engellenmesi kararının verilmesi belirli bir düzeye kadar etkinliğe sahip olmakla birlikte belirli bir noktadan sonra bu etkinlik geçerliliğini yitirmeye başlamaktadır. Erişimin engellenmesi kararları internet kullanıcıları tarafından çeşitli teknik yöntemler kullanılarak aşılabilmektedir.

a. Dark Web

Sıradan insanların internette ulaşabildiklerinin ötesinde ücretsiz bir şekilde internetten indirilebilen kimi programlar sayesinde "*dark web"* denilen internet sayfalarına ulaşabilmenin mümkün olduğu ileri sürülmektedir[684].

---

[680] Mayer-Schönberger, **a.g.m.**, s. 614-615.
[681] Mayer-Schönberger, **a.g.m.**, s. 615.
[682] Deibert / Rohozinski, **a.g.m.**, s. 48.
[683] Weckert, **a.g.m.**, s. 105.
[684] http://www.bbc.co.uk/news/business-16801382, 02.06.2012.

Uyuşturucu ve silah ticareti, sahte pasaport temini, çocuk pornografisi gibi suç teşkil eden faaliyetler ile terörizm ve kimi anti-demokratik ülkelerde rejim karşıtı faaliyetlerin yürütüldüğü bu internet sayfalarına normal insanların erişmesi mümkün değildir[685]. Bu sayfalara erişim internet düzenleyicileri tarafından engellenmiştir. Gizli ve ayrı bir internet dünyasını oluşturan dark webde bu faaliyetleri yürüten insanların takip edilmesinin ve bunlara ulaşılabilmesinin teknik olarak mümkün olmadığı ileri sürülmektedir[686].

Dark web buzdağının altında kalan kısmını, erişilebilen internet ise üstünde kalan kısmını oluşturmaktadır[687].

b. Erişimin Engellenmesi Kararlarının Aşılmasını Sağlayan Teknik Yöntemler

Erişimin engellenmesi kararının aşılmasını sağlayan birçok teknik yöntem bulunmaktadır. Bunlara her geçen gün bir yenisi eklenmektedir. Yeni yöntemler öncekilere göre daha gelişmiş, kompleks ve etkin şekillerde tasarlanmaktadır. Söz konusu yöntemlere ulaşmak ve bunları kullanmak çoğu zaman oldukça kolaydır. İnternette, erişime engellenmiş sitelere nasıl girileceğine ilişkin bir araştırma yapıldığında gerekli bilgilere kolayca ulaşılabilmektedir. Hatta, erişime engellenmiş sitelere ulaşılmasını sağlayan programların internette satışa sunulduğunu görmek artık sıradan bir hal almıştır.

Proxy ayarlarının değiştirilmesi, içerik aldatması, DNS ayarlarının değiştirilmesi, erişimin engellenmesi kararını bertaraf eden programların kullanılması gibi yöntemler, erişimin engellenmesi kararlarının aşılmasını sağlayan teknik yöntemlerden bazılarıdır[688]. Örneğin, sunucuları ülke dışında bulunan ve Türk hukukuna tabi erişim sağlayıcılar aracılığıyla erişimi engellenen bir internet sitesine, yine sunucuları ülke dışında bulunan başka bir internet sitesi aracılığıyla erişimi engellenen sitenin proxy ayarları

---

685 Deibert / Rohozinski, **a.g.m.**, s. 48.
686 http://www.bbc.co.uk/news/business-16801382, 2.6.2012.
687 http://www.guardian.co.uk/technology/2009/nov/26/dark-side-internet-freenet 2.6.2012.
688 Mehmet Bedii Kaya, **a.g.e.**, s. 41 vd.

değiştirilmek suretiyle erişim sağlanabilmektedir. Türkiye'de *Youtube'*a erişim engellendiği zaman, bu siteye *vtunnel* aracılığıyla erişmek mümkün olmuştu.

Erişimi engellenen bir internet sitesinin anında aynı içerikle başka bir alan adı altında açılabilmesi gibi, bu tür teknik yöntemlerin kullanılması dışında erişimin engellenmesi kararlarını etkisizleştiren başka yöntemler de bulunmaktadır. Birinci derece alan adında değişiklik yapılabileceği gibi ikinci derece alan adında da değişiklik yapılabilir. Özellikle birinci derece alan adında değişiklik yapılarak aynı sitenin açılması, erişimin engellenmesi kararının etkinliğini azaltmaktadır. Erişimi engellenen www.abcd.com internet sitesi, anında www.abcd.net alan adı ile aynı içerikle açılabilir. Yine, erişimi engelleme kararını etkisiz hale getirmek için içerik sağlayıcılar, yer sağlayıcı hizmetini ülke dışından alabilmekte, IP bloklama yöntemini aşmak için yeni bir hosting firması ile anlaşabilmektedir.

Nihayet, erişimin engellenmesi kararı verilmesi durumunda, her ne kadar söz konusu internet içeriğine ülke içinden ulaşmak mümkün olmasa da erişimi engellenen içeriğe ülke dışından erişilmesi imkanı ortadan kaldırılamamaktadır.

Ç. Filtreleme

Erişimin engellenmesinin bir yöntemi olmakla birlikte bireysel olarak alınan erişimin engellenmesi kararlarına göre oldukça farklı bir uygulama olduğundan filtreleme (internet filtering) konusu burada ayrı bir başlık altında incelenmiştir.

1. Genel Olarak Filtreleme

"Filtreleme", geliştirilen yazılım programları ile internette yer alan istenmeyen içeriğe kullanıcılar tarafından erişilmesini otomatik bir şekilde önceden önleyen teknik ve hukuksal bir iş olarak tanımlanabilir[689]. Bireysel erişimin engellenmesi kararlarında olduğu gibi filtreleme de hemen her devlet

[689] Rosenberg, **a.g.m.**, s. 37. McIntyre / Scott, **a.g.m.** s. 1.

tarafından başvurulan bir yöntem haline gelmiştir[690]. Elbette, devletlerin uygulamaları arasında önemli farklılıklar bulunmaktadır. Filtrelemenin konusunu esaslı olarak okul, üniversite, kütüphane ve diğer kamusal alanlarda sunulan internet erişim hizmetleri oluşturabileceği gibi böyle bir sınırlandırma yapılmaksızın ülke genelinde sunulan erişim hizmetleri de oluşturabilir[691]. ABD'de uygulanan filtreleme sistemi kural olarak okul, üniversite, kütüphane ve diğer kamusal alanlarda gerçekleştirilmektedir[692] ve ABD'de uygulanan bu sistemin kapsamı oldukça geniştir[693]. ABD'de, Children's internet Protection Act (CIPA) 2004 yılında yürürlüğe girmiştir. CIPA, okul ve kütüphanelerde yer alan bilgisayarlarda, bu bilgisayarlar ve internete erişim için kamusal mali destek alınması şartı ile çocukların müstehcen (obscene) veya zararlı (harmful) içeriğe erişiminin engellenebilmesi için filtrelemeyi zorunlu kılmaktadır[694]. Ülkemizde, belli suçların önlenmesi açısından genel bir filtreleme sistemi dışında spesifik olarak okul ve kütüphanelerde uygulanabilecek böyle bir sistem kabul edilmemiştir. Ancak, ticari amaçlı toplu kullanım sağlayıcılar nezdinde uygulanabilecek bir filtreleme sistemi ayrıca kabul edilmiştir. Bazı devletler ise düzenleme ihtiyacı duymaksızın filtreleme yapmakta ve filtreleme uygulamalarını kabul etmemektedir. 2009 yılında WikiLeaks tarafından ortaya konulan belgelerle Avusturalya, Finlandiya, Danimarka ve Norveç'in belli sitelere erişimin engellenmesi amacıyla filtreleme uyguladığı anlaşılmıştır[695]. Bu nedenle, bu ülkelerde gerçek anlamda bir filtreleme verisine çoğu zaman

---

[690] OpenNet Initiative, **A Starting Point: Legal Implications of Internet Filtering**, 2004, http://www.opennetinitiative.org, 09.10.2012, s. 4. Faris / Zittrain, **a.g.m.**, s. 90.

[691] Craddock, **a.g.m.**, s. 10.

[692] OpenNet Initiative, **A Starting Point: Legal Implications of Internet Filtering**, 2004, http://www.opennetinitiative.org, 09.10.2012, s. 4.

[693] Rosenberg, **a.g.m.**, s. 40.

[694] ABD' deki düzenlemeler federal ve federe devletler düzeyinde farklılık göstermektedir. Bu nedenle federe bir devlet açısından, diğer alanlarda olduğu gibi, filtreleme alanında da federal ve federe devlet düzenlemelerinin birlikte göz önünde bulundurulması gerekir. Biz çalışmamızda sadece federal devlet düzenlemelerini göz önünde bulundurduk.

[695] Faris / Zittrain, **a.g.m.**, s. 94. http://www.abc.net.au/news/2009-03-19/internet-filter-blacklist-leaked-on-web/1623890, 18.03.2013. Norveç 3518, Finlandiya 797, Danimarka 3863 ve Avusturalya 2395 alan adına erişimi gizlice engellemiştir. Craddock, **a.g.m.**, s. 12.

ulaşılamamaktadır. Filtrelemenin denetimi de tam olarak mümkün olmadığı için, ne şekilde bir filtreleme uygulandığı çoğu zaman anlaşılamamaktadır[696].

Filtrelemenin nedenlerine bakıldığı zaman erişimin bireysel olarak engellenmesini gerektiren nedenlerin burada da etkili olduğu görülmektedir. İngiliz hükümeti, İnternet İzleme Kuruluşu (Internet Watch Foundation) tarafından çocuk pornografisi olarak tanımlanan içeriğe erişimin ülkede faaliyet gösteren tüm internet servis sağlayıcılar tarafından filtrelenmesini zorunlu kılmaktadır[697].

Filtreleme, alan adı düzeyinde anahtar kelimelerin filtrelenmesi yöntemiyle belli internet sitelerine erişimin engellenmesi, e-mail trafiğinin bloke edilmesi, arama sonuçlarının istenilenden farklı sonuçlar ortaya koyması gibi etkilere sahiptir[698]. Ülkenin internet omurgası, internet servis sağlayıcılar, internet kafeler, kurum veya kuruluşlar düzeyinde filtreleme uygulanabilmektedir[699].

Filtrelemenin ortaya çıkardığı en önemli sorunlardan biri, hukuka uygun içeriğin de filtrelemeye takılabilmesidir (overblocking)[700]. Uyuşturucu bağımlılığı ile mücadele konusunda bilimsel bilgiler içeren bir internet sitesini, uyuşturucu ticareti yapan veya uyuşturucu bağımlılığını özendiren bir siteden filtreleme yöntemi ile ayırmak her zaman mümkün olamamaktadır. Yine, "*sex"* kelimesi filtrelendiği zaman İngiltere'nin "*Sussex"* ve "*Essex"* bölgelerinin isimlerini içeren içeriğe de, bu isimler içerisinde sex sözcüğü geçtiği için erişimin engellenebileceği ileri sürülmüştür[701]. Ancak, filtreleme yazılımları günümüzde oldukça gelişmiş bir düzeye ulaşmıştır. Artık, erişimi istenmeyen bir anahtar kelimeden dolayı tüm sitenin erişimini engelleyen

---

[696] Google, Microsoft ve Yahoo gibi bazı uluslararası şirketler Çin veya bazı Arap ülkelerinde, söz konusu ülkelerin belirlediği çerçevede filtreleme uygulamaktadır. Özellikle, anılan şirketler tarafından arama motorları filtrelenmektedir. Deibert / Rohozinski, **a.g.m.**, s. 52. McIntyre / Scott, **a.g.m.** s. 1.

[697] Schultz, **a.g.m.**, s. 827. McIntyre / Scott, **a.g.m.** s. 1.

[698] OpenNet Initiative, **A Starting Point: Legal Implications of Internet Filtering**, 2004, http://www.opennetinitiative.org, 09.10.2012, s. 4.

[699] https://opennet.net/about-filtering, 12.03.2013. Craddock, **a.g.m.**, s. 4.

[700] McIntyre / Scott, **a.g.m.** s. 7.

[701] Rosenberg, **a.g.m.**, s. 41. Ülkemizde güvenli internet hizmeti uygulamasında, "s*ussex"* veya "*essex"* kelimelerini içeren internet sitelerine erişilebilmektedir. Bkz. http://guvenlinet.org.tr/sorgula, 12.10.2012.

filtreleme yazılımlarının yerini, istenmeyen sayfaların erişimini engelleyen filtre yazılımları almıştır[702].

Filtrelemenin ortaya çıkarabileceği bir diğer sorun, kişilerin zihninde, filtrelenmeyen içeriğin ahlaki veya hukuka uygun olduğu yönünde bir algı yaratmasıdır[703].

Filtrelemenin etkisiz, zararlı ve kolayca aşılabilir bir yöntem olduğu ileri sürülmektedir. Bu görüşe göre filtreleme sistemi, sohbet odaları, dosya transfer protokolleri (FTP), internet sohbet protokolleri ve IP ses iletim sistemlerini etkilememektedir[704]. Ayrıca filtreleme uygulaması, filtreleme yazılımı üreten firmaların doğrudan kendileri tarafından filtrelenecek listeler oluşturmalarını sağlayabilmektedir[705]. Hatta, kişilerin ne tür içeriğe ulaşıp ulaşamayacağına ABD filtreleme yazılım firmalarınca karar verilmekte olduğu ileri sürülmektedir[706].

Bazı olumsuz etkilerine rağmen, belli bir düzeyde etki göstermesi bile filtreleme yöntemine başvurulmasını gerektirebilir[707].

2. 5651 Sayılı Kanun Çerçevesinde Filtreleme

5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunda TİB'e bazı şartlar altında filtreleme yapma yetkisi verilmiştir. Bu yetki, TİB'e doğrudan öngörülmüş bir düzenleme ile değil; dolaylı anlatım içeren düzenlemeler ile verilmiştir. Kanunda, TİB'in görev ve yetkileri belirlenirken TİB'e, BTK tarafından işletmecilerin yetkilendirilmeleri ile mülki idare amirlerince ticari amaçlı toplu kullanım sağlayıcılara verilecek izin belgelerinde filtreleme ve bloke etmede kullanılacak sistemlere ve yapılacak düzenlemelere yönelik esas ve usullerin belirlenmesi yetkisi (md. 10/4, ç) ve internet ortamında herkese açık çeşitli servislerde yapılacak filtreleme, perdeleme ve izleme esaslarına göre donanım üretilmesi veya yazılım

[702] http://infopeople.org/resources/filtering/history, 11.10.2012.
[703] McIntyre / Scott, **a.g.m.** s. 13.
[704] Akdeniz / Altıparmak, **a.g.e.**, s. 163.
[705] Uçkan / Beceni, **a.g.m.**, s. 379.
[706] McIntyre / Scott, **a.g.m.** s. 9.
[707] McIntyre / Scott, **a.g.m.** s. 3.

yapılmasına ilişkin asgari kriterleri belirleme yetkisi (md. 10/4, e) de verilmiştir.

Doktrinde bazı yazarlar, 5651 sayılı Kanunun söz konusu düzenlemeleri ile TİB'e filtreleme konusunda sınırsız bir yetkinin tanındığını, bu düzenlemeler ile TİB'in her konuda istediği şekilde filtreleme yapabileceğini ileri sürmüştür[708]. Biz bu görüşlere katılmamaktayız. Söz konusu düzenlemeler TİB'e sınırsız bir filtreleme yetkisi vermemiştir. TİB'in söz konusu düzenlemeler çerçevesinde filtreleme yetkisi ancak "*Başkanlığın bu Kanun kapsamındaki görev ve yetkileri"* ile sınırlıdır. Bu sınırlama 10. maddenin dördüncü fıkrasının ilk cümlesinde açıkça belirtilmiştir. Kanunun 1. maddesinde ise Kanunun amaç ve kapsamı "*internet ortamında işlenen belirli suçlarla mücadeleye ilişkin esas ve usuller"* olarak belirlenmiştir. Kanun kapsamında belirlenen suçlar ise 8. maddede belirlenenlerden ibarettir. Şu halde TİB, sadece 8. maddede belirlenen suçlar açısından bir filtreleme sistemi öngörebilir. Bunun dışında kalan suçlar ve suç oluşturmayan hukuka aykırı eylemler açısından TİB'in bir filtreleme sistemi öngörmesi Kanunen mümkün değildir.

Kanunun yaklaşımı bu şekilde olmakla birlikte erişimin engellenmesi kısmında da bahsedildiği gibi 8. maddede yer almayan terör suçları ve bomba yapım bilgisi verme gibi suçların kapsam dışında bırakılması yerinde bir yaklaşım olmamıştır.

TİB tarafından yapılacak filtreleme, 5651 sayılı Kanunun kapsam alanı açısından sadece internet ortamında yapılabileceğinden ve internet ortamı "*haberleşmeyi"* kapsamadığından internet üzerinden yapılan kişisel haberleşme niteliğindeki iletişimin filtrelenmesi, 5651 sayılı Kanuna göre mümkün değildir. Bu çerçevede örneğin, e-posta veya sosyal paylaşım siteleri üzerinden yapılan iletişim, filtrelemeye tabi tutulamaz.

---

[708] Dülger, **a.g.m**., s. 24-27.

3. Güvenli İnternet Hizmeti

BTK, 24.08.2011 tarihli ve 2011/DK-14/461 sayılı Kurul Kararı ile "*Güvenli internet Hizmetine İlişkin Usul ve Esasları"* kabul etmiş[709] ve güvenli internet hizmetini 22.11.2011 tarihinde uygulamaya geçirmiştir. Söz konusu düzenlemenin amacı, tercihe dayalı güvenli internet hizmetine ilişkin usul ve esasları düzenlemek olarak belirlenmiştir. Usul ve esaslara göre "*güvenli internet hizmeti",* abonelerin talebi üzerine, ücretsiz olarak sunulan çocuk ve aile profilinden oluşan hizmet; "*aile profili"*, BTK tarafından İşletmecilere gönderilen aile profiline ilişkin listedeki alan adı, alt alan adı, IP adresi ve portlara abonenin erişiminin sağlanmadığı profil; "*çocuk profili"* ise BTK tarafından İşletmecilere gönderilen, çocuk profiline ilişkin listedeki alan adı, alt alan adı, IP adresi ve portlara abonenin erişiminin sağlandığı profildir. Güvenli internet hizmetini talep etmeyen abonelerin mevcut internet erişim hizmeti, herhangi bir değişiklik olmaksızın sunulmaya devam edecektir.

Usul ve Esaslar ile çocuk ve aile profil listelerinin oluşturulmasına ilişkin kriterlerin belirlenmesinde BTK'ya yardımcı olacak bir çalışma kurulu (Çocuk ve Aile Profil Kriterleri Çalışma Kurulu) oluşturulmuştur. Söz konusu Kurul, BTK koordinasyonunda 11 üyeden oluşmakta; biri başkan olmak üzere BTK'dan 3, Aile ve Sosyal Politikalar Bakanlığından 2, İnternet Kurulunun sivil toplum temsilcisi üyelerinden 2, Türkiye Dijital Oyun Federasyonundan 1 ve psikoloji, pedagoji, sosyoloji, hukuk gibi ilişkili alanlarda uzmanlığı olan kişiler arasından BTK tarafından seçilen 3 üyenin katılımını gerektirmektedir. Kurulun tespit ettiği ilkeler çerçevesinde, çocuk ve aile profil listeleri BTK tarafından belirlenecektir.

Usul ve Esaslar ile başvuru ve itiraz usulü ayrıca düzenlenmiştir. Kullanıcılar ve internet sitesi sahipleri, internet sitelerinin değerlendirilmesi için BTK tarafından hazırlanan internet sayfası üzerinden Kuruma başvurabilir ve itiraz edebilir. Kullanıcılar, başvurularını Profil Düzenleme internet Sayfasında bulunan bağlantı ile, itirazlarını ise Uyarıcı ve Bilgilendirici internet Sayfasında bulunan bağlantı vasıtasıyla yapabilir. İlgili

[709] Usul ve esasların metni için bkz.
http://www.btk.gov.tr/mevzuat/kurul_kararlari/dosyalar/2011%20DK-14-461.pdf, 24.12.2012.

başvuru ve itiraza ilişkin İşletmeci adı, kullanıcı profili ile alan adı/IP adresi ve port bilgileri, başvuru ve itirazların doğru değerlendirilebilmesi için İşletmeciler tarafından Kuruma gönderilecektir. BTK, başvurular ve itirazların değerlendirilmesi için Çocuk ve Aile Profil Kriterleri Çalışma Kurulunun görüşüne başvurabilir.

Çocuk ve aile profillerinde kumar, intihara yönlendirme, çocukların cinsel istismarı, uyuşturucu ve uyarıcı madde veya sağlık için tehlikeli madde temini, fuhuş, müstehcenlik, ırkçılık, nefret, terör, şiddet, dolandırıcılık ve zararlı yazılım gibi içeriklere sahip siteler yer almamaktadır[710]. Oyun, sohbet ve sosyal medya siteleri çocuk profilinde yer almamakta; aile profilinde ise forum ve paylaşım sitelerine erişilebilmektedir[711]. Güvenli internet hizmetinde, internet sitelerinin alan adı taramasıyla hangi profilde yer aldığı sorgulanabilmekte ve siteler hakkında öneri getirebilme imkanı sunulmaktadır[712].

Güvenli internet hizmetinin yasal dayanaktan yoksun olup olmadığı tartışılabilir. Esasında güvenli internet hizmeti yasal dayanaktan yoksun değildir. Bu kararın dayanağını, devlete ailenin ve çocukların internetin getirmiş olduğu zararlı etkilerden korunması görevini veren Anayasal ve yasal hükümler oluşturmaktadır. Ayrıca, güvenli internet hizmeti, isteğe bağlı bir hizmettir. İsteğe bağlı bir hizmetin sunulmasında ise hukuki bir sorun ortaya çıkmaması gerekir.

Nihayet, 5809 sayılı Elektronik Haberleşme Kanununun amaçlarından biri "*tüketici haklarının gözetilmesi"* olarak belirlenmiş ve tüketici hakları ayrı bir bölüm altında düzenlenmiştir (md. 1 ve dördüncü kısım). BTK'nın görev ve yetkileri belirlenirken "*Abone, kullanıcı, tüketici ve son kullanıcıların hakları ile kişisel bilgilerin işlenmesi ve gizliliğinin korunmasına ilişkin gerekli düzenlemeleri ve denetlemeleri yapmak"* görev ve yetkisi de BTK'ya verilmiştir. Bu çerçevede BTK, 2010 yılında Elektronik Haberleşme

[710] http://www.tib.gov.tr/tr/dokumanlar/internetin_Guvenli_Kullanimi_Sosyal_Aglar_Sunumu.pdf, 12.10.2012.
[711] http://www.guvenlinet.org.tr/tr/menu/14-Profillerde_Neler_Var_.html, 12.10.2012.
[712] http://guvenlinet.org.tr/sorgula, 11.102012.

Sektöründe Tüketici Hakları Yönetmeliğini[713] yürürlüğe koymuştur. Yönetmeliğin 10. maddesine göre *"İşletmeciler, internetin 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 yükümlüdür. Kurum bu maddenin uygulanmasına ilişkin usul ve esaslar belirleyebilir".*

Diğer taraftan, Güvenli internet Hizmetine İlişkin Usul ve Esaslar, içeriği ve etkinliği itibariyle Resmi Gazete'de yayımlanması gereken bir düzenleyici işlem niteliğindedir. Örneğin, yapılan filtrelemeden dolayı hukuka uygun bir siteye erişimin engellenmesi durumunda, bu sitenin sahibinin kullanabileceği hukuksal imkanların belirlenmesi ve önceden herkese duyurulması hukuki güvenlik ilkesinin gereğidir. Bu belirleme ve duyurma işleminin Resmi Gazete'de yayımlanan bir düzenleyici işlem ile olması, Resmi Gazete'de yayımlanmayan bir karar ile olmasından çok daha güvencelidir.

D. İnternete Erişimin Kişisel Olarak Engellenmesi

İngiltere, ABD ve Avustralya gibi bazı ülkelerde çocuk pornografisini önlemek amacıyla, şüpheli durumda bulunan veya çocuk pornografisi suçu işlemiş veya şartlı salınmış kişilerin bir tedbir, suçun bir sonucu veya infaz şekli olarak internete erişiminin kişisel olarak engellenmesi yoluna başvurulabilmektedir[714]. Engelleme, internet ve internete erişim sağlayan her türlü donanıma sahip olmayı engelleme, bilgisayarlarına kurulacak yazılımlarla kişilerin izlenmesi ve yetkililere hukuksal olarak kişilerin bilgisayarlarına her an ulaşabilme ve kontrol edebilme gibi imkanlar tanınarak gerçekleştirilebilmektedir[715]. Bu şekilde devletler, belli suçların işlenmesinin önlenmesi ve kişilerin rehabilitasyonunun sağlanması amacıyla internete erişim hakkını kişisel olarak engelleyebilmektedir.

---

[713] RG. 28.07.2010, 27655.
[714] Gillespie, **a.g.m.**, s. 173.
[715] Gillespie, **a.g.m.**, s. 173.

TCK'da kısa süreli hapis cezasına seçenek yaptırımlar düzenlenmiş ve mahkum olunan cezanın yarısından bir katına kadar süreyle, belirli yerlere gitmekten veya belirli etkinlikleri yapmaktan yasaklanma, kısa süreli hapis cezasına seçenek bir yaptırım olarak öngörülmüştür. İnternet ortamında çocuk pornografisi ile mücadele amacıyla kısa süreli hapis cezaları, kişilerin internet kafeleri kullanmasının yasaklanması, internet aboneliklerinin engellenmesi veya bilgisayarlarına yerleştirilecek programlar ile internet iletişimlerinin takip edilmesi gibi hapis cezasına seçenek yaptırımlara dönüştürülebilmelidir.

Diğer taraftan, TCK'nın 53. maddesinde belli hakları kullanmaktan yoksun bırakılmaya ilişkin hususlar düzenlenmiş; ancak internete erişimin kişisel olarak engellenmesi, bir hak yoksunluğu olarak öngörülmemiştir. Böyle bir düzenleme yapılmasına ihtiyaç bulunmaktadır.

E. 5651 Sayılı Kanunun Genel Değerlendirmesi

Anayasamızın 41. maddesinde yer alan ailenin korunması ve 58. maddesinde yer alan gençliğin korunması hükümlerinin bir gereği olarak Türkiye'de internetin düzenlenmesi konusunda ilk esaslı düzenleme 2007 yılında yürürlüğe giren, 4/5/2007 tarihli ve 5651 sayılı internet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun[716] ile yapılmıştır[717]. Bu Kanun ile belli kişilere internet alanında bazı yükümlülük ve sorumluluklar yüklenmiştir. Kanunda bu kişiler içerik sağlayıcı (content provider), yer sağlayıcı (service provider), erişim sağlayıcı (access provider) ve toplu kullanım sağlayıcı olarak belirlenmiş ve bu kişiler tek tek tanımlamıştır (md. 2). Kanunun amacı

---

[716] RG. 23.5.2007, 26530.

[717] Kanun, bu çalışmada "*5651 sayılı Kanun"* şeklinde kısaltılarak kullanılmıştır. Kanunun genel gerekçesinde Anayasamızın 41. maddesinde yer alan ailenin ve çocukların korunmasına ilişkin hüküm ile 58. maddesinde yer alan gençliğin korunmasına ilişkin hükmün devlete, internette yer alan zararlı içerikle mücadele etme yetkisi verdiği belirtilmiştir. Genel gerekçede ayrıca, bu hükümler uyarınca aileyi, çocukları ve gençleri internet dahil elektronik iletişim araçlarının suiistimal edilmesi suretiyle uyuşturucu ve uyarıcı madde alışkanlığı, intihara yönlendirme, cinsel istismar, kumar ve benzeri kötü alışkanlıkları teşvik eden yayınların içeriklerinden korumak için gerekli önleyici tedbirlerin alınmasının amaçlandığı ifade edilmiştir. Bkz. http://www2.tbmm.gov.tr/d22/1/1-1305.pdf, 16.10.2012.

bu kişiler üzerinden, yani bu kişilere belli yükümlülük ve sorumluluklar yüklenerek, internet ortamında[718] işlenen suçlarla mücadele etmek olarak belirlenmiştir (md. 1)[719]. 5651 sayılı Kanunun yürürlüğe girmesinde önce birçok yazar internet ortamında yapılan yayınlar ve sorumluluk rejimi hakkında acilen yasal düzenlemeye ihtiyaç bulunduğunu ifade etmiştir.

Kanunun genel yaklaşımı internet alanında sorumluluk esaslarını belirleme şeklinde sübut bulmuştur. 5651 sayılı Kanun, interneti cezai, idari ve hukuksal sorumluluk açısından düzenleyen bir kanundur. Kanun ile cezai, idari ve hukuksal sorumluluğun internetteki aktörleri belirlenmiştir. Diğer taraftan, cezai sorumlulukla ilgili olarak internet servis sağlayıcılarını muhatap alan birkaç siber suç ve bir koruma tedbiri olarak erişimin engellenmesi tedbiri; idari sorumlulukla ilgili olarak bazı idari para cezaları ve bir idari tedbir olarak erişimin engellenmesi tedbiri; hukuksal sorumlulukla ilgili olarak ise kişilik haklarını ihlal eden içeriğin yayından çıkarılması ve cevap hakkı müessesesi düzenlenmiştir. Bu nedenle Kanunun ceza hukuku ile ilgili bir boyutu bulunduğu gibi, idare hukuku ve medeni hukuk ile ilgili bir boyutu da bulunmaktadır. Kanun, bu özelliğinden dolayı doktrinde kimi yazarlarca "*sui generis"* bir kanun olarak nitelendirilmiştir[720].

5651 sayılı Kanun özel bir ceza kanunu niteliği taşımamaktadır[721]. Kural olarak bu Kanun ile suç ve ceza tanımlaması yapılmamıştır[722]. Ancak, Kanun İçel'in de belirttiği gibi ceza sorumluluğunun belirlenmesinde yardımcı bir kaynak olarak değerlendirilebilir[723]. Örneğin, içerik sağlayıcı, erişim sağlayıcı ve yer sağlayıcı tanımlamaları kişilerin ceza sorumluluğunun

---

[718] Kanunda "*internet ortamı",* haberleşme ile kişisel veya kurumsal bilgisayar sistemleri dışında kalan ve kamuya açık olan internet üzerinde oluşturulan ortam olarak tanımlanmış; "*internet ortamında yapılan yayın"* ise internet ortamında yer alan ve içeriğine belirsiz sayıda kişilerin ulaşabileceği veri olarak tanımlanmıştır.

[719] 5651 sayılı Kanunun yürürlüğe girmesinde önce birçok yazar internet ortamında yapılan yayınlar ve sorumluluk rejimi hakkında acilen yasal düzenlemeye ihtiyaç bulunduğunu ifade etmiştir. Bu yönde bkz. İlkiz, **a.g.m.**, s. 446.

[720] Mehmet Bedii Kaya, **a.g.e.**, s. 85.

[721] İçel, **a.g.m.**, s. 19.

[722] Kanunun genel gerekçesinde, kanun ile yeni bilişim suçları kategorisi oluşturulmadığı ve suçlar işlendikten sonra devreye girecek cezai ve idari yaptırımlar getirilmediği belirtilmiştir. Bkz. http://www2.tbmm.gov.tr/d22/1/1-1305.pdf, 16.10.2012. Kural bu olmakla birlikte istisnai olarak birkaç cezai hüküm ve idari yaptırımlara ilişkin birçok hüküm anılan Kanunda yer almıştır.

[723] İçel, **a.g.m.**, s. 19.

belirlenmesinde göz önünde bulundurulması gereken önemli bir husustur ve bu tanımlamalar 5651 sayılı Kanun ile yapılmıştır.

5651 sayılı Kanun internete özgü sadece iki tane suç oluşturmuştur. Bunun dışında bu Kanun ile başka bir bilişim suçu öngörülmemiştir. Zaten bu Kanunun amacı bilişim suçlarını düzenlemek de değildir. 1. maddede Kanunun amacı, "*internet ortamında işlenen suçlarla içerik, yer ve erişim sağlayıcılar üzerinden mücadele"* olarak; bir diğer deyişle "*suç unsuru içeren internet siteleri ile mücadele"* olarak belirlenmiştir.

5651 sayılı Kanuna doktrinde birçok eleştiri yöneltilmektedir. Kanunun geneline yönelik olarak bir sansür yasası olduğu ve ifade hürriyetini Anayasaya aykırı bir şekilde sınırlandırdığı İleri sürülmektedir[724]. Bu görüşün karşısında yer alan görüş ise 5651 sayılı Kanunun internet alanında kişilerin sorumluluklarını belirlemesi ve erişimin engellemesi nedenlerini tek tek sayması ve sınırlandırması yönü ile demokratik açıdan ileri düzeyde bir kanun olduğunu savunmaktadır. Bu görüşü savunan yazarlar özellikle çoğu Batı ülkesinde erişimi engelleme nedenlerinin özel olarak ve sınırlı sayıda belirlenme yerine, genel kanun hükümlerine ve sınırsız nedenlere dayanılarak yapıldığını ileri sürmektedir[725].

Bizce de 5651 sayılı Kanun, bazı eksiklikler içermekle birlikte genel itibariyle ülkemiz açısından olumlu bir düzenleme olmuştur. Kanun hükümlerinin Avrupa Konseyi Siber Suç Sözleşmesi ve AB Direktifleri ile genel itibariyle uyumlu olduğu söylenebilir. Ayrıca Kanun, birçok hükmü açısından Alman Telehizmetler Kanunu ile paralellik göstermektedir.

---

[724] Akdeniz / Altıparmak, **a.g.e.**, s. 89.
[725] Kılınç, "Türk Hukukunda", s. 444.

SONUÇ

İnternetin toplum hayatına girmesi ile birlikte başlayan süreçte devletin internete yaklaşımı birçok tartışmayı beraberinde getirmiştir. Başlangıçta devlete karşı bir özgürlük alanı olarak ilan edilen internet, zamanla devletin yürürlüğe koyduğu hukuksal düzenlemelerin konusu haline gelmiş; özellikle kamu hukuku düzenlemeleri ile internet, devlet açısından ulusal bir nitelik kazanmıştır.

İnternetin ulusal nitelik kazanması, bilişim suçları ile mücadele, internet ortamında kişisel verilerin korunması, önleme amaçlı internet iletişiminin denetlenmesi ve ulusal siber güvenliğin sağlanması gibi haklı nedenlere dayanılarak yürürlüğe konulan kamu hukuku düzenlemeleri ile gerçekleştirilmiştir. Yürürlüğe konulan düzenlemelerin etkinlik gösterebilmesi için cezai, idari ve hukuksal sorumluluk araçları geliştirilmiştir. Bu süreç hızlanarak devam etmektedir. Gelecekte bilişim teknolojilerinin sunacağı yeni imkanlarla bu gelişimin daha da hızlanacağı söylenebilir.

Anılan nedenlerden birincisini bilişim suçları ile mücadele oluşturmaktadır. İnternet ortamında nefret söylemi, şiddet, çocuk pornografisi, dolandırıcılık, fikri mülkiyet haklarının ihlali ve terör propagandası gibi fiiller suç olarak öngörülmekte ve cezai yaptırım altına alınmaktadır. İkinci neden, internet ortamında kişisel verilerin korunmasıdır. AB'nin bu alanda yürürlüğe koyduğu direktifler, üye ülkelerin tamamının kişisel verilerin korunmasına yönelik özel düzenlemeler kabul etmesi sonucunu doğurmuştur. Söz konusu düzenlemeler ile internet ortamında kişisel verilerin işlenmesi sıkı koşullara bağlanmış ve kişiler açısından önemli hukuksal güvenceler öngörülmüştür. Bir diğer neden, önleme amaçlı internet iletişiminin denetlenmesidir. Suç işlenmesinin önlenmesi açısından uygulanan bu tedbir, belli şartlar altında toplum nezdinde de genel kabul görmektedir. Nihayet bu çalışmada ele alınan son neden, ulusal siber güvenliğin sağlanmasıdır. Yürürlüğe konulan ulusal siber güvenlik stratejileri ve oluşturulan siber güvenlik kurulları her geçen gün daha etkin yetkilerle donatılmaktadır. Bu nedenlerin sayısı artırılabilir.

Düzenleme yaklaşımı, beraberinde sorumluluğu da getirmektedir. Öngörülen cezai ve idari sorumluluk sistemi, devletin internete yaklaşımını göstermesi açısından önemlidir. Özellikle internet içeriğine erişimin engellenmesi ve filtreleme, düzenlemenin etkinlik kazanması açısından devletin her geçen gün artan bir şekilde başvurduğu hukuksal araçlar halinde gelmiştir.

Mevcut tablo karşısında küreselleşme süreci ile birlikte ulus-devlet egemenliğine meydan okuyan bir tarzda karşımıza çıkan internetin, artık bu özelliğini kaybetmeye başladığı söylenebilir. Ancak bu yargı, devletin internet içeriğini sınırsız bir şekilde düzenleyebileceği anlamına gelmemektedir. Bu noktada demokratik devlet; ifade özgürlüğü, haberleşme özgürlüğü, özel hayatın gizliliği, bilim ve sanat özgürlüğü gibi temel hak ve özgürlükleri güvence altına alma zorunluluğu ile karşı karşıya kalmaktadır.

Devletin internet ortamını düzenlemesi hassas bir denge gerektirmektedir. Bu dengenin iyi sağlanamadığı her durumda zarar gören temel hak ve özgürlükler olacaktır. Örneğin, ulusal siber güvenliğin sağlanmasına yönelik bir düzenleme, ifade özgürlüğünün sınırlandırılması açısından ağır hükümler içeriyorsa ifade özgürlüğünün; ulusal siber güvenliğin sağlanmasına yönelik yeterli güvenceler içermiyorsa yaşam hakkı veya güvenli bir toplumda yaşama hakkı gibi hak ve özgürlüklerin ihlali sonucunu doğurabilir.

Ülkemizde genel olarak internet içeriğinin düzenlemesine ilişkin her karar olumsuz değerlendirilmekte ve Devletin sansür uyguladığı ileri sürülmektedir. Aslında bu görüşün gerisinde, devletin hiçbir şekilde internete müdahale etmemesi gerektiği düşüncesi yatmaktadır. Ancak, artık günümüzde bu görüş etkinliğini kaybetmiştir. Her devlet interneti düzenlemektedir. Hatta, interneti düzenlemek ulus-devletin meşruiyetinin bir uzantısı kabul edilmektedir. Önem kazanan konu ise düzenlemenin içeriğine ilişkin hususlardır. Bu nedenle, her düzenleme açısından özel değerlendirme yapmak en doğru yol olacaktır.

İnternet ortamına ilişkin ülkemiz düzenlemeleri ile Avrupa ülkelerinin ve ABD'nin düzenlemeleri genel bir bakış açısı ile ele alındığında aslında

devletin internete yaklaşımının paralel bir seyir izlediği söylenebilir. Spesifik olarak düzenleme yaklaşımları açısından elbette farklılıklar bulunmaktadır. Ancak genel yaklaşım, internete ulusal bir karakter kazandırılması ve temel hak ve özgürlüklerin korunmasında hassas dengenin sağlanmasına yöneliktir. Bu çerçevede hassas bir dengenin kurulabilmesi için;

1. Devlet; bilişim suçları ile mücadele, internet ortamında kişisel verilerin korunması, önleme amaçlı internet iletişiminin denetlenmesi ve ulusal siber güvenliğin sağlanması gibi haklı nedenlerle internet içeriğini düzenlemelidir. Bu nedenlere dayanarak devletin düzenleme öngörmesi, temel hak ve özgürlüklerin güvence altına alınması açısından bir zorunluluktur.

2. Haklı nedenlere dayanılarak internet içeriğine erişim engellenebilmeli ve filtreleme uygulanabilmelidir. Ancak, haklı nedenler hukuksal bir temele dayanmalı, tek tek ve sınırlı sayıda belirlenmeli ve devlet sıkı şartlar altında erişimi engelleyebilmelidir. Bu çerçevede örneğin, hukuka ayıkırı içerikten dolayı internet sitelerinin tamamına erişim engellenmemeli, URL bazlı erişim engelleme yöntemi kullanılmalıdır. Aksi yaklaşım, ifade özgürlüğü ve haberleşme özgürlüğü gibi hak ve özgürlüklere ölçülü olmayan bir müdahale oluşturur.

3. Kural olarak internet içeriğine erişimin engellenmesi hakim kararı ile gerçekleştirilmeli; ancak özellikle yurt dışı kaynaklı zararlı içeriğin önlenmesi veya ülke kaynaklı olsa bile çocuk pornografisi veya terörizmle mücadele gibi nedenlere bağlı olarak ve sıkı şartlar altında idare tarafından da internet içeriğine erişim engellenebilmelidir. Birçok Avrupa ülkesinin uygulaması da bu yöndedir. Ancak, idareye böyle bir yetki tanınırken bu yetkinin çerçevesi çok iyi çizilmeli ve kişilere yeterli hukuksal güvenceler sağlanmalıdır. Bu noktada örneğin, ülkemizde TİB tarafından uygulanan resen erişimi engelleme yöntemi bir gerekliliği bünyesinde barındırmakla birlikte usul olarak bazı sakıncaları da bünyesinde barındırmaktadır. Bu sakıncalardan en önemlisi resen erişimi engelleme kararlarının bağımsız bir kurul tarafından verilmemesi ve kararların alınmasında kişilere yeterli hukuksal güvencelerin sağlanmamasıdır. Resen erişimi engelleme kararları bağımsız bir kurul

tarafından verilmeli ve kararların alınmasında savunma hakkı, gerekçe ilkesi, ve ölçülülük gibi idari usul ilkelerine uyulmalıdır.

4. Hukuka aykırı içerik taşıyan internet sitesi sorumluları hakkında bazı durumlarda internet içeriğine erişimin engellenmesi tedbiri yerine idari para cezası yaptırımının uygulanması söz konusu olabilir. Her durumda içerik hakkında doğrudan erişimi engelleme tedbiri uygulamak, bazen adil olmayan sonuçların ortaya çıkmasına neden olabilir. Çoğu durumunda idari para cezası, erişimin engellenmesi tedbirinden daha caydırıcı bir nitelik de taşıyabilir.

5. Erişimi engellenen siteler, engelleme gerekçesi ile birlikte açıklanmalıdır. Bu konuda şeffaflığın sağlanması, kişilerin kendilerini hukuksal güvence içerisinde hissetmesini sağlayacak, zararlı içerikle mücadeleye katkı verecek ve erişimi engelleme konusunda devlete karşı yapılan eleştirileri ortadan kaldıracaktır. Aynı esaslar filtreleme uygulamaları açısından da geçerlidir. Uygulanan filtreleme yöntemleri ve filtrelenen içerik şeffaf bir şekilde kamuoyu ile paylaşılmalıdır. Bu konuda Telekomünikasyon İletişim Başkanlığının uygulaması maalesef olumlu değerlendirilememektedir.

6. Çocuk pornografisini önlemek amacıyla, şüpheli durumda bulunan veya bu suçu işlemiş veya şartlı salınmış kişilerin bir tedbir, suçun bir sonucu veya infaz şekli olarak internete erişiminin kişisel olarak engellenmesine yönelik düzenlemeler yapılmalıdır.

7. Bomba yapım bilgisi sunma ve terörizm, erişimi engelleme ve filtreleme nedenleri arasına alınmalıdır. Önleme amaçlı internet iletişiminin denetiminde terörizmle etkin bir şekilde mücadele edilmelidir.

8. internet alan adlarının yönetimi, Amerikan hukuku ve yargı yetkisi çerçevesinde faaliyet gösteren ve özel bir Amerikan kuruluşu sayılan ICANN'dan alınmalı ve Uluslararası Telekomünikasyon Birliği'ne verilmelidir.

9. Birçok ülkede ulusal siber güvenlik kanunu çıkartılmış ve ulusal siber güvenlik stratejisi hazırlanmıştır. Ülkemizde de bu çerçevede bir strateji ve kanun ihtiyacı bulunmaktadır.

10. İnternet üzerinde devletin uluslararası yetkisi açısından uluslararası işbirliğine ihtiyaç duyulmaktadır. İnternet ortamında gerçekleşen

fiillerden dolayı her devletin uluslararası yetki iddiasında bulunması, çözümü imkansız sorunların ortaya çıkmasına neden olmaktadır. Özellikle etki ilkesi göz önünde bulundurularak internet ortamında bizzat devletin veya vatandaşlarının menfaatinin ihlal edilmesi durumunda devlete uluslararası yetki iddiasında bulunma imkanı tanınmalıdır. Öte yandan, çocuk pornografisi veya terörizm gibi bazı fiilerin işlenmesi, evrensellik ilkesi gereği her devlet tarafından cezalandırılabilmelidir.

11. Devlet internet ortamını düzenlerken ceza hukuku kurallarına son çare olarak başvurmalıdır. Bu noltada özellikle internet servis sağlayıcılar açısından cezai sorumluluk yerine, idari sorumluluk sistemi geliştirilmelidir.

12. Arama motorları ve Web 2.0 teknolojisini kullanan interaktif internet sitesi sorumlularının, hukuksal statüsü ve sorumluluk rejimi ayrıca düzenlenmeli ve bunların başkalarına ait içeriği sırf yayınlamasından dolayı cezai veya idari sorumluluğuna gidilmemelidir. Bunlar sadece, yetkili makamlar tarafından alınmış hukuka aykırı içeriğe erişimi engellememeleri durumunda sorumlu tutulmalı ve bu sorumluluk cezai değil; idari sorumluluk olmalıdır.

13. Çocuk pornografisi suçu, evrensellik ilkesi gereği her devlet tarafından cezalandırılabilmeli ve bunun için uluslararası işbirliği geliştirilmelidir.

14. Kişisel verilerin korunmasına yönelik özel düzenlemeler yapılmalıdır. Genel nitelikli bir kişisel verilerin korunması kanunu bazen hassas kişisel verilerin korunması açısından yeterli hukuksal güvenceyi oluşturmayabilir. Sağlık verisi gibi hassas kişisel verilerin gerektiği gibi korunabilmesi için hassas veri alanlarında özel düzenlemeler yapılmalıdır.

15. Bilgi ve iletişim teknolojilerindeki hızlı gelişme, devlet tarafından yürürlüğe konulan hukuksal düzenlemelerde kısa zamanda değişlik ihtiyacı ortaya çıkarabilmektedir. Kanun düzeyinde yürürlüğe konulan düzenlemelerin kolay bir şekilde değiştirilememesi gerçekliğini de göz önünde bulundurarak, internet ortamına yönelik düzenlemelerde esnek bir düzenleme yöntemi benimsenmeli ve bu çerçevede idarenin düzenleyici işlemleri ile internet ortamını düzenlemesine gereken önem verilmelidir. Ancak bu yapılırken

özellikle temel hak ve özgürlükleri güvence altına alan düzenlemelere kanunlarda yer verilmeli; teknik ve uygulamaya yönelik hususlar düzenleyici işlemlerle düzenlenmelidir. Örneğin, telekomünikasyon sektöründe kişisel verilerin korunmasına yönelik yeterli hukuksal güvenceler kanun ile sağlandıktan sonra Telekomünikasyon Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğin Korunması Hakkında Yönetmelik yürürlüğe konulmalıdır. Yine, ulusal süber güvenliğin sağlanması ile yetkili kılınan Siber Güvenlik Kurulu, temel hak ve özgürlükler açısından yeterli bir hukuksal güvence kanun ile sağlandıktan sonra Bakanlar Kurulu kararı ile oluşturulmalıdır.

16. Günümüzde organize suç örgütleri ve terörizmle mücadele açısından internet iletişiminin önleme amaçlı denetlenmesi zorunlu hale gelmiştir. Bu nedenle internet iletişimi önleme amaçlı olarak etkin bir şekilde denetlenebilmelidir. Ancak, bu yapılırken etkin bir şekilde özel hayatın gizliliği ve haberleşme özgürlüğünü güvence altına alan hukuksal düzenlemeler de yürürlüğe konulmalı; bu güvenceler uygulamada hayata geçirilmelidir.

KAYNAKÇA

AKDENİZ, Yaman, ALTIPARMAK, Kerem; **İnternet: Girilmesi Tehlikeli ve Yasaktır Türkiye'de İnternet İçerik Düzenlemesi ve Sansüre İlişkin Eleştirel Bir Değerlendirme**, İmaj Yayınevi, Ankara, Kasım 2008.

AKDENİZLİ, Banu; "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, 26.11.2012, s. 31-51.

AKILLIOĞLU, Tekin; "İdari Usul ve Kişisel Verilerin Korunması", http://www.idare.gen.tr/akillioglu-idariusul.htm, 05.09.2012.

AKYILMAZ, Bahtiyar, SEZGİNER, Murat, KAYA, Cemil; **Türk İdare Hukuku**, 2. Güncellenmiş Baskı, Seçkin Yayınları, Ankara, 2011.

ALKAN, Mustafa, CANBAY, Cafer; "İnternet Alan Adları Yönetimi, Mevcut Sorunlar ve Çözüm Önerileri", http://www.tk.gov.tr/kutuphane_ve_veribankasi/raporlar/arastirma_raporlari/dosyalar/WEB_DE_YAYINLANAN_RAPOR.pdf, 06.09.2012, s. 1-24.

ATAY, Ender Ethem; **İdare Hukuku**, 3. Bası, Turhan Kitabevi, Ankara, 2012.

AVŞAR, B. Zakir, ÖNGÖREN, Gürsel; **İnternet Hukuku**, Türkiye Odalar ve Borsalar Birliği, Mart 2009.

BAUMER, David L.; EARP, Julia B.; POINDEXTER, J.C.; "Internet Privacy Law: A Comparison Between the United States and the European Union", **Computers & Security**, 23, 2004, s. 400-412.

BERNSTORFF, Jochen von; "Democratic Global Internet Regulation? Governance Networks, International Law and the Shadow of Hegemony", **European Law Journal**, Vol. 9, No. 4, September 2003, s. 511-526.

BİLGİ GÜVENLİĞİ DERNEĞİ, **Ulusal Siber Güvenlik Stratejisi**, Haziran 2012, http://www.bilgiguvenligi.org.tr/index_files/pdf/Ulusal_Siber_Guvenlik_Strateji si.pdf, 27.11.2012.

BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU; **Faaliyet Raporu 2011**, http://www.tk.gov.tr/kutuphane_ve_veribankasi/raporlar/faaliyet_raporlari/index.php, 05.10.2012.

DEVLET PLANLAMA TEŞKİLATI; **Bilgi Toplumu Stratejisi Eylem Planı (2006-2010) Değerlendirme Raporu Rapor No: 5**, http://www.bilgitoplumustratejisi.org/tr/doc/8a3247663bd29634013bdda974630002, 28.01.2012.

BOZBEL, Savaş; "5651 Sayılı Kanuna İstinaden Bazı İnternet Sitelerine Erişimin Engellenmesi Tedbirlerine Eleştirel Bir Yaklaşım", **e-Akademi**, Sayı 72, Şubat 2008, http://www.e-akademi.org/makaleler/sbozbel-5.htm, 10.04.2013, s. 1-10.

BREINDL, Yana, WRIGHT, Joss; "Internet Filtering Trends in Western Liberal Democracies: French and German Regulatory Debates", http://www.academia.edu/2870660/internet_Filtering_Trends_in_Western_Liberal_Democracies_French_and_German_Regulatory_Debates, 15.03.2013, s. 1-8.

BROWN, Ian; "Communications Data Retention in an Evolving Internet", **International Journal of Law and Information Technology**, Vol. 19, No. 2, Oxford University Press, 2010, s. 95-109.

CANDAN, Menderes, HUNGER, Uwe; "Nation Building Online: A Case Study of Kurdish Migrants in Germany", **German Policy Studies**, Volume Four, Number 4, 2008, s. 125-153.

CAREY, Peter; **Data Protection A Practical Guide to UK and EU Law**, Third Edition, Oxford University Press, 2009.

CHADWICK, Andrew; **Internet Politics States, Citizens, and New Communication Technologies**, Oxford University Press, New York, Oxford, 2006.

COHEN, Aviv; "Cyberterrorism: Are We Legally Ready?", **The Journal of International Business & Law**, http://law.hofstra.edu/pdf/academics/journals/jibl/jibl_vol9no1_cohen_cyberterrorism.pdf, 2010, s. 1-40.

CRADDOCK, Peter A.; **Legal Implications of Internet Filtering**,

http://www.arpia.be/public/PACraddock%20-%20Legal%20Implications%20of%20internet%20Filtering.pdf, 19.03.2013.

CZOSSEK, Christian, OTTİS, Rain and TALIHARM, Anna-Maria; "Estonia After the 2007 Cyber Attacks: Legal, Strategic and Organisational Cahnges in Cyber Security",
http://www.securitydefenceagenda.org/Contentnavigation/CyberInitiative/Cyberreferencelibrary/tabid/1333/Default.aspx, 10.04.2013, s. 57-64.

ÇAĞLAYAN, Ramazan; **İdari Yaptırımlar Hukuku**, Asil Yayın Dağıtım, 1. Baskı, Ankara, 2006.

ÇAKMAK, Münci; "İdare Hukuku ve İnternet", **GÜHFD**, Cilt, IX, Sayı. I-II, Haziran-Aralık 2005, http://webftp.gazi.edu.tr/hukuk/dergi/9_12.pdf, 02.10.2012.

ÇEÇEN, Anıl; **İnsan Hakları**, Savaş Yayınevi, Genişletilmiş 3. Basım, Ankara, 2000.

ÇİMEN, Ali; **Echelon İstihbarat Dünyasının Perde Arkası**, Timaş Yayınları, 5. Baskı, İstanbul, 2006.

DEIBERT, Ronald J.; "Deep Probe: The Evolution of Network Intelligence", **Intelligence and National Security**, Vol. 18, No. 4, 2003, s. 175-193.

DEIBERT, Ronald, ROHOZINSKI, Rafal; "Liberation vs. Control: The Future of Cyberspace", **Journal of Democracy**, Volume 21, Number 4, 2010, s. 43-57.

DEMİREL, Demokaan; "e-Devlet ve Dünya Örnekleri", **Sayıştay Dergisi**, Sayı: 61, Nisan-Haziran 2006, s. 83-118.

DENNING, Dorothy E.; "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy", **Networks and Netwars: The Future of Terror, Crime, and Militancy**,
http://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1382/MR1382.ch8.pdf, 04.12.2012, s. 239-288.

DOLGUN, Uğur; "İnternet ve Demokrasi",
http://www.journals.istanbul.edu.tr/tr/index.php/iktisatsosyoloji/article/viewFile/11379/10639, 27.01.2013, s. 221-236.

DUDNEY, Robert S.; "Rise of the Cyber Militias", **Air Force Magazine**, 2011,

http://www.airforce-magazine.com/MagazineArchive/Documents/2011/February%202011/0211cyber.pdf, 06.12.2012, s. 88-89.

DURNAGÖL, Yasemin; "5651 Sayılı Kanun Kapsamında İnternet Aktörlerine Getirilen Yükümlülükler ile İdari ve Cezai Yaptırımlar", **TAAD**, Cilt. 2, Yıl. 2, Sayı. 4, 20 Ocak 2011, s. 375-416.

DÜLGER, Murat Volkan; "İnternet İletişiminin Engellenmesinin Hukuki Açıdan Değerlendirilmesi ve 5651 Sayılı Yasayla Getirilen Düzenleme", **İstanbul Barosu Dergisi**, Cilt. 81, Sayı. 2007/4, 2007, http://www.dulger.av.tr/assets/pdf/interneterisimininengellenmesi.pdf, 14.12.2012, s. 1-57.

DÜLGER, Murat Volkan, BECENİ, Yasin; **Türkiye'de İnternet Sitelerinin Erişiminin Engellenmesi Konusunda Farklı Hukuk Disiplinleri Açısından Değerlendirmeler**, Yayın No: TÜSİAD-T/2011, 03; 512, Mart 2011.

ERDOĞAN, Mustafa; **İnsan Hakları Teorisi ve Hukuku**, Genişletilmiş 2. Baskı, Orion Kitabevi, Ankara, 2011.

ERKUT, Celal; **İptal Davasının Konusunu Oluşturma Bakımından İdari İşlemin Kimliği**, Danıştay Yayınları, Ankara, 1990.

FARIS, Robert, ZITTRAIN, Jonathan; "Web Tactics", **Index on Censorship**, http://ioc.sagepub.com/content/38/4/90, 18.03.2013, s. 90-96.

GEDİK, Ömer; **Türk Yargı Kararları Çerçevesinde Türkiye'de Kitle İletişim Özgürlüğü**, Seçkin Yayınları, Ankara, 2008.

GILLESPIE, Alisdair A.; "Restricting Access To The Internet By Sex Offenders**", International Journal of Law and Information Technology**, Oxford University Press, Vol. 19, No. 3, 2011, s. 165-186.

GOLDSMITH, Jack, WU; Tim; **Who Controls the Internet? Illusions of a Borderless World**, Oxford University Press, 2006.

GÖLCÜKLÜ, Feyyaz; "İdari Ceza Hukuku ve Anlamı; İdarenin Cezai Müeyyide Tatbiki", **AÜSBFD**, Cilt. 18, Sayı. 2, 1963, s. 115-182.

GÖZÜBÜYÜK, Şeref; **Yönetsel Yargı**, 30. Bası, Turhan Kitabevi, Ankara, 2010.

GÜNAYDIN, Barış; **İnternet Yayıncılığı ve İfade Özgürlüğü**, Adalet Yayınevi, Ankara 2010.

GÜNDAY, Metin; **İdare Hukuku**, İmaj Yayıncılık, Ankara, 2011.

GÜRKAYNAK, Gönenç, YILDIZ, İlay, KARA, Pınar; "Türk İnternet Hukuku Uygulamasının ve Mevzuatının Evriminin İlk Dönemini Tamamlaması İçin Öneriler ve Gözlemler", http://www.elig.com/docs/Turk_internet_Hukuku_Uygulamasinin_ve_Mevzuatinin_Evriminin_Ilk_Donemini_Tamamlamasi_Icin_Oneriler_ve_Gozlemler.pdf , 10.04.2013, s. 1-12.

GÜRKAYNAK, Muharrem, İREN, Adem Ali; "Reel Dünyada Sanal Açmaz: Siber Alanda Uluslararası İlişkiler", **Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi**, C. 16, S. 2, 2011, s. 263-279.

HENN, Julie, L.; "Targeting Transnational Internet Content Regulation", **Boston University International Law Journal**, Vol. 21: 157, 2003, s. 157-177.

HENRY, Jamal; **Reducing the Threat of State-to-State Cyber Attack Against Critical Infrastructure Through International Norms and Agreements**, CISSM Working Paper, 2010.

HERZOG, Stephen; "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses", **Journal of Strategic Security**, Volume IV, Issue 2, 2011, s. 49-60.

HOEREN, Thomas; "Liability for Online Services in Germany", **German Law Journal**, Vol. 10, No. 05, s. 561-584.

IŞIKLI, Hasibe; **İnternet Alan İsimleri Sistemi Markalar ve Alan İsimleri Arasındaki İlişki**, http://ekutup.dpt.gov.tr/, Şubat 2001.

İÇEL, Kayıhan; "Türkiye'de İnternet Ortamında İşlenen Suçlardan ve Kabahatlerden Sorumluluğun Genel Esasları – Erişimin Engellenmesi – İçeriğin Yayından Çıkarılması ve Cevap Hakkı", **İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi,** Yıl: 8, Sayı: 16, Güz 2009, s. 17-28.

İÇEL, Kayıhan, ÜNVER, Yener; **Kitle İletişim Hukuku**, Yeniden İncelenmiş 9. Bası, Beta Yayınları, İstanbul, 2012.

İLKİZ, Fikret; "İnternet Ortamında Yayınlar", **İnternet ve Hukuk**, Derleyen: Yeşim M. Atamer, İstanbul Bilgi Üniversitesi Yayınları, İstanbul, 2004, s. 433-490.

İNCE, N. Murat; **Elektronik Devlet Kamu Hizmetlerinin Sunulmasında Yeni İmkanlar**, Devlet Planlama Teşkilatı Yayınları, Ankara, Mayıs 2001.

KARAHANOĞULLARI, Onur; **İdarenin Hukukla Kavranması: Yasallık ve İdari İşlemler**, Turhan Kitabevi, Ankara, 2011.

KAYA, Mehmet Bedii; **Teknik ve Hukuki Boyutlarıyla İnternete Erişimin Engellenmesi**, XII Levha, 1. Baskı, İstanbul, Şubat 2010.

KAYA, Cemil; "Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi", **İÜHFM**, C. LXIX, S. 1-2, 2011, s. 317-334.

KETİZMEN, Muammer; **Türk Ceza Hukukunda Bilişim Suçları**, Adalet Yayınevi, Ankara, 2008.

KETİZMEN, Muammer, ÜLKÜDERNER, Çağlar; "e-Devlet Uygulamalarında Kişisel Verilerin Korun(ma)ması", **XII. "Türkiye'de İnternet" Konferansı**, Ankara, 8-10 Kasım 2007, s. 189-193.

KILINÇ, Doğan; "Anayasal Bir Hak Olarak Kişisel Verilerin Korunması", **AÜHFD**, 61 (3), 2012, s. 1089-1169.

KILINÇ, Doğan; "Türk Hukukunda ve Mukayeseli Hukukta İnternet Sitelerine Erişimin Engellenmesi ve İfade Hürriyeti", **GÜHFD**, C. XIV, S. 2, 2010, s. 407-454.

KUNER, Christopher; "Data Protection Law and International Jurisdiction on the Internet (Part 1)", **International Journal of Law and Information Technology**, Oxford University Press, Vol. 18, No. 2, 2010, s. 176-193.

KURU, Baki, ARSLAN, Ramazan, YILMAZ, Ejder; **Medeni Usul Hukuku**, Yetkin Yayınları, 22. Baskı, Ankara, 2011.

KÜZECİ, Elif; **Kişisel Verilerin Korunması**, Turhan Kitabevi, Ankara, 2010.

LYON, David; **Elektronik Göz Gözetim Toplumunun Yükselişi**, Çev. Dilek Hattatoğlu, Sarmal Yayınevi, İstanbul, 1997.

LYON, David; **Surveillance After September 11**, Polity Press, 2004.

MAIER, Bernhard; "How Has The Law Attempted to Tackle The Borderless Nature of The Internet?", **International Journal of Law and Information Technology**, Vol. 18, No. 2, Oxford University Press, 2010, s. 142-175.

MARSOOF, Althaf; "Online Social Networking and The Right to Privacy: The Conflicting Rights of Privacy and Expression", **International Journal of Law**

and Information Technology, Oxford University Press, Vol. 19, No. 2, 2011, s. 110-132.

MAYER, Franz C.; "Europe and The Internet: The Old World and The New Medium", **EJIL**, Vol. 11, No. 1, 2000, s. 149-169.

MAYER-SCHONBERGER, Viktor; "The Shape of Governance: Analyzing the World of Internet Regulation", **Virginia Journal of International Law**, Vol. 43, 2003, s. 605-673.

MCINTYRE, TJ, SCOTT, Colin; "Internet Filtering: Rhetoric, Legitimacy, Accountability and Responsibility", http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1103030, 18.03.2013, s. 1-15.

MEDYA DERNEĞİ; **Türkiye'nin İnternet Sansürü Sorunu**, Redaksiyon ve Güncelleme: Aslı Telli Aydemir, Temmuz 2010.

MEMİŞ, Tekin; "Erişimin Engellenmesi, Hukuki Sorunlar ve Çözüm Önerileri", **EÜHFD**, C. XIII, S. 3-4, 2009, s. 161-176.

MERAN, Necati; **Adli ve Önleme Amaçlı İletişimin Denetlenmesi**, Adalet Yayınevi, Ankara, 2009.

NAZARIO, Jose; "Politically Motivated Denial of Service Attacks", http://static.ow.ly/docs/12_NAZARIO%20Politically%20Motivated%20DDoS_iWO.pdf, s. 1-20.

NISSENBAUM, Helen; "Where Computer Security Meets National Security", **Ethics and Information Technology**, 7, 2005, s. 61-73.

NOMAN, Helmi; **In The Name of God: Faith-Based Internet Censorship In Majority Muslim Countries**, Opennet Initiative, August 2011.

OĞURLU, Yücel; **İdari Yaptırımlar Karşısında Yargısal Korunma**, Seçkin Yayınevi, Ankara, 2000.

OĞURLU, Yücel; **Karşılaştırmalı İdare Hukukunda Ölçülülük İlkesi**, Seçkin Yayınları, Ankara, 2002.

OPENNET INITIATIVE; **A Starting Point: Legal Implications of Internet Filtering**, 2004, http://www.opennetinitiative.org, 09.10.2012.

ÖZBEK, Veli Özer; "İnternet Kullanımında Ortaya Çıkabilecek Bazı Ceza Hukuku Sorunları", **DEÜHFD**, C. 4, S. 1, 2002, s. 101-158.

ÖZBUDUN, Ergun; **Türk Anayasa Hukuku**, Gözden Geçirilmiş 12. Baskı, Yetkin Yayınları, Ankara, 2011.

ÖZCAN, Mehmet; "Siber Terörizm ve Ulusal Güvenliğe Tehdit Oluşturma Boyutu", http://www.ozhankalac.info/dokumanlar/siber.pdf, 06.12.2012, s. 1-24.

ÖZEN, Muharrem, BAŞTÜRK, İhsan; **Temel Hak ve Özgürlükler Bağlamında Bilişim – İnternet ve Ceza Hukuku**, Adalet Yayınevi, Ankara, 2011.

ÖZTÜRK, Burak; **Fransız ve Türk Hukukunda İdarenin Düzenleme Yetkisinin Kapsamı**, Yetkin Yayınları, Ankara, 2009.

PAZARCI, Hüseyin; **Uluslararası Hukuk**, 10. Bası, Turhan Kitabevi, Ankara, 2011.

PLANT, Robert; "Online Communities", **Technology in Society**, 26, 2004, s. 51-65.

ROSENBERG, R. S.; "Controlling Access to the Internet: The Role of Filtering", **Ethics and Information Technology** 3 (1), 2001, s. 35 – 54.

SCHULTZ, Thomas; "Carving up the Internet: Jurisdiction, Legal Orders, and the Private/Public International Law Interface", **EJIL**, Vol. 19, No. 4, 2008, s. 799-839.

SEGURA-SERRANO, Antonio; "Internet Regulation and the Role of International Law", **Max Planck Yearbook of United Nations Law**, Volume 10, 2006, s. 191-272.

SOYSAL, Tamer; "İnternet Alan Adları Sistemi ve Tahkim Kuruluşlarının UDRP Kurallarına Göre Verdikleri Kararlara Eleştirel Bir Yaklaşım – 1", **Erciyes Üniversitesi Sosyal Bilimler Enstitüsü Dergisi**, Sayı: 21, 2006, s. 481-507.

SOYSAL, Tamer; "İnternet Servis Sağlayıcılarının Hukuki Sorumlulukları", **TBB Dergisi**, Sayı. 61, 2005, s. 304-339.

SPINDLER, Gerald; **Study on The Liability of Internet Intermediaries**, 2007, http://ec.europa.eu/internal_market/e-commerce/docs/study/liability/final_report_en.pdf, 23.10.2012.

SVANTESSON, Dan; “A Legal Method for Solving Issues of Internet Regulation”, **International Journal of Law and Information Technology,** Vol. 19, No. 3, Oxford University Press, 2011, s. 243-263.

ŞAHİN, Ali, TEMİZEL, Handan, TEMİZEL, Metehan; “Türkiye’de Demokrasiden e-Demokrasiye Geçiş Süreci ve Karşılaşılan Sorunlar”, www.siyasaliletişim.org/pdf/edemokrasiyegecis.pdf, 08.01.2013, s. 253-262.

ŞİMŞEK, Oğuz; **Anayasa Hukukunda Kişisel Verilerin Korunması**, Beta, 1. Baskı, İstanbul, Şubat 2008.

TAN, Turgut; **İdare Hukuku**, Turhan Kitabevi, Ankara, 2011.

TANGÖR, Burak, SAYIN, Sevinç; “Avrupa Birliği’nin Terörizmle Mücadele Stratejisi: Yeni Bir Bütünleşme Alanı mı?”, **Ankara Avrupa Çalışmaları Dergisi**, Cilt: 11, No: 1, 2012, s. 85-118.

TANŞU, Okan; “Bilişim Çağı, Yeni Tanımlamalar ve Hukuki Düzenlemeler”, **İnternet ve Hukuk**, Derleyen: Yeşim M. Atamer, İstanbul Bilgi Üniversitesi Yayınları, İstanbul, 2004, s. 139-154.

TAŞKIN, Mustafa; **Adli ve İstihbari Amaçlı İletişimin Denetlenmesi**, Seçkin Yayınları, Ankara, 2008.

TEZCAN, Durmuş ve Diğerleri; **İnsan Hakları El Kitabı**, Seçkin Yayınları, Genişletilmiş 3. Baskı, Ankara, 2010.

TEZCAN, Durmuş, ERDEM, Mustafa Ruhan, ÖNOK, R. Murat; **Uluslararası Ceza Hukuku**, Seçkin Yayınları, Ankara, 2009.

THEOHARY, Catherine A., ROLLINS, John; **Terrorist Use of the Internet: Information Operations in Cyberspace**, Congressional Research Service Report for Congress, March 2011.

TIIRMAA-KLAAR, Heli; “Cyber Security Threats and Responses at Global, Nation-State, Industry and Individual Levels”, Mart 2011, http://www.sciencespo.fr/ceri/sites/sciencespo.fr.ceri/files/art_htk.pdf, s. 1-10.

TOROSLU, Nevzat, FEYZİOĞLU, Metin; **Ceza Muhakemesi Hukuku**, Savaş Yayınları, Ankara, 2009.

TUNÇ, Hasan, BİLİR, Faruk, YAVUZ, Bülent; **Türk Anayasa Hukuku**, 3. Baskı, Berikan Yayınevi, Ankara, 2011.

TÜRKİYE BİLİŞİM DERNEĞİ; **e-Devlet Üst Yapısı Nihai Rapor**, http://www.tbd.org.tr/usr_img/cd/kamubib14/raporlarPDF/RP1-2011.pdf, 29.01.2012.

UÇKAN, Özgür; **e-Devlet, e-Demokrasi ve Türkiye**, Literatür Yayınları: 95, 1. Basım, İstanbul, Nisan 2003.

UÇKAN, Özgür, BECENİ, Yasin; "Bilişim-İletişim Teknolojileri ve Ceza Hukuku", **İnternet ve Hukuk**, Derleyen: Yeşim M. Atamer, İstanbul Bilgi Üniversitesi Yayınları, İstanbul, 2004, s. 363-430.

ULUSOY, Ali; "İdari Ceza Hukuku'nun İşlevi ve Hukuk Düzeni İçindeki Yeri", **İdari Ceza Hukuku Sempozyumu**, Editörler: İlhan Ulusan / Funda Başaran Yavaşlar, TC İstanbul Kültür Üniversitesi, Seçkin Yayınları, Ankara, 2009.

UNITED NATIONS; **e-Government Survey 2012**, New York, 2012, http://unpan1.un.org/intradoc/groups/public/documents/un/unpan048065.pdf, 19.12.2012.

ÜNVER, Mustafa, CANBAY, Cafer, ÖZKAN, Hüseyin Burhan; **Kritik Altyapıların Korunması**, BTK, Ankara, Mayıs 2010.

WALKER, Clive; "Cyber-Terrorism: Legal Principle and Law in the United Kingdom", **Penn State Law Review**, Vol. 110: 3, s. 625-665.

WECKERT, John; "What Is So Bad About Internet Content Regulation", **Ethics and Information Technology** 2, Kluwer Academic Publishers, 2000, s. 105-111.

WEISER, Philip J.; "Internet Governance, Standard Setting and Self-Regulation", **Northern Kentucky Law Review**, Vol. 28: 4, s, 822-846.

WILSKE, Stephan, SCHILLER, Teresa; "International Jurisdiction in Cyberspace: Which States May Regulate the Internet?", **Federal Communications Law Journal**, Vol. 50, Iss. 1, 1997, s. 117-178.

WILSON, Clay; **Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress**, CRS Report for Congress, January 2008.

WIMMER, Kurt, POGORILER, Eve, SATTERFIELD, Stephen; "International Jurisdiction and the Internet in the Age of Cloud Computing", http://www.cov.com, 05.03.2013, s.1-15.

YILDIZ, Sevil; **Suçta Araç Olarak İnternetin Teknik ve Hukuki Yönden İncelenmesi**, Nobel Yayın Dağıtım, Ankara, 2007.

YOKUŞ SEVÜK, Handan; "Kolluk Tarafından Suçun Önlenmesine Yönelik Yapılan İletişimin Denetlenmesine İlişkin Değerlendirmeler", **TBB Dergisi**, Sayı: 67, 2006, s. 41-56.

YÜKSEL CİVELEK, Dilek; **Kişisel Verilerin Korunması ve Bir Kurumsal Yapılanma Önerisi (Uzmanlık Tezi)**, Devlet Planlama Teşkilatı Müsteşarlığı, Yayın No: 2821, Ankara, Nisan 2011.

YÜKSEL, Saadet; **Özel Yaşamın Bir Parçası Olarak Telekomünikasyon Yoluyla Yapılan İletişimin Gizliliğine Önleyici Denetimle Müdahale**, Beta, İstanbul, 2012.

İNTERNET KAYNAKLARI

http://www.un.org/terrorism/instruments.shtml, 10.04.2013.

http://www.internetworldstats.com/stats.htm, 28.12.2012.

http://www.iana.org/numbers, 28.01.2012.

http://www.icann.org/en/about/agreements/mou-jpa/icann-mou-25nov98-en.htm, 27.01.2013.

http://www.icann.org/en/about/governance/bylaws/bylaws-16mar12-en.htm, 27.01.2013.

http://www.icann.org/en/groups/chart, 27.01.2013.

http://www.icann.org/en/about/welcome, 06.09.2012.

http://www.icann.org/en/about/governance/bylaws, 27.01.2013.

http://www.icann.org/registrar-reports/accredited-list.html, 27.01.2013.

http://www.bilgitoplumustratejisi.org/tr/node/hakkimizda, 28.01.2013.

http://www.internetworldstats.com/stats.htm, 28.12.2012.

http://www.internetworldstats.com/top20.htm, 28.12.2012.

http://www.internetworldstats.com/stats.htm, 28.12.2012.

http://www.internetworldstats.com/top25.htm, 28.12.2012.

http://www.internetworldstats.com/stats7.htm, 28.12.2012.

http://www.sms.uyap.gov.tr/, 28.01.2013.

https://www.turkiye.gov.tr/hizmetler, 28.01.2013.

http://www.cio.noaa.gov/itmanagement/egovact.pdf, 19.12.2012.
http://www.epractice.eu/files/media/media_928.pdf, 19.12.2012.
http://www.epractice.eu/en/document/288279, 19.12.2012.
http://www.epractice.eu/files/eGovernmentFrance.pdf, 19.12.2012.
http://www.epractice.eu/files/eGovernmentSpain.pdf, 19.12.2012.
http://www.gelisim.org/makaleler/e-devlet.doc, 19.12.2012.
http://akgul.bilkent.edu.tr/e-devlet/taslak.pdf, 19.12.2012.
http://www.mevzuat.gov.tr/Kanunlar.aspx, 16.10.2012.
http://www.alexa.com/topsites/countries/TR, 21.12.2012.
http://www.alexa.com/topsites, 21.12.2012.
http://www.alexa.com/topsites/countries;0/TR, 21.12.2012.
http://www.memurlar.net/haber/290958/, 03.10.2012.
http://www.socialbakers.com/facebook-statistics/?interval=last-6-months
#chart-intervals, 21.12.2012.
http://www.google.com/zeitgeist/2012/#turkey/searches, 24.12.2012.
http://www.google.com/zeitgeist/2012/#the-world/searches, 24.12.2012.
http://www.socialbakers.com/twitter/group/politics/, 21.12.2012.
http://www.mevzuat.adalet.gov.tr/html/844.html, 22.02.2013.
http://www.youtube.com/watch?v=8EnUzdkL_WU, 19.07.2012.
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:012:0001:
0023:en:PDF, 11.09.2012.
http://www.youtube.com/watch?v=DqdtEyLQKf4, 03.10.2012.
http://www.meb.gov.tr/belirligunler/insan_haklari/bildirge.htm, 2.1.2013.
http://www.un.org/en/documents/udhr/, 2.1.2013.
http://www.tbmm.gov.tr/komisyon/insanhaklari/pdf01/53-73.pdf, 2.1.2013.
http://www2.ohchr.org/english/law/ccpr.htm, 2.1.2013.
http://www.anayasa.gov.tr/files/bireysel_basvuru/AIHS_tr.pdf, 2.1.2013.
http://www.conventions.coe.int/Treaty/en/Treaties/Html/005.htm, 2.1.2013.
http://www.acma.gov.au/WEB/STANDARD/pc=ACMA_ORG_OVIEW,
30.01.2013.
http://www.acma.gov.au/webwr/aca_home/about_aca/organisational_structur
e/acma_org_structure-1_aug_2012.pdf, 30.01.2013.

http://bundespruefstelle.de/bpjm/information-in-english.html, 15.03.2013.
http://www.coe.int/t/dghl/standardsetting/DataProtection/Liste_autorites_fr.pdf , 29.01.2013.
http://www.ico.gov.uk/about_us.aspx, 29.01.2013.
http://www.cnil.fr/english/the-cnil/status/, 29.01.2013.
http://www.bfdi.bund.de/EN/Home/homepage_node.html, 29.01.2013.
http://www.whitehouse.gov/omb/e-gov, 29.01.2012.
http://www.cabinetoffice.gov.uk/resource-library/chief-information-officers-council, 29.01.2013.
https://www.ria.ee/about-estonian-information-systems-authority/, 29.01.2013.
https://www.bsi.bund.de/EN/Home/home_node.html, 29.01.2013.
http://www.mevzuat.gov.tr/Kanunlar.aspx, 16.10.2012.
http://www.memurlar.net/haber/309117/, 31.01.2013.
http://www.danistay.gov.tr/e2010_2072.htm, 01.02.2013.
http://legislationline.org/documents/section/criminal-codes, 14.02.2013.
http://www.turkhukuksitesi.com/showthread.php?t=6203, 19.12.2012.
http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG, 31.12.2012.
http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm, 13.02.2013.
http://www.iuscomp.org/gla/statutes/StGB.htm, 15.03.2013.
http://en.wikipedia.org/wiki/Communications_Decency_Act, 11.10.2012.
http://www.fcc.gov/guides/childrens-internet-protection-act, 11.10.2012.
http://www.iuscomp.org/gla/statutes/StGB.htm, 15.03.2013.
http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm, 13.02.2013.
http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm, 17.09.2012 .
http://conventions.coe.int/Treaty/EN/treaties/html/181.htm, 18.9.2012.
http://www.coe.int/t/dghl/standardsetting/dataprotection/legal_instruments_en.asp, 18.09.2012.
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML, 18.09.2012.
http://www.turkhukuksitesi.com/showthread.php?t=52705, 18.09.2012.

http://www.sabah.com.tr/Yasam/2010/07/28/yetmis_milyon_kisinin_kimlik_bilgileri_calindi, 18.09.2012.
http://www.ftc.gov/reports/privacy3/fairinfo.shtm, 13.09.2012.
http://oecdprivacy.org/, 12.09.2012.
http://eur-lex.europa.eu/LexUriServ/site/en/oj/2007/l_204/l_20420070804en00180025.pdf, 03.12.2012.
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2002L0058:20091219:EN:PDF, 04.02.2013.
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF, 22.8.2012.
http://www.mevzuat.gov.tr/MevzuatMetin/1.3.2559.pdf, 08.02.2013.
http://www.mevzuat.gov.tr/MevzuatMetin/1.5.2803.pdf, 08.02.2013.
http://www.mevzuat.gov.tr/MevzuatMetin/1.5.2937.pdf, 08.02.2013.
http://www.mevzuat.gov.tr/Metin.Aspx?MevzuatKod=7.5.9596&MevzuatIliski=0&sourceXmlSearch=telekomünikasyon, 08.02.2013.
http://www.mevzuat.gov.tr/Metin.Aspx?MevzuatKod=7.5.11092&MevzuatIliski=0&sourceXmlSearch=telekomünikasyon, 08.02.2013.
http://www.legislation.gov.uk/ukpga/2001/24/contents, 22.08.2012.
https://opennet.net/research/profiles/united-kingdom, 14.03.2013.
http://afasam.org/tr/savunma-guvenlik/turkiyenin-yeni-guvenlik-sorunu-siber-terorizm/, 03.12.2012.
http://www.haberalfa.com/haber/teknoloji/mit-ve-emniyete-darbe/833.html, 03.12.2012.
http://www.informationweek.com/government/security/cyber-attacks-becoming-top-terror-threat/232600046, 10.9.2012.
https://opennet.net/research/profiles/italy, 14.03.2013.
http://treaties.un.org/doc/db/Terrorism/english-18-11.pdf, 07.12.2012.
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:En:HTML, 23/10/2012.
http://eur-lex.europa.eu/LexUriServ/site/en/consleg/1998/L/01998L0034-20070101-en.pdf, 23/10/2012.

http://www.btk.gov.tr/elektronik_haberlesme_sektoru/yetkilendirme/isletmeciler/isletmeci.php?yetkitipi=ISS_B, 19.10.2012.
http://www.tib.gov.tr/tr/tr-menu-57-yer_saglayicilar_listesi.html, 23.10.2012.
https://opennet.net/research/profiles/france, 15.03.2013.
https://opennet.net/research/profiles/italy, 14.03.2013.
http://www.google.com/transparencyreport/map/, 15.10.2012.
http://www.google.com/transparencyreport/removals/government/US/?p=2011-12, 15.10.2012.
https://opennet.net/research/profiles/united-kingdom, 14.03.2013.
http://www.google.com/transparencyreport/removals/government/GB/?p=2011-12, 15.10.2012.
http://www.bbc.co.uk/news/technology-18479137, 15.10.2012.
https://opennet.net/research/profiles/germany, 15.03.2013.
http://www.indexoncensorship.org/2011/06/france-on-its-way-to-total-internet-censorship/, 15.03.2013.
http://www.mevzuat.gov.tr/Kanunlar.aspx, 16.10.2012.
http://www.danistay.gov.tr/128sayi.pdf, 24.12.2012.
http://www.google.com/transparencyreport/removals/government/TR/?p=2011-12, 15.10.2012.
http://www.iwf.org.uk/about-iwf/remit-vision-and-mission, 30.01.2013.
https://opennet.net/research/profiles/united-kingdom, 14.03.2013.
http://www.legislation.gov.uk/ukpga/2006/11/section/3, 14.03.2013.
http://bundespruefstelle.de/bpjm/information-in-english.html, 15.03.2013.
https://opennet.net/research/profiles/germany, 2010, s. 309, 14.03.2013.
http://www.acma.gov.au/WEB/STANDARD/pc=INT_IND_CONTENT_ABOUT, 30.01.2013.
http://www.comlaw.gov.au/Series/C2004A04401, 30.01.2013.
http://www.guvenliweb.org.tr/istatistikler/node/20, 24.12.2012.
http://www.mevzuat.gov.tr/MevzuatMetin/1.5.2802.pdf, 24.12.2012.
http://eekg.tib.gov.tr/, 12.10.2012.
http://www.guvenliweb.org.tr/istatistikler/files/ihbar_istatistikleri_13.12.2012.pdf, 24.12.2012.

http://www.bbc.co.uk/news/business-16801382, 2.6.2012.
http://www.guardian.co.uk/technology/2009/nov/26/dark-side-internet-freenet 2.6.2012.
https://opennet.net/about-filtering, 12.03.2013.
http://guvenlinet.org.tr/sorgula, 12.10.2012.
http://infopeople.org/resources/filtering/history, 11.10.2012.
http://www.btk.gov.tr/mevzuat/kurul_kararlari/dosyalar/2011%20DK-14-461.pdf, 24.12.2012.
http://www.tib.gov.tr/tr/dokumanlar/internetin_Guvenli_Kullanimi_Sosyal_Aglar_Sunumu.pdf, 12.10.2012.
http://www.guvenlinet.org.tr/tr/menu/14-Profillerde_Neler_Var_.html, 12.10.2012.
http://www2.tbmm.gov.tr/d22/1/1-1305.pdf, 16.10.2012.
http://www.bilgitoplumu.gov.tr/Documents/1/BT_Strateji/Diger/060700_Eylem Plani.pdf, 10.04.2013.
http://www.danistay.gov.tr/e2009_5240.htm, 10.04.2013.