

AKDENİZ ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ

İlker TEPE

MODERN CEZA HUKUKU ANLAYIŞINDA İNTERNET SUÇLULUĞU
VE
TÜRK CEZA HUKUKUNDAKİ YANSIMALARI

Kamu Hukuku Anabilim Dalı

Yüksek Lisans Tezi

Danışman

Prof. Dr. Hayrettin ÖKÇESİZ

Antalya, 2009

AKDENİZ ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ

İlker TEPE

MODERN CEZA HUKUKU ANLAYIŞINDA İNTERNET SUÇLULUĞU
VE
TÜRK CEZA HUKUKUNDAKİ YANSIMALARI

Kamu Hukuku Anabilim Dalı

Yüksek Lisans Tezi

Danışman

Prof. Dr. Hayrettin ÖKÇESİZ

Antalya, 2009

İÇİNDEKİLER

KISALTMALAR	vi
ÖZET	ix
ABSTRACT	x
GİRİŞ	1

BİRİNCİ BÖLÜM

MODERN CEZA HUKUKUNDA İNTERNET SUÇLULUĞUNUN DURUMU VE KONUSU, İNTERNET VE ULUSLAR ARASI CEZA HUKUKU, İNTERNET ORTAMINDA İŞLENEN SUÇLARIN SINIFLANDIRILMASI SORUNU

1- MODERN CEZA HUKUKU TEORİSİNDE İNTERNET SUÇLULUĞUNUN DURUMU VE KONUSU	8
1.1.- Genel Açıklamalar	8
1.2.- Klasik Ceza Hukuku Anlayışının Temel Özellikleri	11
1.2.1.- Genel Olarak	11
1.2.2.- Winfried Hassemer ve Wolfgang Naucke'nin Değerlendirmeleri	14
1.3.- Klasik Ceza Hukuku Anlayışından Modern Ceza Hukuku Anlayışına Geçiş	16
1.4.- Modern Ceza Hukuku Anlayışının Belirleyici Özellikleri	18
1.4.1.- Küreselleşme ve Ceza Hukukuna Etkisi	18
1.4.2.- Cezalandırılabilirliğin Öne Çekilmesi	22
1.4.3.- Ceza Hukuku Normlarının Son Araç Olarak Kullanılması Prensibinde Yaşanan Dönüşüm	26
1.4.4.- Ceza Hukukunun Yapısal Özelliklerinin Esnekleştirilmesi Eğilimi	28
1.5. - Modern Ceza Hukuku Morfolojisi Üzerine Doktrindeki Bazı Görüşler	31
1.5.1. - Winfried Hassemer	31
1.5.2.- Ulrich Sieber	34
1.5.3.- Peter Alexis Albrecht	36

1.5.4.- Felix Herzog	37
1.5.5.- Cornelius Prittwitz	38
1.5.6. Eric Hilgendorf	39
1.5.7. Yener Ünver	40
1.5.8.- Görüşlerin Değerlendirmesi	42
1.6.- Modern Toplumun Temel Dinamiklerinden Olan İnternet Teknolojisinin Gelişim Seyri	43
1.7. – İnternetin Bir Suçluluk Alanı Olarak Normatif Ceza Hukuku Alanına Dahil Edilme Süreci	48
1.7.1.- Uluslar arası Düzenlemeler	53
1.7.1.1.- Avrupa Konseyi Siber Suç Sözleşmesi	53
1.7.1.2.- Irkçı ve Yabancı Düşmanlığı Eylemlerine İlişkin Siber Suç Sözleşmesi Ek Protokolü	58
1.7.1.3.- Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşme	60
1.7.1.4.- A.B. Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Konusunda Bireylerin Korunmasına Dair Yönerge	62
1.7.1.5.- B.M. Çocuk Haklarına Dair Sözleşmeye Ek Çocuk Satışı, Çocuk Fahişeliği Çocuk Pornografisi İle İlgili İhtiyari Protokol	64
1.7.2.- Türk Ceza Hukukunda İnternet de Dahil Olmak Üzere Genel Anlamda Bilişim Suçlarına İlişkin Normatif Düzenleme Süreci	66
1.7.2.1.- - 1989 TCK Ön Tasarısı	66
1.7.2.2.- 3756 Sayılı Kanunla Gerçekleştirilen Düzenleme	67
1.7.2.3.- 1997 TCK Ön Tasarısı	69
1.7.2.4.- 2000 TCK Ön Tasarısı	70
1.7.2.5.- 2003 TCK Ön Tasarısı	71
1.7.2.6.- 5237 Sayılı TCK	72
1.7.2.7.- 5651 Sayılı “İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Hakkında Kanun”	72
1.8.- İnternet Bakımından Modern Ceza Hukuku Anlayışının Normatif Alana Yansımaya Örnek Olarak Federal Alman Anayasa Mahkemesinin 27.02.2008 Tarihli “Online- Araştırma” Kararı	73

1.9.- Deęerlendirme: Modern Ceza Hukuku Teorisinde İnternet Suçluluęunun Yeri ve Türk Hukukundaki Yansımaları	85
2.- İNTERNET SUÇLULUęU VE ULUSLAR ARASI CEZA HUKUKU	95
3.- İNTERNET ORTAMINDA İŞLENEN SUÇLARIN SINIFLANDIRMA SORUNU	100
3.1.- Genel Açıklamalar	100
3.2. - Avrupa Konseyi Siber Suç Sözleşmesine Kadar Yapılan Bilişim Suçlarına İlişkin Sınıflandırma Örnekleri	102
3.3. - Avrupa Siber Suç Sözleşmesinin Getirdięi Sınıflandırma	104
3.4.- İnternet Özelinde Yapılan Sınıflandırma Örnekleri	105
3.5.- Deęerlendirme	110

İKİNCİ BÖLÜM

SUÇ GENEL TEORİSİ ÇERÇEVESİNDE İNTERNET ORTAMINDA İŞLENEN SUÇLARA İLİŞKİN YAPISAL DEęERLENDİRİLMELER

1. – 5237 SAYILI TCK MD. 6/1-G HÜKMÜNCE BİR KİTLE İLETİŞİM ARACI OLARAK İNTERNET	112
1.1.- Genel Açıklamalar	112
1.2.- Deęerlendirmeler	115
2.- İNTERNET ARACILIęIYLA İŞLENEN İÇERİK SUÇLARDA İHMALİ VE İCRAİ HAREKETLER	118
2.1. Genel Olarak İcrai – İhmali Suç Ayırımı	118
2.2.- İnternet Ortamında İşlenen Suçlarda İhmali ve İcrai Hareketler	123
3.- İNTERNET ORTAMINDA İŞLENEN SUÇLARDA MANEVİ UNSUR SORUNU	124
4- İNTERNET ORTAMINDA İŞLENEN İÇERİK SUÇLARI BAKIMINDAN TCKMD. 26 ANLAMINDA HAKKIN KULLANILMASI HUKUKA UYGUNLUK NEDENİNİN ANLAMI	132
4.1.- Genel Açıklamalar	132
4.2.- Ceza Hukuku Bağlamında İnternetin Bazı Temel Hak Ve Özgürlüklerle İlişkisi	137
4.2.1.- Düşünce ve İfade Özgürlüęü	137
4.2.1.1.- Düşünce Özgürlüęü	138

4.2.1.2.- İfade Özgürlüğü	142
4.2.1.3.- Ceza Hukuku Perspektifinden İnternetin Düşünce ve İfade Özgürlüğü ile İlişkisi	146
4.2.2. – Haberleşme Özgürlüğü	152
4.2.2.1.- Ceza Hukuku Perspektifinden İnternetin Haberleşme Özgürlüğü İle İlişkisi	158
5.- SUÇA ETKİ EDEN NEDEN OLARAK ALENİYET UNSURUNUN İNTERNET ARACILIĞIYLA İŞLENEN SUÇLAR BAKIMINDAN DEĞERLENDİRİLMESİ	162
5.1.- Genel Açıklamalar	162
5.2.- Aleniyet Kavramı	163
5.3.- Aleniyet İle İhtilat Arasındaki Fark	167
5.4.- Aleniyet Unsuru Bakımından İnternet Yayıncılığı	168
6.- SUÇA İŞTİRAK HÜKÜMLERİ BAĞLAMINDA İNTERNET SÜJELERİNİN KONUMLARI VE CEZAİ SORUMLULUKLARI	171
6.1.- Genel Açıklamalar	171
6.2.- İçerik Sağlayıcının Sorumlulukları	173
6.3.- Yer Sağlayıcının Sorumlulukları	175
6.4.- Erişim Sağlayıcının Sorumlulukları	176
6.5.- Toplu Kullanım Sağlayıcının Sorumlulukları	177
6.6.- İnternet Süjelerinin Ceza Sorumlulukları Bakımından Bir Uygulama Örneği Olarak Compu-Serve Davası	178
6.7.- TCK'ye Hakim İştirak Sistemi İçinde İnternet Süjelerinin Konumu	181
7.- İNTERNET ORTAMINDA İŞLENEN SUÇLARA YÖNELİK UYGULANACAK HUKUKUN TESPİTİ SORUNU	184
7.1.- Genel Açıklamalar	184
7.2.- Alman Ceza Hukukunda İnternet Ortamında İşlenen Suçlara Uygulanacak Hukukun Tespiti Sorununa İlişkin Tartışmalar	185
7.3.- Türk Ceza Hukuku Sisteminde İnternet Ortamında İşlenecek Suçlara Uygulanacak Hukukun Tespiti	189
8.- TÜRKİYE'DE İNTERNET ORTAMINDA İŞLENEN İÇERİK VE MÜDAHALE SUÇLARIDA YER BAKIMINDAN YETKİ SORUNU	190
8.1.- Genel Açıklamalar	190

8.1.1.- Müdahale Suçlarında Yer Yönünden Yetkili Mahkemenin Tespiti Sorunu	191
8.1.2.- İçerik Suçlarında Yer Yönünden Yetkili Mahkemenin Tespiti Sorunu	193

ÜÇÜNCÜ BÖLÜM

TÜRK CEZA KANUNUNDA İNTERNET ORTAMINDA İŞLENEBİLEN SUÇLAR

1.- TÜRK CEZA HUKUKUNDA İNTERNET ORTAMINDA İŞLENEBİLEN BAZI SUÇLARIN DEĞERLENDİRİLMESİ	196
1.1.- Genel Olarak	196
1.2.- TCK'de Düzenlenen Bazı İçerik Suçlarının Değerlendirilmesi	197
1.2.1.- İntihara Yönlendirme	197
1.2.2.- Cinsel Taciz	205
1.2.3.- Tehdit	211
1.2.4.- Şantaj	218
1.2.5.- Hakaret	222
1.2.6.- Haberleşmenin Gizliliğini İhlal	228
1.2.7.- Özel Hayatın Gizliliğini İhlal	235
1.3.- TCK'de Düzenlenen Bazı Müdahale Suçlarının Değerlendirilmesi	239
1.3.1.- Eğitim ve Öğretimin Engellenmesi	239
1.3.2.- Kişinin Huzur ve Sükununu Bozma	244
1.3.3.- Haberleşmenin Engellenmesi	250
1.3.4.- Kişisel Verilerin Kaydedilmesi	255
1.3.5.- Verilerin Hukuka Aykırı Bir Biçimde Verilmesi veya Ele Geçirilmesi	264
1.3.6.- Bilişim Sistemine Girme	267
1.3.7.- Bilişim Sistemini Engelleme, Bozma, Veriler Yok Etme veya Değiştirme	280
SONUÇ	304
KAYNAKÇA	306
Ö Z G E Ç M İ Ş	319

KISALTMALAR

AB	: Avrupa Birliđi
ABD	: Amerika Birleşik Devletleri
AİHM	: Avrupa İnsan Hakları Mahkemesi
AİHS	: Avrupa İnsan Hakları Sözleşmesi
AÜHFD	: Ankara Üniversitesi Hukuk Fakültesi Dergisi
AÜSBFD	: Ankara Üniversitesi Siyasal Bilimler Fakültesi Dergisi
AYM	: Anayasa Mahkemesi
AYMK	: Anayasa Mahkemesi Kararı
B	: Band
Bkz	: Bakınız
BM	: Birleşmiş Milletler
C	: Cilt
CD	: Ceza Dairesi
CGK	: Ceza Genel Kurulu
CHD	: Ceza Hukuku Dergisi
CÜSBED	: Cumhuriyet Üniversitesi Sosyal Bilimler Enstitüsü Dergisi
Çev	: Çeviren
Der	: Derleyen
DÜHFD	: Dicle Üniversitesi Hukuk Fakültesi Dergisi
E	: Esas
Ed	: Editör
EÜSBED	: Ege Üniversitesi Sosyal Bilimler Enstitüsü Dergisi
GA	: Goldammer's Archiv für Strafrecht
GÜMMFD	: Gazi Üniversitesi Mimarlık ve Mühendislik Fakültesi Dergisi

H	: Heft
HD	: Hukuk Dairesi
HFSA	: Hukuk Felsefesi ve Sosyolojisi Arkivi
HGK	: Hukuk Genel Kurulu
HPD	: Hukuki Perspektifler Dergisi
Hrsg	: Herausgeber
İBD	: İstanbul Barosu Dergisi
in	: İçinde
İTÜSBED	: İstanbul Teknik Üniversitesi Sosyal Bilimler Enstitüsü Dergisi
İÜHFMD	: İstanbul Üniversitesi Hukuk Fakültesi Mecmuası
JA	: Juristische Arbeitsblätter
K	: Karar
KHukA	: Kamu Hukuku Arşivi
KGCHS	: Karşılaştırmalı Güncel Ceza Hukuku Serisi
KritV	: Kritische Vierteljahrsschrift für Gesetzgebung und Rechtswissenschaft
md	: Madde
MHD	: Milletler arası Hukuk Bülteni
NJW	: Neue Juristische Wochenschrift
No	: Numara
OECD	: Organisation for Economic Co-operation and Development (Ekonomik Kalkınma ve İşbirliği Örgütü) İktisadi İşbirliği ve Gelişme Teşkilatı
Prg	: Paragraf
sh	: Sayfa
S	: Sayı
SBFD	: Siyasal Bilgiler Fakültesi Dergisi

TBA	: Türkiye Bilişim Ansiklopedisi
TBBD	: Türkiye Barolar Birliği Dergisi
TBMM	: Türkiye Büyük Millet Meclisi
TCK	: Türk Ceza Kanunu
TDK	: Türk Dil Kurumu
TMK	: Türk Medeni Kanunu
UEİS	: Ulusal Elektronik İmza Sempozyumu
vb	: ve benzeri
vd	: ve devamı
vs	: ve sair
Y	: Yıl
YÜHFD	: Yeditepe Üniversitesi Hukuk Fakültesi Dergisi
ZRP	: Zeitschrift für Rechtspolitik
ZStW	: Zeitschrift für die gesamte Strafrechtswissenschaft

ÖZET

İnternet modern toplum olarak kabul edilen bilgi toplumunun en önemli kaynaklarından biri haline gelmiştir. Özellikle yaygınlaşan bilgisayar ağları ve veri transferi imkanıyla dünyanın herhangi bir noktasından başka bir noktaya ulaşım çok hızlı ve az maliyetli olarak mümkün hale gelmiştir. Bu bağlamda bilişim – iletişim teknolojileri arasında en etkin rolü hiç şüphe yok ki internet üstlenmektedir.

Klasik iletişim araçları olarak nitelendirilebilecek olan telgraf, telefon, mektup artık internet sayesinde çok sık kullanılmaz olmuş, bunların yerini e- posta, eş zamanlı görüntülü ve/veya sesli iletişim imkanı veren programlar almaktadır. Artık basın kuruluşları yatırımlarını kullanıcının isteği ve beklentisi doğrultusunda gazete, dergi v.b. kitle haberleşme araçlarına değil internete yapmaktadırlar. Çünkü bilgi toplumunda bilgiye erişim hızı çok önem arz etmektedir. Örneğin gazeteler internet ortamında hazırladıkları web siteleri aracılığıyla gelişmeleri anında kamuoyu ile paylaşabilir hale gelmişlerdir. Bu anlamda toplumsal yaşamı kolaylaştıran birçok avantajı bünyesinde barındıran internet, aynı zamanda bir o kadar da riskli bir yapılanmadır. Çünkü internet, ağların ağı olması hasebiyle küresel bir bütünlük arz ettiği için mutlak kontrolü çok zor ve hatta imkânsızdır. Bunun dışında tüm teknolojik sistemler gibi internet de düzenleme boşlukları olan ve bu boşluklar dolayısıyla büyük zarar olasılıklarını bünyesinde barındıran bir sistemdir. Bu çıkar - risk dengesi içerisinde toplumsal yaşamın barış ve huzur içerisinde sürdürülebilmesi için en önemli araç hukuk ve bilhassa ceza hukukudur. Dolayısıyla modern toplumun en önemli sorunsalı olan internetin ceza hukuku çerçevesinde değerlendirilmesi ancak modern ceza hukuku anlayışı içerisinde mümkün olmaktadır.

Modern ceza hukuku anlayışında internet bir suçluluk alanı olarak ele alınırken, modern toplumun temel karakterini yansıtan araçlardan olan interneti, modern toplumun ceza hukuku içindeki yerini ve Türk Ceza Hukuku bakımından bu konunun yansımalarını teorik bir arka plan üzerinde sorunsallaştırılmaya çalışmak, bu sorunsallaştırma esnasında ceza hukuku gelişimi süreçsel bir bütünlük içerisinde ele almak gerekmektedir. Bunun yanında suç genel teorisi anlamında internetin özellikli durumları ve klasik suç tiplerinin internet ortamında işlenebilirliği de ayrıca ele alınmalıdır.

INTERNET CRIMINALITY FROM THE PERSPECTIVE OF MODERN CRIMINAL LAW UNDERSTANDING AND ITS REFLECTION IN TURKISH CRIMINAL LAW

ABSTRACT

Internet is one of the most important sources of the information society which is assumed as the modern society. Especially with the development of computer networks and possibility of data transfer, it has been possible to reach to any point of the world cheaply and quickly. In this context internet has the most efficient role among informatics and communication technologies.

Telegraph, telephone and letters, which are considered as classical communication instruments, are not used so often anymore and they can be said to be replaced by e-mail and synchronous communication programs. Nowadays media corporations are investing in internet instead of other mass media products such as newspapers, magazines etc. in accordance with the demand of users. Because the speed of access to information is very important in an information society. For example, newspapers are able to share information with the public instantly through their internet sites. In this context internet has got so many advantages as it's risky structure. While internet is the network of networks and constitutes a global integrity, it is so difficult almost impossible to control. At the same time internet just like other technological systems has got so many harms because of legal loopholes. In this context of benefit-risk balance, law especially criminal law is the most important tool to obtain social peace. Accordingly, internet; the most important problematic of the modern society can be evaluated only according to modern criminal law doctrine.

In modern criminal law doctrine internet is considered as a crime zone. The position of internet which reflects the characteristics of the modern society in criminal law and Turkish Criminal Law can be theoretically problemized by considering the evaluation of criminal law entirely. In addition to that special situations and committing classical crimes through internet are issues that must be considered in context of crime theory.

GİRİŞ

Günümüzde modern toplum denildiğinde bilgi toplumu akla gelmektedir. Bilgi toplumu, 1950 ve 1960'lı yıllarda A.B.D., Japonya, Batı Avrupa ülkeleri gibi gelişmiş ülkelerde bilgi teknolojilerinin giderek artan bir şekilde kullanımıyla ortaya çıkmış bir sürecin neticesi olarak kabul edilmektedir.¹ Farklı bir ifade ile bilgi toplumu, bilginin sermaye, hammadde, enerji ve insan gücü gibi üretim unsurlarından biri haline dönüştüğü, ekonomide hammadde ve ürün olarak kullanıldığı, herkes tarafından paylaşıldığı ve toplum içerisinde kültürel bir değer olarak kabul edildiği ve bilgi-iletişim teknolojisinin her alanda kullanılmaya başlandığı bir toplum yapısı olarak tanımlanabilmektedir.² Gelişmiş ülkelerde şekillenen bu toplum tipinin en önemli özelliği, bilginin ve bilgi teknolojilerinin tarım, sanayi, hizmet sektörleriyle birlikte eğitim, sağlık, iletişim gibi alanlarda da kullanılabilir olmasıdır. Bu nedenle, bilgi toplumundaki gelişmeler yeni teknolojik, ekonomik, sosyal ve kültürel gelişmeleri de beraberinde getirmektedir. Bu yönüyle bazı yazarlar bilgi toplumu olarak adlandırılan bu olgunun, aslında Endüstri Toplumu'nun bir ileri aşamasını olduğunu ifade eder.³

Gelişim süreci ne olursa olsun üzerinde hemfikir olunan nokta, bilgi toplumunun temel dinamiğinin bilimsel ve teknolojik gelişmelerle ortaya çıkan bilgi ve bu bilginin hayatın tüm alanlarında etkili olarak kullanılmasıdır. Son yarım yüzyılda özellikle genetik, atom, enerji ve bilgi – iletişim teknolojileri gibi doğrudan toplumsal yapıları etkileyecek bilgi alanlarında meydana gelen gelişmeler sosyal, siyasal ve ekonomik ilişkileri ciddi bir dönüşüme uğratmıştır. Bu dönüşüm dinamik bir toplumsal değişim sürecine sebebiyet vermiştir. Çünkü bilim- teknoloji alanında hemen her gün bir yeniliğe tanık olunmakta ve meydana gelen her yenilik bir önceki aşamayı demode kılmakta, böylece devre dışı bırakmaktadır. Toplumsal

¹ **KÖKSAL**, Aydın, Bilişim Devrimi, Küreselleşme ve Uygarlıklar Çatışması Ortamında Kimliğini Arayan Türkiye, http://www.bilisim-ltd.com.tr/akoksal/yayinlar/2003/Bilisim_Devrimi_Kuresel_Uygar_Catismasi.html (Erişim Tarihi: 18.09.2007, Saat:20:05)

² Bilgi Toplumuna ilişkin daha detaylı bilgi için bkz. **ERKAN**, Hüsnü, Bilgi Toplumu ve Ekonomik Gelişme, Ankara, 1993, sh: 96-101; **ÇOBAN**, Hasan, Bilgi Toplumuna Planlı Geçiş: Gelecekte Kaçılmaz: Bilgi Toplumuna Planlı Geçiş İçin Stratejik Planlama ve Yönetim Bilgi Sistemi Uygulamaları, İstanbul, 1997, sh: 12; **TEKELİ**, Hasan, Bilgi Çağı: Bilgi Çağının Sosyal, Kültürel, Ekonomik Etkileri, İstanbul, 1994, sh: 10 v.d.

³ **SEZAL**, İhsan, “Enformasyon Toplumu ve Demokrasi”, in : Sosyoloji Konuşmaları (Der: Saadettin ELİBOL) Ankara, 1991, s: 29 – 30; **AVCI**, Nabi , Kitle Kültürü ve Enformatik Cehalet, Genişletilmiş 3. Baskı, Ankara, 1990, s: 71 vd.

yaşamın sürekli deęişip gelişmesi, teknolojik ve bilimsel alanda bireyin gerek toplumsal gerek bireysel yaşamında daha çok etken olması, bireye bir taraftan büyük kolaylıklar sağlarken dięer yandan kaçınılmaz olarak sayısız zarar ve tehlike neticelerine de yol açmaktadır. Çünkü genel anlamda bilgi, kullanana ve kullanım amacına baęlı olarak farklı sonuçları ortaya çıkarmaktadır. Hatta kimi durumlarda dışarıdan hiçbir müdahale gerçekleşmemesine rağmen bizatihi kullanılan bilgi veya teknolojinin kendisi bir takım risk ve tehlikeler içerebilir.

Bu durumda yukarıda da ifade edilmeye çalışıldığı üzere toplumsal yaşam, bilimsel ve teknolojik gelişmelere baęlı olarak ortaya çıkan, yaşam koşullarını iyileştirici nitelikteki neticelerin güvencesi ile bu gelişmelerin barındırdığı risk ve tehlikeleri bir arada bulundurmaktadır. İşte tam bu noktada modern toplumun yani bilgi toplumunun aktarılmaya çalışılan anatomisi içinde bilgi – iletişim teknolojileri, bilhassa internet teknolojisi dięer alanlara oranla bir adım önde yer almaktadır ve bir bakıma bünyesinde tüm bu denklemleri içermektedir. Çünkü örnek olması anlamında atom, enerji, genetik teknolojileri gibi bilgi alanlarındaki gelişmeler konunun uzmanları tarafından bir takım bilimsel – teknik süreçlerden sonra toplumsal yaşama sadece neticelerin aktarıldığı alanlar olup bu durum bilişim- iletişim, özellikle de internet teknolojisi için farklılık arz etmektedir. Başka bir anlatımla bu teknoloji alanına toplumun her kesiminden insanlar kolaylıkla erişebilmekte ve kullanabilmekte, dolayısıyla da etkileri çok daha geniş, açık ve doğrudan hissedilmektedir.

Modern toplumu şekillendiren bu çıkar-risk dengesi özellikle 1980’li yıllardan sonra bilim ve teknolojideki gelişmelerin hız kazanmasıyla daha çok tartışılı olmuştur. Bu tartışmalar son yıllarda çevreye verilen farklı nitelikte zararlar, atık maddelerin hayvan ve bitkilere verdiği zarar, atmosfer felaketleri, canlıların genetik yapısına yapılan müdahalelerle ortaya çıkan problemler, aslında bilgi üretim ve kullanım alanları olarak modern teknolojilerin potansiyel riskler içerdiği, toplumun bu riskler karşısında korunması gerektiği yönünde eğilimleri beraberinde getirmiştir.⁴ 1986 yılında Çernobil Nükleer Reaktöründe meydana gelen patlamanın onlarca ülkede milyonlarca insanın yaşamına mal olması yada yaşamlarının tehlike altında kalması, 1995 yılında Dolly adlı bir koyunun kopyalanmasının ardından genetik kodlar üzerinde oynama yapılarak 1997 yılında insan kopyalandığının iddia edilmesi, 2000 yılında Filipinler kaynaklı olan ve bir öğrenci tarafından kullanılan “I Love You” adlı bir bilgisayar virüsü ile dünya çapında çok büyük finansal zararlara neden olması⁵ gibi

⁴ ÜNVER, Yener, Ceza Hukukuyla Korunması Amaçlanan Hukuksal Deęer, Ankara, 2003, s: 943.

vakalar neticesinde, modern toplumda bilgiye ulaşım ve bilginin kullanımının kontrol edilemeyen riskler barındırdığı gerçeği kabul edilmiştir. Bu noktadan itibaren de modern toplum “Risk Toplumu” olarak kabul görmüştür.⁶

“Risk Toplumu” kavramı ilk kez Alman sosyolog *Ulrich Beck* tarafından kullanılmış olup, söz konusu toplum tasarımı modernitenin evrim sürecinin bir neticesi olarak görülmüştür.⁷ Bu evrimin en önemli noktasını küreselleşme olgusu teşkil etmektedir. Çünkü bilginin sınır tanımaksızın dünyanın her yerindeki insanlar tarafından erişilebilir kılınması ile bu bilginin kullanımı hususunda kontrol imkanları oldukça azalmakta dolayısıyla da bilgi özünde potansiyel bir risk unsuruna dönüşmektedir. *Beck* bu süreci “ikinci modernite” süreci olarak görmektedir. Yazara göre birinci modernite ulusal devletleri bilgiyi kullanma ve bilgi kaynağına sahip olmaları sürecinde hakim unsur olarak görürken, “ikinci modernite” sürecinde küreselleşme ile birlikte bilginin kaynağının ve bizatihi kendisinin ulusal sınırlar ötesinde anonimleşmiş ve kontrol imkanlarındaki eksiklik dolayısıyla bir belirsizlik ortaya çıkmıştır.⁸ Bu neticeden hareketle bilgi ve kaynakları üzerindeki söz konusu belirsizlik ortamının risk unsurunu tetiklediği, böylece “ikinci modernite” olarak kabul ettiği sürecin “Risk Toplumu” tasarımının genel gerekçesi olarak görmektedir.

“Risk Toplumu” tasarımı özünde küreselleşmenin somut anlamda ilk neticelerinin alındığı bilgi – iletişim teknolojilerindeki özellikle de internet teknolojisindeki gelişmeye bağlı olarak olgunlaşmış bir tasarımdır. Çünkü yukarıda da ifade edildiği üzere temel problem bilgi ve kaynaklarının gerek erişim gerekse kullanım imkanları bakımından kontrol altında tutulamaması ile bunların amacı dışında kullanılarak hem bireyler hem de topluma zarar verme riskini doğurmasıdır. Böyle bir yaklaşım da doğal olarak gittikçe artan bir güvenlik ihtiyacını ortaya çıkarmıştır.

⁵ “I Love You” adlı virüsün Microsoft Outlook üzerinden dünyanın birçok yerine yayılması verdiği zararlara ilişkin detaylı açıklamalar için bkz. **HILGENDORF**, Eric, Die Neuen Medien und das Strafrecht, in: Zeitschrift für die Gesamte Strafrechtswissenschaft 113, H: 4, Berlin/Newyork, 2001, sh: 651.

⁶ **HONG**, Seung- Hee, Flexibilisierungstendenzen des modernen Strafrechts und das Computerstrafrecht, Kaynak: <http://w3.ub.uni-konstanz.de/v13/volltexte/2003/954/pdf/Hong.pdf> (Erişim Tarihi : 17.09.2007, Saat: 20:08), sh: 39 v.d.

⁷ **YALÇINKAYA**, Mehmet/ **ÖZSOY**, Esat Risk Toplumu: Bilgi Toplumunun Evriminde Yeni Boyut, Kaynak: <http://www.tkgm.gov.tr/turkce/dosyalar/diger%5Cicerikdetaydh342.doc> (Erişim Tarihi: 18.09.2007, Saat:20:12).

⁸ **HONG**, Seung- Hee, Flexibilisierungstendenzen, sh: 40.

Buraya kadar özetlenmeye çalışılan, modern toplum olarak kabul edilen bilgi toplumunun tarihsel süreç içinde yaşadığı dönüşüm ile hangi koşullar altında “Risk Toplumu”na dönüştüğüdür. Bu sürecin ortaya konulması modern ceza hukukunun algılanışı ve ana konu olan internet suçluluğuna bakışın teorik temelleriyle kavranması bakımından hayati önem taşımaktadır. Çünkü bilinmektedir ki, modern ceza hukukunun amacı toplumsal açıdan önemli, değer taşıyan yaraların yani insanların toplum içinde birlikte yaşamalarının koşullarını koruyarak bireylerin güvenli, barışçıl, sağlıklı, özgür ve demokratik bir ortamda yaşayabilmelerini sağlamaktır.⁹

İnternetin her geçen gün artan oranda bireysel ve toplumsal hayatı etkiliyor olması, birçok alanla beraber hukuk alanında bilhassa da ceza hukuku alanında sorunlara neden olmaktadır. Bu sorunların kaynağına ve yine bu sorunlar karşısında ceza hukukunu özellikli kılan hareket noktalarına ilişkin birinci bölümde detaylı bir çözümleme yapılacaktır¹⁰. Bu çözümlemenin ortaya koyduğu teorik arka planın ardından internete ilişkin ceza hukuku sisteminin normatif yapısı ele alınacak olursa her şeyden önce ceza hukuku bakımından internetin gelmiş olduğu durumun kısa bir değerlendirmesi yapılmalıdır.

Özellikle 90'lı yıllardan itibaren artış gösteren ve 2000'li yıllardan itibaren çok ciddi bir artış gösteren internet ortamında işlenen suçlar teknik olarak bilişim suçları kapsamında ele alınmıştır. Bilgi – iletişim teknolojisinin gelişim süreci dikkate alındığında bu durum metodolojik açıdan da isabetli bir tercih olarak kabul görmektedir. Çünkü internet teknolojisi bilgisayarın herkes tarafından kullanılabilir hale gelmesinin ardından gelişen bir teknolojidir. Haliyle bilgisayar kullanımının - müstakil veya bir ağ dahilinde – artmasından kaynaklanan ceza hukuku sorunlarına ilişkin oluşturulan bilişim suçları kavramı daha sonra işlevsel hale gelen internet teknolojisini de kapsamış ve internet ortamında işlenen suçlar da bilişim suçları olarak kabul görmüştür. Ancak internet teknolojisinin gösterdiği gelişim bir anda farklı bir seyri beraberinde getirmiştir. Öyle ki şu anda normatif düzenlemelerle belirlenen bilişim suçlarına dikkat edilecek olursa, neredeyse tüm suç tipleri bakımından internet temel unsur olarak kabul edilmektedir. İnternetin doğrudan bir unsur olarak kabul edilmediği suç tipleri bakımından da uygulamada bu suç tiplerinin sıklıkla internet aracılığıyla işlendiği

⁹ ÜNVER, Hukuksal Değer, sh: 442.

¹⁰ Özellikle internetin günümüz ceza hukuku anlayışı bakımından taşıdığı değer ve anlam için bkz. Birinci Bölüm, 1.8.- Değerlendirme: Modern Ceza Hukuku Teorisinde İnternet Suçluluğunun Yeri ve Türk Hukukundaki Yansımaları.

görülmektedir. Bu da gösteriyor ki her ne kadar bilişim suçları sadece internet aracılığıyla işlenen suçlara indirgenemeyecekse de, artık bilişim suçları olarak sınıflandırılan suç tipleri bakımından interneti tüm boyutlarıyla ele almak bir zorunluluk haline gelmiştir.¹¹

İnternetin yeni bir suçluluk alanına kaynaklık etmesi ve buna paralel olarak internet üzerinden gerçekleştirilen suç teşkil eden eylemlerin gerek nitelik gerekse nicelik olarak giderek artan bir önem kazanması birçok farklı bakış açısıyla temellendirilebilmektedir. Bu temellendirme noktalarından en önemlisi internet ile sunulan hizmetlerin ulusal sınırları aşarak herhangi bir kitle haberleşme aracına kıyasla çok daha geniş bir yayılım sağlaması ve bu suretle daha etkili neticelere vücut vermesidir. Bu durumu *Hilgendorf* şöyle ifade etmektedir¹²:

“ Data ağları ve internetin dünya çapında hızlı gelişimi ve bunun sonucu olarak sınır aşan veri transferleri, tikel devletlerin hukuk düzenlerinde önemli sorunları meydana çıkartmıştır. Aynı sorun milli hukuk kültürünün bir mahsulü olan ceza hukuku açısından da mevcuttur. Kişiler, internetteki yayınlara kural olarak tikel devletlerin milli ülkesinin sınırlarını aşarak dünya çapında ulaşabilmektedir. Milli sınırlar dahilinde kalan bir ceza hukuku anlayışı bu sebeplerden ötürü data ağı suçluluğu ile mücadelede kifayetsiz kalmaktadır. Sınır aşan bir ceza hukuku anlayışı şimdiye kadar sadece uluslar arası ceza hukuku alanında kendini var edebilmiştir. Ceza hukukunun gücü kendini, geleneksel anlayış uyarınca kendini tikel devletlerin bağımsızlığı üzerinde inşa etmektedir. Her bir devlet ise bu özellikleri sınırlayan gelişmeler belli bir sınıra karar müsamahakar olabilmektedir. Ortaya serilen bu tablodan milli ceza hukuklarının data ağı suçluluğuna yönelik müeyyideler tanzim etme hususunda etkin olmayacaklarını tespit etmekteyiz. Mesele ancak uluslar arası iş birliği ile hal olabilecek kadar geniş, küresel bir hal almıştır. Bu nedenle herhangi bir devletin kendi başına “ağların beyi” rolüne heveslenmesi de uluslar arası nezaketle bağdaşmayan bir sonuca hasıl olacaktır”.

Hilgendorf bu tespiti yaparken aslında bir ceza hukuku alanı olarak internet suçluluğunu örnek olarak kabul etmekte ve birinci bölümde de ayrıntısıyla ortaya konulduğu üzere, ceza hukukunun klasik yapılarında modern toplumun gereklerine paralel olarak

¹¹ İnternetin bir ceza hukuku alanı olma süreci hakkında daha detaylı bilgi için bkz. **HEINRICH**, Bernd, Aktuelle Probleme des Internetstrafrecht, <http://thinklaw.wordpress.com/2006/11/30/prof-dr-bernd-heinrich-aktuelle-probleme-des-internetstrafrechts> (Erişim Tarihi: 08.11.2007).

¹² **HILGENDORF**, Eric, Yeni Medya Araçları ve Ceza Hukuku (Çev: Mehmet Cemil OZANSÜ), in: KGCHS/7, “Özel Yaşam, Medya ve Ceza Hukuku, (Der: Yener ÜNVER) Ankara, 2007, sh: 266.

yaşanan dönüşüme dikkat çekmektedir. Artık ceza hukuku klasik anlamda, yazarın değimiyle, salt “ milli kültürün bir mahsulü” olmaktan çıkmış, küreselleşmenin etkisiyle uluslar arası/ uluslar üstü işbirlikleriyle şekillenen kolektif bir iradenin görünümü olarak anlam kazanmıştır.¹³ Keza bu durum internet ortamında gerçekleşen kötüye kullanımlar bakımından önemli bir denek taşı olarak kendini göstermektedir.¹⁴ Öyle ki klasik suçla mücadele yöntemlerinin, internette işlenen suçlar yönünden ne denli yeterli olduğu ve internetin gerek teknik yapısından gerekse ulusal üstü karakterinden kaynaklanan engeller karşısında, bu yöntemlerin etkinlikleri son yıllarda ciddi bir biçimde tartışılan bir husustur.¹⁵

Bu denli önemli ve hassas bir konunun incelendiği bu tezde, Türk Ceza Hukuku sistemi içinde internet ortamında işlenen suçlar tek başına ele alınmamış, modern ceza hukukunun teorik problemleri ve internet sùjelerinin ceza sorumluluğu ile birlikte değerlendirilmiştir. Dolayısıyla internet özelinde bir modern ceza hukuku incelemesi özelliğini de barındırmaktadır.

Bu bağlamda tezin birinci bölümünde öncelikle modern toplumun temel karakterini yansıtan araçlardan olan interneti, modern toplumun ceza hukuku içindeki yeri ve Türk Ceza Hukuku bakımından bu konunun yansımaları teorik bir arka plan üzerinde sorunsallaştırılmaya çalışılmıştır. Bu sorunsallaştırma esnasında kanaatimizce kaçınılmaz olarak ceza hukuku gelişimi süreçsel bir bütünlük içerisinde ele alınmış ve klasik ceza hukuku anlayışından itibaren tarihsel gelişim çizgisine paralel bir seyir, doktrinden teorik değerlendirmelerle ortaya konulmaya çalışılmıştır. Devamında internetin bir suçluluk alanı olarak normatif ceza hukuku alanına dahil edilme süreci göz önünde bulundurularak bir değerlendirme yapılmıştır. Ardından internetin sınır aşan karakteri nedeniyle internet ortamında işlenen suçların uluslar arası ceza hukuku çerçevesinde değerlendirilip değerlendirilmeyeceği tartışılmış ve son olarak da internet ortamında işlenen suçların sınıflandırılması sorunu üzerinde durulmuştur.

¹³ Bu konuda örnek uygulama ve tartışmalar için bkz. **HONG**, Seung Hee, Compu- Serve Davası (Çev: İlker TEPE), : in: KGCHS/7- “Özel Hayat, Medya ve Ceza Hukuku”, sh: 323 vd.

¹⁴ Ulusal ceza hukuku ile internet suçluluğunun küresel boyutu arasındaki ilişki üzerine ayrıca bkz. **KOCH**, Arnd, Nationales Strafrecht und globale Internet – Kriminalitaet, in: GA – 2002, sh: 703 vd.

¹⁵ **SINAR**, Hasan, İnternet ve Ceza Hukuku, İstanbul, 2001, sh: 69.

İkinci bölümde ise internet ortamında işlenen suçları suç genel teorisi çerçevesinde özellikli görülen alanlarda değerlendirmeler yapılmış ve bu değerlendirmeler 5237 sayılı TCK'nin sistematığı içerisinde olgunlaştırılmaya çalışılmıştır.

Üçüncü bölümde ise ilk bölümde yapılan hem teorik hem de normatif değerlendirmelerin yansıtılabileceği ve somutlaştırılabileceği tartışmaları içeren belli suç tipleri değerlendirilmiştir. Bu bölümde tüketici bir yaklaşım tarzı içerisine girilmeyip internet ortamında işlenmesi bakımından özellik arz ettiği düşünülen suç tipleri ele alınmıştır. Bu bakımdan hareket noktasını da 5237 sayılı TCK'de düzenlenen suçlar oluşturmuştur.

BİRİNCİ BÖLÜM

MODERN CEZA HUKUKUNDA İNTERNET SUÇLULUĞUNUN DURUMU VE KONUSU, İNTERNET VE ULUSLAR ARASI CEZA HUKUKU, İNTERNET ORTAMINDA İŞLENEN SUÇLARIN SINIFLANDIRILMASI SORUNU

1- MODERN CEZA HUKUKU TEORİSİNDE İNTERNET SUÇLULUĞUNUN DURUMU VE KONUSU

1.1.- Genel Açıklamalar

Teorik düzlemde bakıldığında, üzerinde hem fikir olunan bir modern ceza hukuku yaklaşımı bulunmamaktadır. Göreli bir ifade olan “*modern*” kavramının ceza hukukuna kattığı özellik, söz konusu kavramın algılanış ve yorumlanış tarzına bağlı olarak farklı anlam içeriklerine bürünmektedir. Modern kelimesi sözlüklerde “günümüze ait olan, çağdaş, çağcıl” gibi ifadelerle açıklanmakta ve bu açıklamalar kelimenin dil bilimsel kökeni ile de uyum göstermektedir¹⁶. Dil bilimsel açıdan “*Modern*” kavramı M.S. 5. y.y.’da Latince “tam, şimdi, bugüne ait” anlamına gelen “*modo*” kelimesinden türetilmiş ve ilk aşamada Hıristiyanlığı benimseyen toplumun eski pagan kültüründen koptuğunu ve yeni bir kültürün doğduğunu anlatmak için kullanılmıştır¹⁷. *Modern* kelimesinden türetilen “*modernite*” ise batı merkezli ortaya çıkan ve birbiriyle bağlantılı bütün alanları kapsayan yeni bir algılama ve anlamlandırma biçimidir. Kelimenin terminolojisine uygun olarak geleneksel olandan köklü bir kopuşu ifade eden modernite çok yönlü bir değişim ve dönüşüm sürecine tekabül etmektedir. Bu bağlamda modernite sosyal, kültürel, ekonomik, estetik ve siyasal alanlarda yaşanan dönüşümü ifade etmektedir¹⁸. Bu alanlarda yaşanan değişim ve dönüşüm doğal olarak makro düzeyde hukuk, mikro düzeyde ceza hukuku sistemi için de geçerli olmaktadır.

¹⁶ İŞİK, Hüseyin Murat, Modernite ve Postmodernite Bağlamında Farklılıklar, in: HFSA – 15 (Der: Hayrettin ÖKÇESİZ), İstanbul, 2006, sh: 185.

¹⁷ BERİŞ, Hamit Erhan, Moderniteden Postmoderniteye, in: Siyaset (Der: Mümtaz’er TÜRKÖNE), 2. Baskı, Ankara, 2005, sh: 484.

¹⁸ YÜKSEL, Mehmet, Modernleşme, Toplumsal Yaşamın Hukuksallaşması ve Etik, in: HFSA- 17 (Der: Hayrettin ÖKÇESİZ), İstanbul, 2007, sh: 97.

Genel olarak modern veya çağcıl¹⁹ ceza hukuku yaklaşımlarını ikili bir ayırım dahilinde düşünmenin mümkün olduğu kanaatindeyiz. Birincisi, olması gereken ceza hukukunu betimleyen modern ceza hukuku anlayışıdır. Bu anlayış öz itibariyle, ceza hukukunun amacının çağdaş hümanist ve liberal dengelerle şekillendirildiği bir yaklaşım tarzını barındırmaktadır. Şu halde ideal modern ceza hukuku denilebilecek bu anlayış bir ölçüsüyle klasik – liberal çizginin çağdaş formlarda tasarlandığı bir bakış açısını yansıtmaktadır. Böyle bir yönelimin temelinde, bilhassa İkinci Dünya Savaşı’ndan sonra ağırlık kazanan *Yeni Kantçı* felsefenin de etkisiyle, amaç değer ekseninde ele alınan insanı ve onun haklarını önceleyen bir hukuk anlayışının ortaya çıkması, ülkeler arasında savaş sonrası doğan güvenlik hassasiyetine paralel olarak çok yönlü anlaşma ve ortaklıklara gidilmesi yatmaktadır. Bu girişimlerin ilerleyen zamanlarda ilk amaç olan güvenlik ihtiyacının dışında sosyal, ekonomik, kültürel amaçlara da hizmet eder tarzda genişletilmesi ile birlikte hazırlanan B.M. Evrensel İnsan Hakları Bildirgesi, Avrupa İnsan Hakları Sözleşmesi gibi temel hak bildirilerinin felsefesi de, bu temelin sağlamlanmasına neden olmuştur.²⁰

Modern ceza hukuku kavrayışını ikinci perspektiften ele alanlar ise idealize edilmiş bir ceza hukuku amacından değil “yaşayan” ceza hukukunun görünümünden hareket etmektedirler²¹. Özellikle *Frankfurt Okulu* temsilcileri tarafından hassasiyetle üzerinde durulan bu anlayış modern toplumun sorunlarının ve bu sorunlara çözüm bulma kaygısının öncelendiği bir yaklaşım tarzını barındırmaktadır²². Bu anlamda yaşayan modern ceza

¹⁹ **DÖNMEZER**, Sulhi, Genel Ceza Hukuku Dersleri, İstanbul, 2002, sh: 26.

²⁰ İkinci Dünya Savaşı’ndan sonraki gelişmelerin ceza hukukuna etkisi için bkz. **ÜNVER**, Hukuksal Değer, sh: 232 v.d.

²¹ Bu yaklaşım tarzının en radikal temsilcilerinden biri hiç şüphe yok ki *Günther Jakobs*’tur. *Jakobs*, günümüzde sayıları gün geçtikçe artan terör, organize suçluluk, cinsel suçlar ve diğer tehlikeli eylemlerle mücadeleyi öncelikli sorun haline getirmekte ve bu suçların failleri olarak hukukun belirlediği alan dışına çıkan kişilerin tehlikelilik durumları ne kadar artarsa onların bir düşman olarak muamele görmelerinin o kadar meşru kabul edileceğini kabul etmektedir. *Jakobs*’un “Düşman Ceza Hukuku” olarak tasarladığı bu düşünce yaşayan modern ceza hukukunun “radikal” görünüm tarzlarından birini teşkil etmektedir. *Jakobs*’un bu tasarımı ile ilgili görüşlerinin ve doktrinden yöneltilen eleştirilerin ayrıntıları için bkz. **JAKOBS**, Günther, Yurttaş Ceza Hukuku ve Düşman Ceza Hukuku (Çev: Mehmet Cemil OZANSÜ), in: KGCHS - Terör ve Düşman Ceza Hukuku (Der: Yener ÜNVER), Cilt: 8, Ankara, 2008, sh: 489 v.d.; **JAKOBS**, Günther, Düşman Ceza Hukuku?- Hukukiliğin Şartlarına Dair Bir İnceleme (Çev: Mehmet Cemil OZANSÜ), in: KGCHS/8, sh: 507 v.d.; **ARNOLD**, Jörg, Beş Tezde Düşman Ceza Hukukunun Gelişim Süreçleri (Çev: İlker TEPE), in: KGCHS/8, sh: 527 v.d.; **ÖKÇESİZ**, Hayrettin, “Düşman Ceza Hukuku” Düşüncesinin Eleştirisi, in: KGCHS/8, sh: 553 v.d.; **MALEK**, Klaus, Düşman Ceza Hukuku – 2006 Yılı 30. Müdafiler Günündeki “Düşman Ceza Hukuku – Hukuk Devletindeki Hortlak” Çalışma Grubuna İlişkin Birkaç Düşünce (Çev: Yener ÜNVER), in: KGCHS/8, sh: 591 v.d.

²² **HILGENDORF**, Eric (Unter Mitarbeiter von Thomas FRANK, Brain VALERIUS), Die deutsche Strafrechtswirkung 1975 – 2000- Reformen im Besonderen Teil und neue Herausforderungen, in: Das Strafgesetzbuch, Sammlung der Änderungsgesetze und Neubekanntmachungen (Der: Thomas VORMBAUM/Jürgen WELP), Berlin, 2004, sh: 378 – 379. Ceza Hukukunun geçirdiği evrim konusunda ayrıca

hukuku, ideal modern ceza hukukunun ilkesel yapısından ziyade çağın sorunlarını aşmaya yönelik daha esnek ve amaca uygun yapılarla hareket etmektedir. Her geçen gün etkinliği artan terör ve organize suçluluk, sınır aşan karakteri ile internet suçluluğu ve uyuşturucu veya insan kaçakçılığı suçları dünyayı, *Sieber'in* deyimiyle, risk altında yaşayan bir toplumdaki ibaret görme eğilimini ortaya koymaktadır²³. Böyle bir durumda modern zamanların toplumu da risk toplumu olarak kabul edilmektedir²⁴ ve bu toplumun huzur içinde devamlılığının sağlanması için başvurulacak bir ceza hukukunun da temel amacının söz konusu riskleri olabildiğince ortadan kaldırmak olacağından şüphe duyulmamaktadır.

Kanaatimizce modern ceza hukuku anlayışının çerçevesi çizilirken doğrudan modern ceza hukukunun amacından hareket etmek gerekmektedir. Modern ceza hukukunun temel gayesi insanların toplum içinde ve barış halinde birlikte yaşamalarının korunmasıdır²⁵. Başka ve daha ayrıntılı bir ifade ile modern ceza hukuku toplumsal açıdan önemli, bir değer içeriği barındıran yararların ve insanların toplum içinde birlikte yaşamalarının koşullarını koruyarak bireylerin güvenli, barışçıl, sağlıklı, özgür ve demokratik bir ortamda yaşayabilmelerini sağlamayı amaçlamaktadır²⁶. Bu amacı gerçekleştirmeye yönelik olarak, kendini gösteren her türlü ihtiyacın gidermesinin de ancak modern toplumun kurumlarına uygun alt sistemlerle sağlanabileceği açıktır. Dolayısıyla toplumsal bir alt sistem olan ceza hukuku modern yapılarıyla ele alınırken, modern toplumun ceza hukuku olarak kavranmalıdır.

Bu bakış açısıyla her şeyden önce modern toplumun temel dinamiklerinden olan internet ve onun odak olduğu bir suçluluk analizinin nasıl bir ceza hukuku yaklaşım tarzı içerisinde sorunsallaştırılacağı önem arz etmektedir. Böyle bir değerlendirmeden mahrum bir internet suçluluğu analizi metodolojik açıdan eksik ve hatalı sonuçlara götürebileceği gibi bu alana dair sorunlara ilişkin çözüm önerilerini ceza hukuku teorisi anlamında temelsiz bırakacaktır.

bkz. **EICKER**, Andreas, Ceza Hukukunun Prosedürleştirilmesi Işığında Terörle Mücadele Kanunu Yapma (Çev. Ali Kemal YILDIZ), in: KGCHS/8, sh: 678- 679.

²³ **SIEBER**, Ulrich, Ceza Hukukunun Sınırları (Çev: Feridun YENİSEY), in: Alman Ceza Hukukuna Giriş, İstanbul, 2007, sh: 173.

²⁴ **HILGENDORF**, Eric, Strafrechtliche Produzentenhaftung in der "Rizikogesellschaft", Berlin, 1993, sh: 17.

²⁵ **İÇEL**, Kayıhan/**DONAY**, Süheyl, Karşılaştırmalı ve Uygulamalı Ceza Hukuku – Genel Kısım - , 4. Baskı, İstanbul, 2005, sh: 4; **ÖZTÜRK/ ERDEM**, Uygulamalı Ceza Hukuku ve Güvenlik Tedbirleri Hukuku, 9. Baskı, Ankara, 2006, sh:32-33; **WESSELS**, Johannes, Strafrecht Allgemeiner Teil, 28. Auflage, Münster, 1996, sh:2; **GROPP**, Walter, Strafrecht Allgemeiner Teil, Leibzig, 1997, sh: 5 vd.

²⁶ **ÜNVER**, Hukuksal Değer, sh: 442.

Modern ceza hukuku anlayışının teknik olarak ortaya konulması ve internet suçluluğunun bu anlayış içindeki yerinin sabitlenmesi için ceza hukukunun tarihsel gelişim süreci içerisinde kat ettiği çizginin göz önünde bulundurulması gerekmektedir. Bu çerçevede “Klasik veya geleneksel ceza hukuku” olarak tanımlanan ceza hukuku anlayışının uğradığı dönüşümün neticesi olarak modern ceza hukuku anlayışı²⁷ mutlak suretle klasik ceza hukuku anlayışı ile birlikte düşünülmeli ve tartışılmalıdır²⁸. Başka bir ifade ile; klasik ceza hukukunun temel özelliklerini dikkate almadan ve söz konusu dönüşümü karşılaştırmalı olarak ortaya koymadan modern ceza hukuku anlayışının bugün geldiği nokta üzerinden, modern toplumun belirleyici aracı niteliğindeki internet ekseninde şekillenen bir suçluluk alanını çözümlenmek güçtür. Öyle ki böyle bir tercih internet suçluluğuna ilişkin düzenlemelerin arkasındaki kanun koyucu inisiyatifinin yorumlanması bakımından da anlamlı olacaktır.

1.2.- Klasik Ceza Hukuku Anlayışının Temel Özellikleri

1.2.1.- Genel Olarak

Klasik ceza hukuku anlayışının temeli 18. yüzyıl aydınlanma felsefesi ile birlikte ortaya çıkan yenilik hareketlerine dayanmaktadır. Aydınlanma çağı felsefecileri Ortaçağın Skolastizminin etkisi altında kalan tanrısal iradenin yansıması olarak dinsel ve otoriter ceza hukuku anlayışını reddetmekte, irade hürriyetini temel kabul eden hümanist bir ceza hukuku anlayışının zorunlu olduğunu benimsemişlerdir. Böyle bir ceza hukuku anlayışını şekillendirebilmenin ilk adımı cezalandırma yetkisinin kaynağının değiştirilmesi olduğunu savunan aydınlanma dönemi düşünürleri Toplumsal Sözleşme teorisini kabul etmişlerdir.²⁹ Buna göre “toplum sözleşmesi ilkel dönemde doğanın ve güçlülerin saldırılarından korunmak için insanların birbirleriyle anlaşmasıyla oluşturulan ve böylece insanların bir arada barış içinde ve herkesin kendi haklarından yararlanabilmeleri hedefleyen bir sözleşmedir. Bu amaçla organize olan toplumlar her bireyin o toplumun üyesi olan diğer bireylerin haklarına riayet etmesini garanti etmek amacıyla devlet örgütlenmesine gidilmiştir. Devletin amacı toplum üyelerini toplumsal sözleşmeye uymalarını kontrol etmek ve yeni oluşturulan bu barış

²⁷ HONG, Flexibilisierungstendenzen, sh: 56.

²⁸ HONG, Flexibilisierungstendenzen, sh:57.

²⁹ Ayrıntılı bilgi için bkz. NAUCKE, Wolfgang, Über die Zerbrechlichkeit des rechtsstaatlichen Strafrecht, Baden- Baden, 2000, sh: 19 v.d.

*düzenini korumaktır. Bu amaç uyarınca bir kişinin eylemi toplumsal sözleşmeyle oluşturulan düzeni bozduğu takdirde ceza yaptırımına hükmedilecektir.”*³⁰

Buradan da anlaşılacağı üzere aydınlanma döneminde ortaya konulmaya çalışılan ceza hukuku anlayışının temelinde Ortaçağ Skolastizminin keyfi ve sınırları muğlâk ceza hukuku anlayışına standart, hümanizmi temele alan bir sınır getirmek kaygısının yattığı görülmektedir. Keza bu kaygı 1789 sonrası ağırlık kazanan Hukuk Devleti düşüncesiyle olgunlaşan ve Hukuk devletinin ceza hukukuna dair prensipleri olarak kabul edilen “Belirlilik, Kanunilik, Kusur, Şüpheden Sanık/Özgürlük Yararlanır (in dubio pro reo / libertate)³¹ Prensipleri”nin şekillenmesine zemin hazırlamıştır. *Dönmezer*, Fransız Devrimi’nin etkisi altında kalan klasik anlayışın, kişi hürriyet ve dokunulmazlığını hiçbir suretle tehlikeye düşürmeksizin toplumun savunulmasını bir ilke olarak ele aldığını kabul etmektedir³². *Hong ise*, Hukuk Devletinin Ceza Hukuku (*rechtsstaatliches Strafrecht*) olarak da adlandırılan bu sistemin unsurlarını kısaca şöyle maddelemiştir³³:

a- Kanunilik prensibine bağlıdır³⁴.

b- Genelin – Kamunun hukuksal değerlerinden ziyade bireyin hukuksal değerlerini korur.

c- Sadece açıkça gösterilmiş ve belirlenmiş suç unsurlarından oluşur.

d- Cezalandırma etkinliği ile doğrudan suçluyla mücadele edilmemeli, temel hedef suçlulukla mücadele olmalıdır.

e- Ceza hukukunun bir amacı hümanizmi muhafaza altına alınması adına devlet gücünü sınırlandırılmak iken, aynı zamanda bir başka amacı da ceza hukukunun etkinliğini/etkililiğini arttırmaktır.

³⁰ **ÜNVER**, Hukuksal Değer, sh: 169. Ayrıca konu ile ilgili ayrıntılı bilgi için bkz. **ÖZTÜRK/ ERDEM**, Uygulamalı Ceza Hukuku, sh: 55 v.d.

³¹ “Şüpheden sanık yararlanır (In dubio pro reo)” ve “Şüpheden özgürlük yararlanır (In dubio pro libertate) ilkeleri birbiriyle ilişkili olmakla birlikte farklı ilkelerdir. Ancak tekrardan kaçınmak amacıyla bu iki ilkenin aynı anda kullanılacağı yerlerde “Şüpheden Sanık/Özgürlük Yararlanır (in dubio pro reo / libertate)” şeklinde bir kullanım tercih edilmiştir.

³² **DÖNMEZER**, Genel Ceza Hukuku Dersleri, sh: 20.

³³ **HONG**, Flexibilisierungstendenzen, sh: 57.

³⁴ Kanunilik prensibinin tarihsel gelişimi ile ilgili bkz. **JESCHECK**, Hans Heinrich/ **WEIGEND**, Thamas, Lehrbuch des Strafrechts/ Allgemeiner Teil, 5. Auflage, Berlin, 1996, sh: 131-132.

Yukarıda aktarılan unsurlar göz önünde bulundurulduğunda klasik ceza hukuku anlayışında cezalandırma yetkisinin kaynağının toplum sözleşmesiyle devlete bırakıldığı ancak bu yetkinin devlet tarafından sınırsızca kullanılmasının önüne geçilmeye çalışıldığı görülmektedir. Bu gayretin temelinde Ortaçağ Skolastizminin tanrısal yetkiye dayanan yaklaşımının sınırsız ve ölçüsüz uygulamaları yatmaktadır. Aydınlanma Çağı ve Fransız Devrimi öncesinde de devletin korunması gerekçesi altında siyasi gücü elinde bulunduran Monark'ın korunmasına yönelik düzenleme ve uygulamaların yapılmış olduğunu ifade eden *Demirbaş'a* göre, bu devlet- birey ilişkisinin Aydınlanma felsefesinin etkisiyle değiştirilmesiyle insan birey olarak ele alınmış, onun ve onurunun korunması amacıyla kişi dokunulmazlığı ve güvenliği kavramı geliştirilmiş ve hatta yalnızca maddi ceza hukuku normları değil, ceza muhakemesi normları da bu yeni anlayış çerçevesinde şekillendirilmeye başlanmıştır³⁵. Ayrıca cezalandırmanın bir araç olarak suçluyla mücadele için kullanılmaması gerektiği yönündeki eğilim de aydınlanma ile birlikte ortaya çıkan hümanist yaklaşımın ceza hukukuna yansımış şekli olarak kabul etmek gerekir. Keza bu yaklaşım tarzı daha sonra "Fail Ceza Hukuku"nun yerine "Fiil Ceza Hukuku"nun benimsenmesi tercihinde de kendini göstermiştir.³⁶

Yine bireysel hukuksal değerlere özel önem atfedilmesi de bu anlayışın karakteristik özelliklerinden biri olarak dikkat çekmektedir. Ayrıca dikkate değer bir başka husus da söz konusu dönem itibariyle bireysel ölçekteki korunması hedeflenen hukuksal değerlerin ancak bir zarar neticesi doğurabilecek nitelikte eylemlere karşı güvenceye alınması durumudur. Dolayısıyla zarar suçları endeksli bir koruma alanından bahsedilmektedir. Böyle bir tercihin yapılmış olması anlaşılır bir gerekçeye dayanmaktadır. Şöyle ki; yukarıda bahsedilen Hukuk Devletin Ceza Hukukuna dair prensipleri yani Belirlilik, Kanunilik, Kusur, Ultima Ratio ve Şüpheden Sanık/Özgürlük Yaralanır (*in dubio pro reo / libertate*) prensiplerinin uygulanabilirliği bakımından zarar neticesi doğuran eylemler birebir uyumluluk göstermektedir. Dolayısıyla cezalandırılabilirlik alanı zarar neticesi doğuran eylemlerle belirlenmektedir. Bu bağlamda söz konusu ceza hukuku anlayışının şekillendiği dönemler itibariyle toplumsal ilişkiler günümüzde olduğu kadar karmaşık ve bir çok riski bünyesinde

³⁵ DEMİRBAŞ, Timur, Türk Ceza Hukukunda İşkence Suçu, Ankara, 1992, sh: 17.

³⁶ Fiil Ceza Hukuku ile Fail Ceza Hukuku arasındaki ilişki ve farklılıklar ile ilgili bkz. JESCHECK/WEIGEND, Lehrbuch , sh: 54.

barındıran bir yapıda değildir. Buna bağlı olarak da zarar suçları merkezinde şekillenen bir bakış açısından bahsetmek mümkündür.³⁷

1.2.2.- Winfried Hassemer ve Wolfgang Naucke'nin Değerlendirmeleri

Genel anlamda klasik ceza hukukunun çerçevesini çizdikten sonra, klasik ceza hukuku anlayışına yönelik olarak örnek olması anlamında *Winfried Hassemer* ve *Wolfgang Naucke'nin* değerlendirmelerine kısaca göz atmak isabetli olacaktır. Özellikle bu iki değerlendirmenin tercih edilmesinde, her iki yazarın da genel ceza hukuku teorisini süreçsel bir ilişki içerisinde anlamaya çalışmaları etkili olmuştur. Zaten modern ceza hukuku anlayışına giden yolun öncelikle klasik ceza hukuku formlarını anlamaktan geçtiği düşünülecek olursa, ceza hukukunun tarihsel gelişim süreci içerisindeki seyrinin göz önünde bulundurulması elzemdir.

Hassemer, devletsel ceza hukukunu tarihsel gelişim süreci içerisinde üç ayrı kategori bağlamında ele almaktadır³⁸. Bunlardan ilki 18. y.y.a kadar geçen sürede farklı görünümde dahi olsa hakimiyetini gösteren doğal hukuk eksenli bir ceza hukuku konseptidir. Yazar bu konsept içerisinde özellikle Orta Çağ Avrupa'sında doğal hukuk anlayışının yaşadığı dönüşüme paralel olarak, kilise merkezli tanrısal egemenlik anlayışının etkili olduğu kanaatini taşımaktadır. Bu dönemde egemen ceza hukukunu, toplumsal ve yönetsel düzenin sağlanması için tek taraflı, kontrol mekanizmalarının işlemediği ve devletsel uygulamalar bakımından keyfilik riskinin kendini ciddi bir biçimde gösterdiği bir güvenlik düşüncesinin etkili bir aracı olarak kabul etmiştir. Aydınlanma dönemine kadar devam eden bu yaklaşım, Aydınlanma Felsefesinin de etkisiyle çok köklü değişikliklere uğramıştır³⁹. Öyle ki bu değişim, devletsel ceza hukukunun yeni bir aşamasının da habercisi niteliğindedir.

Yazara göre ceza hukuku gelişim sürecinin ikinci aşamasında ise; öncelikle doğal hukukun ceza hukukuna ilişkin ilke ve yasakların bir kaynağı olarak kabul edilmesinden vazgeçilmiş, genel bağlamda hukuk özel bağlamda ise ceza hukuku için başka bir nokta

³⁷ HASSEMER, Winfried, Kennzeichnen und Risiken des Modernen Strafrechts, in ZRP, H: 10, 1992, sh: 381.

³⁸ KIM, Jae- Yoon, Umweltstrafrecht in der Risikogesellschaft – Ein Beitrag zum Umgang mit den abstragten Gefährungsdelikten, sh: 49 (Kaynak: http://books.google.com.tr/books?id=G_8M3G7SvWQC&pg=PA52&dq=modernes+Strafrecht&hl=de#PPA53_M1 , Erişim Tarihi: 10.01.2009, Saat:16:00).

³⁹ KIM, Umweltstrafrecht, sh: 49.

üzerinden hareket edilmeye başlanmıştır. Bu hareket noktası Toplum Sözleşmesi tasarımıdır⁴⁰. *Hassemer*, bu dönemde herkes için özgürlükçü bir toplum modelinin oluşturulmasında, eşitlik ve karşılıklılık prensipleri rehberliğinde tüm yurttaşların üzerinde mutabık kaldıkları bir sözleşmeden bahsetmekte ve sosyal sözleşme etrafında birleşen kişilerin insan odaklı bir ceza hukuku konseptine yöneldiklerini ifade etmektedir. Bu konseptin temel dayanak noktaları ise bir taraftan toplumsal sorunların çözümünde ceza hukuku normlarının başka hiçbir imkan söz konusu olmadığı konumda son araç olarak kullanılmaları (*ultima ratio*) ve diğer taraftan mevcut ceza hukuku normlarının özellikle bireysel hukuksal değerlerin korunmasına hizmet etmeleri yönünde bir yoğunlaşmadır⁴¹. İşte bu ikinci dönemde oluşan ceza hukuku anlayışı bugün klasik ceza hukuku olarak kabul gören anlayışın kendisidir. Dolayısıyla modern ceza hukuku anlayışının temelleri incelenirken Aydınlanmayla ortaya çıkan ve 18. – 19. y.y.’larda etkisini gösteren idealist felsefenin göz önünde bulundurulması gerekmektedir.

Wofgang Naucke'nin ise nispeten *Hassemer* ile paralel bir değerlendirme ortaya koyduğunu söylemek mümkündür. Yazara göre 18. y.y.a kadar geçen sürede ceza hukuku devletin mutlak hakimiyeti altında kötüye kullanılan bir zorbalık aracıdır. 18. y.y.ın ikinci yarısından itibaren hareketlilik kazanan hukuk felsefesi tartışmaları nihayetinde, ceza hukukunun bu karakterinin değişmesinin bir zorunluluk olduğu düşüncesi hakim olmaya başlamıştır⁴². Çünkü ceza hukukunun amacı içerisinde, sadece kişilerin birbirlerine karşı güvenliği tehdit edici nitelikte eylemlerinin önlenmesi amacıyla değil bizzat devletin ve hatta bu kuralları koyanların da benzer nitelikteki eylemlerinin de göz önünde bulundurulması gerektiği de yer alması gerekmektedir. Bu bağlamda Aydınlanma dönemiyle birlikte, bir hukuk devletinde ceza hukukunun bireylerin ve devletin gerçekleştirdikleri suç teşkil eden eylemlere karşı tesis edilen ve cezai müeyyide içeren kurallar bütünü olduğu kabul edilmiştir⁴³.

Ancak yazar burada ceza hukuku tanımlanırken esas kabul edilen “suç” kavramının dar anlamda ele alındığını ifade etmektedir. Dolayısıyla klasik ceza hukuku anlayışı çerçevesinde, ceza hukuku özgürlük ihlaline karşı sıkı bir cezalandırıcı reaksiyon temelinde kavranmış

⁴⁰ **KIM**, Umweltstrafrecht, sh:49.

⁴¹ **KIM**, Umweltstrafrecht, sh:49.

⁴² **KIM**, Umweltstrafrecht, sh:50.

⁴³ **KIM**, Umweltstrafrecht, sh:50.

ancak, 19. y.y.dan itibaren deęişen ve dönüşen toplum yapısına baęlı olarak klasik ceza hukuku anlayışının ortaya koyduęu ilke ve güvenceler yetersizleşmiş ve özellikle siyasetin hukuk üzerindeki etkisini arttırmasıyla ceza hukuku özgürlük güvencesi mutlak amacını gerçekleştiren sınırlı bir araç olmaktan çıkıp her türlü politik amacı gerçekleştirmeye elverişli sınırsız bir araca dönüşme riskiyle karşı karşıya kalmıştır⁴⁴. *Naucke*, bu sürecin sonucu olarak, hukuk devletinin ceza hukuku şeklinde tabir ettięi klasik ceza hukukundan oldukça farklı bir ceza hukukunun kendini gösterdiğini kabul etmiştir. Öyle ki *Naucke* bir adım daha ileri giderek, klasik yani hukuk devletinin ceza hukukunun çağının kapandığını ifade etmiştir.

1.3.- Klasik Ceza Hukuku Anlayışından Modern Ceza Hukuku Anlayışına Geçiş

Klasik ceza hukuku anlayışını genel çerçevesiyle ortaya koyduktan sonra, modern ceza hukuku anlayışına yönelen çizgiyi isabetli tespit edebilmek için klasik ceza hukuku anlayışından modern ceza hukuku anlayışına geçişin alt yapısını da oluşturmak gerekecektir.

Tarihsel arka planı ile birlikte genel çerçevesi çizilen klasik ceza hukuku yaklaşımı özellikle 19. y.y. başlarından itibaren şekillenen dünyada sosyal, ekonomik ve siyasi ilişkilerin dönüşüme uğraması, ülkeler arasındaki ilişkilerin yoğunluk kazanması, bilim ve teknolojideki gelişmelerin toplumu doğrudan ve birinci derecede etkilemeye başlaması ve buna baęlı olarak da toplumsal yapılanmanın endüstri devrimiyle şekillenen yapısının yeniden anlamlandırılmaya çalışılması ile bir dönüşüm süreci içerisine girmiştir. Nitekim bu sürecin, toplumsal yaşamın tüm yapılarını etkiledięi gibi toplumsal bütünlüğün ve sürekliliğin kaynaęı / güvencesi olan hukuku , bilhassa da ceza hukukunu yakından etkilemeyi doğaldır. Çünkü bilindięi gibi ceza hukuku temel olarak “hukuksal deęer” kavramı etrafında şekillenmekte ve toplumsal yaşamda gerçekleşen bu gibi köklü deęişiklikler de yeni hukuksal deęerlerin ortaya çıkmasına vesile olmaktadır.⁴⁵

Farklı bir anlatımla sosyo-ekonomik gelişim çizgisinin tarihsel süreç içindeki seyri dikkate alındığında (ilkel toplumdan tarım toplumuna, tarım toplumundan endüstri toplumuna, günümüzde ise endüstri toplumundan bilgi toplumuna geçiş) her toplum

⁴⁴ **KIM**, Umweltstrafrecht, sh:50.

⁴⁵ Hukuksal deęerlerin üretimi ve oluşumu ile ilgili ayrıntılı bilgi için bkz. **ÜNVER**, Hukuksal Deęer, sh: 470 vd. ; **ÜNVER**, Yener, TCK ve Ceza Kanunu Tasarısı'nın İnternet Açısından Deęerlendirilmesi, in: İÜHFİM, C: XIII, S: 1-2, 2001, sh: 56- 57.

modelinin, içinde buldukları dönemin niteliklerine bağlı olarak (tarım devrimi tarım toplumunu, endüstri devrimi endüstri toplumunu ve nihayet bilgi - bilişim devrimi bilgi - bilişim toplumunu şekillendirdiği gibi) şekillendikleri görülmektedir. Bu da; her dönemde gerçekleşen köklü değişikliklerine paralel olarak o toplumun, başta hukuksal değer tercihleri olmak üzere, temel dinamiklerinde yeni anlam içeriklerinin ortaya çıkmasına sebebiyet vermektedir⁴⁶.

Modern toplum olarak ifade edilen bilgi toplumunun aynı zamanda risk toplumu olduğu kabulünden hareketle, klasik ceza hukuku normlarının ve yapılarının yeniden gözden geçirilmesi ihtiyacı, bugün modern ceza hukuku anlayışı olarak ifade edilen yaklaşım tarzının kapısını aralamıştır. *Ünver'e* göre, bir risk toplumu haline gelen, endüstri, sanayi, tıp, nükleer ve atom bilimleri, uzay araştırmaları, yeni gen teknolojisi metotları, çevre ve ekonomik alan bakımından oldukça ileri bir düzeye gelen toplumlarda, bu alanlardaki gelişmelerden ve hukuksal değerlerden bireysel veya toplumsal yararlanmalar kanun koyucuları klasik ceza hukuku normları kurumlarında değişiklikler yapmaya zorlamaktadır. Bazı yeni suç tipleri ve ceza yaptırımları ile diğer ceza kurumlarının kabulü ve düzenlenmesi veya mevcut düzenlemelerin tamamen veya kısmen ortadan kaldırılması faaliyetlerinin yanında modern risk toplumunun yaşama şekli ve yapısına uygun davranış modellerini saptamak,, bu tespitleri rasyonel olmayan metafizik gerekçelendirmeler yerine rasyonel, amaca uygun ve hukuksal değerlerin korunması ilke ve ölçütlerine dayandırmak gerekmektedir⁴⁷.

Aynı şekilde *Mylonopoulos* 19. yüzyıl ceza hukuku düzenlerine nazaran günümüzde ortaya çıkan yeni hukuksal değerlerin doğasının farklılık arz ettiğine değinirken⁴⁸, *Bustos* da suç yapılarındaki yaşanan değişikliğe dikkat çekmiştir. *Bustos* bu tespitine örnek olarak uyuşturucu madde kullanmak, arenalarda cebir şiddet uygulamak, aile içinde cebir şiddet

⁴⁶ *Sieber* bu gelişim ve dönüşüm sürecinin, bizim de katıldığımız gibi, ceza hukukuna etkisini tartışırken özellikle toplumsal yapının özelliklerine dikkat etmiştir. *Sieber'e* göre günümüzde “dünya toplumu”, “bilgi toplumu” ve risk toplumu” sosyal açıdan büyük bir hızla değişmektedir. Bu değişiklikler, suçluluğun artmasına ceza hukukunda ve suç siyaseti alanında ağır sonuçlar doğmasına ve şimdi, ceza hukuku alanındaki “ önleme düşüncelerinin ön plana çıkmasından da anlaşılacağı gibi, temel ilkelerin değişmesine yol açmaktadır. Bu değişiklik, günümüzde sadece Avrupa Ceza Hukuku ve Devletler Ceza Hukuku alanında, uluslar arası adli yardımlaşmada yeni yapılanmaya gidilmesi ve devletler üstü bir ceza hukuku oluşması şeklinde değildir. Daha köklü değişiklikler, terörle mücadele açısından klasik yaklaşımı yansıtan siyasi ve hukuki yöntemlerin terk edilmesi biçiminde görülmektedir; bunun gibi, eskiden beri yapılmış olan iç ve dış güvenlik, savaş ve suç, istihbarat teşkilatları ve polis, polis ve asker ile, savaş ve barış kavramlarının içi yeniden oluşturulmaktadır. Ayrıntılı değerlendirme için bkz. **SIEBER**, Ceza Hukukunun Sınırları, sh: 173-174.

⁴⁷ **ÜNVER**, Hukuksal Değer, sh:500.

⁴⁸ **ÜNVER**, Yener, Uluslar arası Bir Ceza Hukuku Sempozyumundan Notlar, in KHuKA -7, 2000, sh: 163'den naklen.

kullanmak, iaşe yükümlülüğünü yerine getirmemek ve ırza tasaddi eylemlerini göstererek, bunların bir kısmının daha önceleri hazırlık hareketi sayıldığı ve yalnızca belirli şekillerinin cezalandırıldığını, bugün ise aynı eylemlerin (yaratılan suç tipleri dolayısıyla) icra hareketleri niteliğinde sayıldığına işaret etmiştir. Buna paralel başka bir gelişmenin suç ortaklığı (iştirak) alanında olduğuna dikkat çeken yazar, daha önceden bir yağma eyleminde kullanılacağını bilerek bir silahı satan kişinin eylemi müzaheret ve muavenette bulunmak olarak sayılmayıp, bir toplumda olması olağan karşılanan riskli hareket sayılırken, bugün aynı eylemlerin ceza hukuku sonuçlarındaki genişleme düşüncesi dolayısıyla, suç ortaklığı kapsamında cezalandırıldığını belirtmiştir⁴⁹. İşte bu perspektiften yaklaşıldığında klasik ceza hukuku anlayışının gelişen toplum düzeninin ihtiyaçlarını karşılamakta yetersiz kaldığı ve bu anlayışın hakim olduğu sistemlerde değişim gerekli olduğu gözlemlenmektedir. Bu gereklilik de modern ceza hukuku anlayışının yolunu hazırlamaktadır.

1.4.- Modern Ceza Hukuku Anlayışının Belirleyici Özellikleri

1.4.1.- Küreselleşme ve Ceza Hukukuna Etkisi

Küreselleşme; ekonomik, sosyal, teknolojik, kültürel, politik ve ekolojik açılardan global bütünleşmenin, entegrasyon ve dayanışmanın artması anlamına gelmektedir.⁵⁰ Küreselleşme olgusu klasik ceza hukuku düşüncesinin geçirmekte olduğu evrimin en kilit noktalarından biridir. Özellikle ulus devlet anlayışının egemen olduğu bir dönemde şekillenen Klasik Ceza Hukuku özellikle 20.yy. ikinci yarısına kadar geçen sürede tüm etkinliğini ulusal sınırlar içinde göstermekteydi. Bu nedenle ceza hukukuyla korunması amaçlanan hukuksal değerler yalnızca söz konusu devlet sınırları içerisinde yaşayan insanların oluşturduğu toplumsal yapının gereksinimlerine göre şekillenmekteydi. Bununla birlikte cezalandırma yetkisi mutlak bir şekilde söz konusu devlete bırakılmıştı. Fakat 20. yy. ikinci yarısından sonra bilişim – iletişim teknolojilerindeki gelişmeler, sermayenin serbest dolaşımını mümkün kılacak yasal düzenlemelerin artması, ulaşım imkanlarının kolaylaşması gibi etkenlerle

⁴⁹ ÜNVER, Sempozyum Notları, sh: 156'dan naklen.

⁵⁰ Bkz. <http://tr.wikipedia.org/wiki/K%C3%BCreselle%C5%9Fme> (Erişim Tarihi: 18.09.2007, Saat: 14:00).

birlikte resmi olarak muhafaza edilmekte olan sınırlar fiili olarak yavaş yavaş ortadan kalkmaya başlamıştır.⁵¹

Küreselleşme olgusunun hukuk ve özellikle ceza hukuku sisteminde ne tür değişikliklere yol açtığı üzerinde duran *Bergalli* 19. yüzyıl ile 20. yüzyılın ilk yarısındaki ceza hukukunun dayandığı ve devlet gücüne sınırsız olanak tanıyan devlet ve sivil toplum arasındaki ilişkinin, küreselleşmeyle zayıflayıp çözülmeye yüz tuttuğunu belirtmiştir. Bunun beraberinde devletin ceza koyma gücünün sınırlanması ve kontrolü anlayışını getirdiğini belirten yazar, bu kontrolün özellikle organize suçluluk ve bilgilenme alanlarında başladığını ifade etmiştir. Hemen akabinde 70'li yıllarda devletlerin terör eylemlerine tepki olarak yaptığı düzenlemelere değinen yazar, ceza hukukunun hümanist, ıslah edici ceza hukuku eğiliminin sekteye uğradığını, ceza normlarının meşruluğunun denetimi ve orantılılık ilkeleri gibi ilkelerin geri plana atıldığını ifade ederek, toplumların o dönem açısından yaşadığı şaşkınlık dolayısıyla ölüm cezası, uygulaması, hürriyeti bağlayıcı cezaların ağırlaştırılması, polisin ağır ve sert metotlar uygulamasının talep edildiğine ve bir ölçüde uygulamaya geçirildiğine değinmiştir.⁵²

Yine risk toplumunun özelliklerine dikkat çeken *Donna*, hukuksal değerlerin korunması ve gelecek açısından güvenceler için hukuksal araçların gözden geçirilmesi gerektiğine işaret ederek, 21. yüzyılın sorunlarının 19. yüzyılın araçlarıyla çözümlenemeyeceğini belirtmiştir. Küreselleşme sürecine ve devletsel kurumlardaki yolsuzlukların artışına değinen yazar, organize suçluluğun da yapı değiştirdiğini, artık lokal bir sorun olmadığını, yönetimlerden bağımsız olarak toplumun ekonomik kurumlarına ve demokratik sisteme olumsuz müdahalelerde bulunduğunu belirtmiştir. Gelişmekte olan ülkeler ile küreselleşmeyi yeterince özümsemeyen, devletin gücünün azaldığı ve yolsuzluklar nedeniyle idaresi oldukça zayıflayan devletlerin durumlarının içinde bulunduğu koşullara değinen *Donna*, bu tür sorunlar arttığında liberal ceza hukuku anlayışının gözden kaçırıldığını, cezaların artırılmasına, infaz alanında yeni düzenlemelere girişildiğini ve ceza muhakemesi ve ceza hukuku güvencelerinin ortadan kaldırıldığını ve bunun da bazı Güney Amerika ülkelerinde olduğu gibi totaliter devlet yapılarının sayısında artışa neden olduğunu belirtmiştir.⁵³

⁵¹ Konu ile ilgili detaylı tartışmalar için bkz. **VEC**, Milos, Internet, Internationalisierung und nationalstatlichen Rechtsgüterschutz, in: NJW 2002, H. 21, sh: 1535; **KOCH**, Arnd, Nationales Strafrecht und globale Internet – Kriminalität, in: GA, 2002, sh: 703.

⁵² **ÜNVER**, Sempozyum Notları, sh: 158den naklen.

⁵³ **ÜNVER**, Sempozyum Notları, sh: 175'den naklen.

Küreselleşmenin belki de en etkili neticesinin alındığı alanlardan biri bilişim – iletişim teknolojilerinin en yaygını olan internettir⁵⁴. İnternetin sağladığı sanal paylaşım ortamı ile sınırlar ortadan kalkmakta ve 21. yüzyılın temel kaynağı olan bilginin her türüne rahatlıkla ulaşılabilmektedir⁵⁵.

Bu sanal ortam, dünyanın dört bir tarafındaki insanları coğrafi sınırlar ve tabiiyet unsuru söz konusu olmaksızın bir araya getirmekte ve bu insanların kendi tespit edecekleri çerçevede ortak paylaşım alanlarında iletişime geçmeleri, bilgi alış verişinde bulunmalarına imkan vermektedir. Hatta bu durumun yeni bir yapılanmaya sebebiyet verdiği ve sanal alem üzerinden küresel bir köy tasarımının olduğu kabul görmektedir. Bu yapılanmaya “*Küresel Köy*” denilmesinin nedeni de, kullanıcıların bu ortamda mesafeleri tanmaksızın bir arada bulunmaları, sanal dünyanın kendi kültürünü, kendi dilini ve değer sistemini oluşturmasıdır. Söz konusu köyün sakinleri de kendine has özellik ve değer tercihleriyle “*(inter)net halkı (net citizen, netizen)*” şeklinde kategorize edilebilmektedir.⁵⁶

Bu örnek üzerinden küreselleşme olgusunun ceza hukuku bakımından önemi birkaç madde ile özetlenecek olursa;

i.- Öncelikle sınırların nispeten veya tamamen kalktığı ve global bütünleşmenin gerçekleştiği bir ortamda ulusal sınırlarla çerçevesi belirlenmiş bir ceza hukuku anlayışının değişikliğe uğraması kaçınılmazdır. Çünkü artık ceza hukukunun merkezi kavramı olan hukuksal değer kavramı ulusal ölçekte değil küresel ölçekte dikkate alınmalı, buna bağlı olarak da ulusal nitelikli mikro çerçevede bir hukuksal değer koruması değil evrensel nitelikli

⁵⁴ “Özellikle 20. y.y’ın son çeyreğinde yaşanan gelişmeler dünyada önemli değişimlere yol açmaktadır. Bilişim ve iletişim teknolojilerinde gerçekleşen bir dizi baş döndürücü buluşlar bilginin neredeyse sınırsız dolaşımını ve etkileşimini mümkün kılmakta ve dünyayı adeta küresel köy haline getirmektedir. Televizyon, bilgisayar ve internet alanındaki teknolojik atılımlar sayesinde insanlar artık farklı bilgi kaynaklarına ulaşabilmekte ve dünyanın dört bir köşesindeki insanlarla iletişim içine girmektedirler. Bilgi ve haber kaynaklarına ulaşma konusunda ulus devletlerin her türlü sınırlamaları aşılabilmekte ve böylelikle devletlerin bilgi tekelleri kırılmaktadır. Bu süreç daha önceleri kendilerini tanımlamada ve ifade etmekte güçlük çeken çeşitli kültürel grupları hareketlendirmektedir. Özellikle ulus devletlerin tanımadıkları ve/veya asimile etmeye çalıştıkları bu grupların dış dünya ile etkileşimi artmakta ve kendilerini içeride ve dışarıda ifade etmeleri kolaylaşmaktadır. Böylece ulus devleti oluşturan çeşitli toplulukların örgütlenmeleri ve bu doğrultudaki taleplerini dillendirebilmeleri daha kolaylaşmaktadır. Aynı bu topluluklar ulus devletin bakışına karşı kendilerini uluslar arası arenada kolay destekçiler bulabilmektedirler.” **İŞİK**, a.g.m., sh: 185.

⁵⁵ **KÖKSAL**, Aydın, Bilişim Toplumu, in: TBA, İstanbul, 2007, sh: 252.

⁵⁶ **ÇELİK**, Tolga/ **KARAASLAN**, Enis, İnternet Toplumu Oluşum Süreci, <http://inet-tr.org.tr/inetconf9/bildiri/45.doc> (Erişim Tarihi: 18.09.2007, Saat: 14:10).

makro düzeyde bir hukuksal değer koruması esas alınmalıdır.⁵⁷ Bu duruma örnek olarak internet aracılığıyla işlenen suçlar, çocuk pornografisi, terörizm ve organize suçlulukla mücadele, uyuşturucu ve silah kaçakçılığı, çevre suçları gibi alanlar gösterilebilir.⁵⁸ Bu tür alanlara ilişkin devletin en etkin mücadele aracı olan ceza hukuku düzenlemeleri, uluslar arası ve/veya ulusal üstü girişimlerle ortak çalışmalarla hazırlanıp taraf olan tüm ülkeleri kapsar nitelikte şekillendirilmektedir⁵⁹.

ii.- Bu yönde bir eğilim aynı zamanda modern dünyada suç ve suçlu ile mücadele açısından da önemli bir gerekeciyi bünyesinde barındırmaktadır. Şöyle ki; suç teşkil eden anılan eylemlerin artık ulusal sınırlar söz konusu olmaksızın dünyanın her bir köşesinden her bir köşesine yönlendirilebilir olması, gerek münferit devletlerin gerekse uluslar arası yapılanmaların suç ve suçlu kaynaklarına yönelik soruşturma ve kovuşturma imkanlarını kısıtlamaktadır⁶⁰. Özellikle halihazırda ülkelerin iç hukuklarında hem suç tasnifleri hem de usul kuralları bakımından bir yeknesaklığa gidilememiş olması, uluslar arası düzlemde suçluların iadesi konusunda halen problemlili alanların⁶¹ mevcudiyeti bunun en önemli göstergesidir. Böyle bir durumda zarar neticesinin doğmasını beklemek ciddi bir riski bünyesinde barındırır. Başka bir ifade ile artık suç teşkil eden bir eylemin gerçekleşmesinden sonra yürütülecek soruşturma ve kovuşturma işlemleriyle elde edilen

⁵⁷ **HILGENDORF**, Eric, Nationales oder transnationales Strafrecht? Europäische Strafrecht, Völkerstrafrecht und Weltgrundsatz im Zeitalter der Globalisierung, in: Raum und Recht , Festschrift für 600 Jahre Würzburger Juristischen fakultät (Der: Horst DREIER, Hans FORKEL, Klaus LAUBENTHAL), Berlin, 2002, sh: 338 – 339.

⁵⁸ Sınır aşan suçlar (*transnationle Delikte*) ilişkin detaylı katalog ve Avrupa Ceza Hukukunun bu suçlara bakış açısına yönelik değerlendirmeler için bkz. **HECKER**, Bernd, Europäisches Strafrecht als Antwort auf transnationale Kriminalität?, in: JA , H. 8/9, 2002, sh: 724 v.d.

⁵⁹ Modern ceza hukukunun gelişim ekseninin risk kavramı üzerinde şekillendiği anlayışından hareket eden *Sieber*, bu yaklaşımını şöyle dile getirmektedir: “Günümüzdeki toplumsal değişiklikler, tek bir başlık altında toplanabilir: “Dünya, risk altında yaşayan bir toplum” haline gelmiştir. Bu kavramın arkasında, her biri diğeri ile sıkı bir şekilde bağlantılı olan “dünya toplumu (Weltgesellschaft)”, “bilgi, veri toplumu (Informationsgesellschaft)” ve “risk toplumu (Risikogesellschaft)” vardır. Yukarıda ana yatlarıyla açıklanan sosyal değişiklikler içinden, suçluluğun artmasını ve ceza hukukundaki değişikliği tetikleyen birbirlerini karşılıklı olarak ve olumsuz yönde güçlendiren, iki temel gelişme yönü, özellikle önemlidir.

1- Küreselleşme olgusu, sınır aşan suçların işlenmesi için yeni olanaklar sağlamakta ve ceza hukukunu ülkesel sınırlarını zorlamakta ve “transnasyonal etkili” yeni bir ceza hukuku modeli oluşmasına neden olmaktadır.

2- “Bilgi toplumu” ve “risk altında yaşayan toplumdaki” gelişmeler, yeni riskler ve karmaşık yapıda bir suçluluk tipi doğurmuştur. Bu durum, dünya suç siyasetinin giderek daha da küreselleşmesine neden olmuş, ceza hukukunun yerine getirmesi gereken bir görev olan, toplumun ve birey özgürlüklerinin korunması açısından, onun yapısal sınırlarını zorlamış ve yeni tip sorunlar doğurmuştur.” **SIEBER**, Ceza Hukukunun Sınırları, sh: 175.

⁶⁰ **PRADEL**, Jean, Ceza Hukukunun Küreselleşmesi: Beklentiler ve Perspektifler (Çev: Zeynel T. KANGAL), in: MHB, Y: 24, S:1-2, İstanbul, 2004, sh: 823 vd.

⁶¹ Suçluların iadesi ile ilgili bkz. **KÖPRÜLÜ**, Timuçin, Yeni Türk Ceza Hukuku’nda Suçlu ve Sanıkların Geri Verilmesi, in: HPD, C: 4, 2005, sh: 221 v.d.

muhtemel netice toplumsal barış, huzur ve güvenliği yeniden tesis etmeye elverişli olmayabilecektir. Bu nedenle artık ceza hukukunun önleyici fonksiyonu daha da ön plana çıkarılarak bu risk bertaraf edilmeye çalışılmaktadır.⁶² Çünkü bu eğilimin taraftarlarınca artık suçun işlenmesini engellemek gerçekleşen bir suçun neticesi ortadan kaldırmaktan daha kolaydır ve etkili çözümler getirir. Dolayısıyla ceza hukuku artık önleyici bir fonksiyon ile suç teşkil eden eylem riskinin varlığı öncelikli kabul etmektedir.⁶³

iii.- Her iki netice birlikte dikkate alındığı takdirde artık ceza hukukunun zarar suçları endeksli sistematiği bir dönüşüme uğramakta ve zarar suçları ağırlıklı sistem her geçen gün sayısını arttıran tehlike suçlarıyla tanımlanmaya başlamaktadır.⁶⁴ Bunun sebebi de modern dünyanın “anonimleşen” riskleri karşısında devletlerin egemenlik sınırları gereği ancak iç hukuklarında gerekli tedbirleri alabilmeleri ve fakat bunun suçlulukla mücadelede etkin sonuçları doğurmaması, müdahale alanını sınırlı kaldığı bir ortamda risklerin toplumsal yaşantıyı tehdit edecek boyutta güvenlik zafiyetlerine neden olması ve her geçen gün yeni suç işleme tekniklerinin artış göstermesi ister istemez ceza hukukunun önleyici fonksiyonunu ön plana çıkarmaktadır.⁶⁵ Buna bağlı olarak da devletler konsantrasyonlarını zarar neticesi doğuran eylemlerden ziyade bizatihi bu neticenin doğma tehlikesine yönlendirilmişlerdir. Çünkü böyle bir yönelim mantıksal olarak zarar neticesi doğuracak eylemin kendisini de evleviyetle kapsamaktadır. Böylece hem neticenin kendisi hem de bu neticenin gerçekleşme tehlikesi ceza hukuku alanına alınarak olabilecek maksimum güvenlik ortamının sağlanacağı kabul edilmektedir⁶⁶.

1.4.2.- Cezalandırılabilirliğin Öne Çekilmesi

Modern ceza hukuku anlayışının, özellikle son yıllarda sıkça tartışılan “Risk Ceza Hukuku”nun etkisiyle, klasik ceza hukuku anlayışının zarar suçları ve bunların korudukları hukuksal değer odaklı yaklaşımından ayrıldığı gözlemlenmektedir⁶⁷. Bunun nedeni de ceza

⁶² Konu ile ilgili ayrıntılı değerlendirme için bkz. **HASSEMER**, Winfried, Staat, Sicherheit und Information, http://www.alfred-buellesbach.de/PDF/21_Hassemer_Staat.pdf (Erişim Tarihi: 18.09.2007, Saat: 14:44)

⁶³ **HONG**, Flexibilisierungstendenzen, sh: 66- 67.

⁶⁴ **ÜNVER**, Hukuksal Değer, sh: 946.

⁶⁵ **HONG**, Flexibilisierungstendenzen, sh: 63.

⁶⁶ **HILGENDORF**, Strafrechtliche, sh: 44.

⁶⁷ **ÜNVER**, Hukuksal Değer, sh: 946.

hukukunda önleme fonksiyonunun çağın ihtiyaçları karşısında daha ön plana çıkmasıdır⁶⁸. Çünkü (yukarıda örnekleri de arz edilen) modern toplum risklerinin kontrol edilemezliği durumu hem bireysel hem de toplumsal bazda telafisi güç veya imkansız zararların doğmasına neden olmakta, böylece toplumsal bir alt sistem olarak (*gesellschaftliches Subsystem*) ceza hukukunun foksiyonel etkisi azalmaktadır.⁶⁹

Prittwitz bu tespiti çevre ceza hukukundan bir örnekle somutlaştırmakta⁷⁰, çevreye verilen zararların ve çevre tahribatına neden olabilecek etkenlerin artış göstermesi, buna bağlı olarak çevrenin korunmasının daha önemli bir hale gelmesi ile önleme fonksiyonunu ön plana çıkararak artık sadece çevreye zarar veren davranışların değil bilakis bu tehlikeyi içeren davranışların da kontrol altında tutulması gerektiğini ortaya koymaktadır.⁷¹ Bu da klasik anlamda zarar suçları ile belirlenen cezalandırılabilirlik alanının zararın meydana gelmesi tehlikesini de kapsar nitelikte öne çekilmesi sonucunu doğurmaktadır. Daha açık bir ifadeyle böyle bir ceza hukuku anlayışında tehlike suçları daha da önem kazanır hale gelmektedir.⁷²

⁶⁸ *Sieber* bu durumu modern toplumun risklerine karşı geliştirilen bir reaksiyon olarak kabul etmektedir. Detaylı açıklama için bkz. **SIEBER**, Ceza Hukukunun Sınırları, sh: 194 v.d.

⁶⁹ **PRITTWITZ**, Cornelius, Risiken des Risikostrafrechts, in: Konstruktion der Wirklichkeit durch kriminalität und Strafe (Der:Detlev FREHSEE, Gabi LÖSPER, Gerlinda SMAUS), Baden – Baden, 1994, sh: 52.

⁷⁰ *Prittwitz'in* bu tespitini *Özcan'da* isabetli bir şekilde ortaya koymuştur. Yazara göre, tarihsel süreç içerisinde değerlendirildiğinde doğa ve insan arasındaki dengenin esas bozulma anının endüstri devrimine denk geldiği görülür. O zamana kadar geçim kaynağı olan doğal kaynaklar, o dönemden sonra ekonomik gelişme ve büyüme şekli haline gelmiştir. Endüstrileşme ile birlikte, daha önce olmayan çevre tehditleri ortaya çıkmıştır. Bu dönemde çevre ye karşı yapılan ihlallerin çeşitlendiği ve arttığı görülür. Endüstrileşme, tesadüfi ve bireysel olarak işlenen ekolojik suçluluk çeşidinden, profesyonel bir şekilde ve her gün işlenen yeni ekolojik suçluluk çeşidinin ortaya çıkmasına neden olmuştur. 1960'lı yılların sonunda iki önemli gelişme insanlarda daha güçlü bir çevre bilincinin ortaya çıkmasını sağlamıştır. Bunlardan biri, büyük felaketlere yol açan çevre kazalarının meydana gelmesidir. Diğeri ise bilim adamlarının çevrenin görünmeyen zararlarını bilimsel olarak ortaya koyması sonucunda, insan neslinin ve dünyanın geleceğinin tehlikede olduğu gerçeğinin ortaya çıkmasıdır. Yazar bu tespitinin ardından çevre suçların özelliklerini şöyle aktarmıştır. Bu özellikler büyük oranda internet suçluluğu bakımından da kabul görececek özelliklerdir. 1- Çevre suçları yapay suç kategorisine girer. 2-Çevre suçlarının mağduru tüm insanlıktır.3- Çevre suçlarının faili genellikle şirketlerdir.4- Çevreye karşı suçlar genellikle tehlike suçlarıdır. 5- Çevreye karşı suçlar sınır tanımaz. 6- Suçun işlendiği anın tespiti güçlük arz eder. 7- Çevreye karşı suçlara genellikle organize ve planlı bir şekilde işlenir. 8 - Çevreye karşı suçların uluslara arası boyutu vardır. Ayrıntılı değerlendirme için bkz. **ÖZCAN**, Onur, Türk Hukukunda Çevre Suçları, in: Uğur Alacakaptan'a Armağan -1 (Der: Mehmet Murat İNCEOĞLU), İstanbul Bilgi Üniversitesi Yayınları, İstanbul 2008, sh: 565 v.d.

⁷¹ **PRITTWITZ**, Risiken, sh: 53.

⁷² *Özbek*, yasa koyucunun sürekli yeni suç tipleri yarattığını ifade etmektedir ve bu suç tiplerini üç kategori altında toplamaktadır. Birinci grup suç tiplerinde bilgisayar, gen teknolojisi ve atom tekniği alanındaki teknik e bilimsel ilerlemenin sonucu olarak kaleme alınan suç tipleridir. İkinci grup suç tipleri önceleri kabahat veya yan ceza kanunlarında düzenlenen ve punitiv yaptırımlarla cezalandırılan ve fakat zamanla değerlendirme tarzındaki değişim ile daha yoğun bir şekilde işlenen ve ceza hukuku içine alınması ihtiyacı olan suçlardır. Bunlar da çok çevre suçları ve ticari suçlardır. Üçüncü grup suç tipleri ise giderek daha da şiddetli cezalandırılabilir davranışları içeren suç tipleridir ki bu suçlara da örnek olarak uyuşturucu madde suçları ve organize suçluluktur. Yazar, zararın henüz ortaya çıkmadığı bir ön alana denk gelen hareketlere ilişkin bu yeni suç tiplerindeki artışın

Bilindiği üzere tehlike suçlarında hareket nedeniyle meydana gelen sonucun suç konusu bakımından bir zararı meydana getirme tehlikesi söz konusudur. Tehlikenin niteliği ve ağırlığına göre tehlike suçları somut ve soyut tehlike suçları olmak üzere iki temel ayrıma tabi tutulmaktadır. Somut tehlike suçlarında gerçekleştirilen hareketin korunan bir hukuksal değer üzerinde aktüel ve saptanabilir bir tehlikeye sebep olması aranırken soyut tehlike suçlarında hareketin somut, saptanabilir bir tehlikeyi yaratması aranmaksızın hareketin tipik tehlikeliliği cezalandırılabilirlik için yeterli görülmektedir.⁷³

Tehlike suçlarında cezalandırılabilirlik sınırının zarar suçlarına oranla daha öne alındığı yönündeki tespite ek olarak da benzer bir tespiti tehlike suçlarının iç sınıflandırması için yapmak mümkündür. Çünkü somut tehlike suçlarında, söz konusu suç teşkil eden neticenin meydana gelmesi tehlikesi aktüel, saptanabilir bir öngörü ile ortaya konulurken, soyut tehlike suçlarında bu öngörü maddi bir belirlenime dayanmamakta bilakis davranışın potansiyel tehlikeliliği nazarı dikkate alınmaktadır.⁷⁴ Dolayısıyla somut tehlike suçlarında isnadiyetin somutlaştırılabilir olması, belli koşulların varlığının tespitini zorunlu kılmakta, buna bağlı olarak da sadece potansiyel bir tehlikeliliği esas alan soyut tehlike suçlarına oranla sınırlı bir cezalandırılabilirlik esası kabul edilmektedir. Tersinden bakıldığı zamanda soyut tehlike suçlarının cezalandırılabilirlik alanının daha da genişlettiği görülmektedir.

Günümüz modern toplumunda, bilim- teknolojiadaki gelişmelere paralel olarak hukuksal değerlerin ihlal edilme risklerinin her geçen gün artış göstermesi⁷⁵, ceza hukukunun bu

doğru olup olmadığına yönelik tartışmaların yaşandığını belirtirken, bu artışın günümüz ceza hukukunun temelini oluşturan hukuksal değer kavramının çözülmesine, soyut suç tiplerinin çoğalmasına yol açtığı ve ceza hukukunun ikincilliği ilkesine önem verilmediği için eleştirildiğini ifade etmiştir. Ayrıntılı değerlendirme için bkz. **ÖZBEK**, Veli Özer, 21. Yüzyılda Ceza Adaleti, in: HFSA- 13(Der: Hayrettin ÖKÇESİZ), İstanbul, 2005, sh: 100.

⁷³ **ÖZTÜRK/ERDEM**, Uygulamalı Ceza Hukuku, sh: 138; **İÇEL**, Kayıhan/ **SOKULLU-AKINCI**, Fisun/ **ÖZGENÇ**, İzzet/ **SÖZÜER**, Adem/ **MAHMUTOĞLU**, Fatih/ **ÜNVER**, Yener, Suç Teorisi, 2. Baskı, İstanbul, 2000, sh: 68.

⁷⁴ **ÜNVER**, Hukuksal Değer, sh: 951.

⁷⁵ Bu konuda *Yalçın*'in internet teknolojisinin gelişimine vurgu yaptığı şu değerlendirmesi ceza hukuku anlamında söz konusu riskin boyutlarını ortaya koymaktadır. "*İnternet'in etkilerinden bir diğeri, onun suç ve suçluluk alanına yapmış olduğu etkidir. Teknolojinin gelişmesiyle ortaya çıkan yeni suçlar eski örgütlenmelerin dayanıklılığını sorgulamada iyi birer araçlardır. Sanal ortamda henüz suç işleme konusu gündemde değilken, insanların kafasında genel bir suçlu profili vardı: Şiddet kullanan, öldüren, yaralayan, fiziki olarak hırsızlık yapan, rüşvet veren-alan, uyuşturucu kaçakçılığı yapan vb gibi. Bunların yaptıkları suç sayılan eylemler toplumdaki düzeni ve ahengi fiziki ortamda bozmakta ve sonuçları hemen oracıkta hem suçu işleyen hem de mağdurlar tarafından hissedilmektedir. Bir başka deyişle suçu işleyen kişi karşısındakine verdiği zarara veya acıya da bizzat şahit olmaktadır. Bu durum, aslında pek önemsiz görülse bile, hem bir yanıyla cesaret isteyen ve hem de bir yanıyla suça niyetli insanları vicdan muhasebesi yaparak suçtan alıkoyabilmektedir. İnternet ortamı maalesef suç ortamına yeni bir boyut katmıştır: Sanal ortamdan gerçek düzene indirilen darbeler olarak bunu nitelendirmek mümkün olabilir. Burada bilginin evrenselliği ilkesinden hareketle teknolojinin sunduğu imkanları*

riskleri bertaraf etmek için en etkin araç olduğu düşüncesiyle bu riski barındıran hareketlerin ne kadar önce önlenibilirse o derece yüksek güvenlik standardına ulaşılabileceği kanaati ceza hukukunda tehlike suçlarının özellikle de soyut tehlike suçlarının tercih edilmesi sonucunu doğurmuştur⁷⁶. Klasik çizgide düzenlenen zarar suçlarının çağın gereklerine bağlı olarak ortaya çıkan hukuksal değer ihlallerini karşılar nitelikte olmadığı ve bu suretle doğabilecek boşlukların tehlike suçlarının düzenlenmesiyle doldurulması prensibi modern ceza hukuku düşüncesi içinde kabul edilen bir eğilimi yansıtmaktadır. Yalnız bu noktada hangi tür tehlike suçlarının tercih edildiği problemi ortaya çıkmaktadır. Çünkü modern toplumun temel dinamikleri üzerindeki bakış açısıyla ortaya çıkan tehlike - güvenlik hassasiyeti doğrudan somut ve soyut tehlike suçlarından hangisi yönünde tercih yapılacağını etkilemektedir. Tehlike - güvenlik geriliminin arttığı bir ortamda güvenlik ihtiyacının da artacağı düşünülecek olursa cezalandırılabilirlik alanının genişletilmesi, başka bir ifade ile cezalandırılabilirliğin hazırlık hareketlerine kadar çekilmesi dolayısıyla soyut tehlike suçları yönünde eğilimi mantıksal bir sonuç olarak ortaya çıkmaktadır.

Gerek soyut gerek somut tehlike suçlarının amacı, farklı tarzlarda da olsa zarar suçlarına nazaran cezalandırılabilir alanı öne çekerek hukuksal değerlerin korunmasını sağlamaktadır. İleride doğabilecek zararlardan kaçınmak için, zarar suçlarına nazaran hazırlık niteliğinde olan hareketler cezalandırılmaktadır.⁷⁷ *“Cezalandırılabilirlik alanının öne çekilmesi ve soyut tehlike suçlarının cezalandırılması günümüz ceza hukukunun en çok tartışılan konularından birisini oluşturmaktadır. Soyut tehlike suçlarının kanuni tipler haline getirilmesi son yıllarda ceza hukukunun yeni gelişen alanlarında olmak üzere çok sık tercih edilen bir yasa yapma tekniği haline gelmiştir.”*⁷⁸

Modern ceza hukuku anlayışının, ceza hukuku normlarının son araç olması, hukuk devleti ve belirlilik ilkelerine uyarlanmaları çok daha kolay olan zarar suçlarının korunduğu hukuksal değerleri korumak için kullanılan klasik ceza hukukundan farklı olarak, bu hukuksal değerler yanında gün geçtikçe artan ve zarar suçlarından tehlike suçlarına doğru yaşanan hızlı

kullanarak bilgi sahibi olan bazı insanların hiçte cesaret gerektirmeyen ve sonucu birebir hissedilmeyen eylemlere giriştiğini ve bu yolla ekonomik yapılanmaya büyük zararlar verilebildiğine yıllardır şahit olmaktadır. (...) İnternet ortamından yapılan saldırıların kaynağına ulaşmak da mümkündür ancak bir farkla; bir çok durumda polisler bastıkları evde cani ruhlu suçlular bulacaklarını hayal ederken, karşılarında çocuk yaşta insanları buluvermektedirler.” Ayrıntılı bilgi için bkz. **YALÇIN**, Cemal, Sosyolojik Bir Bakış Açısıyla İnternet, in: C. Ü. Sosyal Bilimler Dergisi, Mayıs 2003, Cilt: 27, No:1, sh: 83 – 84.

⁷⁶ **HILGENDORF**, Strafrechtliche, sh: 48-49.

⁷⁷ **HONG**, Flexibilisierungstendenzen, sh: 65.

⁷⁸ **ÜNVER**, Hukuksal Değer, sh: 958.

bir genişlemeye sahne olduğunu savunan *Ünver* bu hızlı değişimin beraberinde başta temel ceza hukuku ilkeleri üzerinde olmak üzere birçok açıdan karmaşık sorunlara yol açmakta ve hukuk devleti ilkesinin gerekleri açısından bazı açmazların doğmasına neden olduğunu dile getirmiştir. Bir yandan kaçınılmaz olan bu genişleme olağan görülürken diğer yandan da bu alanlardaki düzenlemelerin mantıklı, hukuksal değerlerin korunması ilkesine uygun ve hukuksal devletinin gereklerine uyularak düzenlenmesi gerektiğine işaret edilmektedir. Yazar bu çerçevede tehlike suçlarının sayısında yaşanan artışı iki temel nedene dayandırmaktadır. Bunlardan ilk neden, hukuksal değerlerin daha iyi bir biçimde korunması için cezalandırılabilirlik alanını öne çekme düşüncesi, diğeri ise hızla gelişen teknoloji alanında klasik zarar suçları yetersiz kalması ve ceza hukukunun uygulama alanının öne doğru çekilmesinin bir ihtiyaç olarak hissedilmesidir.⁷⁹

1.4.3.- Ceza Hukuku Normlarının Son Araç Olarak Kullanılması Prensibinde Yaşanan Dönüşüm

Ceza hukuku normlarının son araç olma özelliğini dile getiren “*ultima ratio*” ilkesi bir hukuksal değer ihlalini mümkün kılacak davranışın önlenmesi için diğer hukuk dallarının yetersiz kaldığı ve söz konusu değerlerin bir ceza normu ile korunmasının kaçınılmaz olduğu durumlarda ceza hukukunun devreye girmesi durumunu açıklamaktadır⁸⁰. Bir davranışı ceza yaptırımına altına alınabilmesi ancak söz konusu davranış ile ortaya çıkan hukuksal değer ihlalinin başka bir hukuksal araçla giderilememesi durumunda söz konusu olacaktır. Şayet diğer hukuk disiplinleri ve toplumsal düzen mekanizmaları aracılığıyla bu ihlallerin önüne geçilebilecekse bir araç olarak ceza hukuku sistemi işletilmemelidir⁸¹.

Şöyle ki; özellikle 20. y.y. ikinci yarısından önce devletler sınırları içinde gerçekleşen ve hukuksal değer ihlaline sebebiyet veren eylemleri ve bu eylemlerle ortaya çıkacak olan neticeleri önlemek amacıyla diğer düzenleme araçlarını kullanabilmekte, böylece insanın irade hürriyetine en açık müdahalenin gerçekleştiği alan olan ceza hukukuna ancak başka bir araçla amaca uygun neticenin alınmamasının kesin olduğu durumlarda başvurulmaktaydı. Nitekim bu anlayış 20. y.y. ikinci yarısından itibaren de kullanılmaya devam etmiştir. Ancak özellikle 1980li yılların başından itibaren küreselleşen dünyada toplumsal ilişkilerin

⁷⁹ ÜNVER, Hukuksal Değer, sh: 946 – 947.

⁸⁰ ÜNVER, Hukuksal Değer, sh: 693.

⁸¹ ÖZBEK, Ceza Adaleti, sh: 101.

dönüşüme uğraması, tıp, bilişim/ iletişim, nükleer ve atom teknolojileri gibi alanlarındaki gelişmelerin hızlanması ve topluma yansımaları daha önce üzerinde durulduğu üzere modern yani bilgi toplumunu risk toplumuna dönüştürmüş ve bu gelişmelere paralel olarak ortaya çıkan risklerle mücadeleyi devletler en sıkı bir biçimde yapmaya başlamışlardır. Keza yukarıda değinildiği üzere küreselleşme olgusunun yansımaları, önleyici ceza hukuku düşüncesi, cezalandırılabilirlik alanının öne çekilmesi ve soyut tehlike suçlarının artışı hep bu “risk yönetimi” kaygısından kaynaklanmaktadır.⁸²

Bir bakıma devletler tabiri caizse insanların dizginlerini ele almak ve bu risk ortamından en az zararla çıkmak için artık en son kullanılması gerektiği kabul edilen kurumlarını öncelikli olarak tercih etmeye başlamıştır. Ceza hukukunun ultima ratio ilkesinin cezalandırma yetkisinin kötüye kullanılmasını frenlediği belirten *Bitzilekls*, ceza mahkemeleri önüne gelen ihtilafların %60'ının yan ceza hukuku alanına dahil eylemler olduğunun ifade edilmesinin bir abartı olamayacağını vurgulamıştır. Özel hukuk ile kamu hukukunun diğer alanlarındaki düzenlemeler yerine, daha ucuz ve politik açıdan toplum politikasının etkileyici aracı olarak ceza hukukunun seçildiğini belirten *Bitzilekls*, bu yaklaşımın ceza hukukunu başarısızlığa yönelteceğini belirtmiştir.⁸³

İşte *ultima ratio* prensibinin konumu da bu bütünlük içinde değerlendirilmelidir. Ceza hukukunun son araç olarak kullanılması prensibi modern dünyanın içinde bulunduğu konjonktürde güvenlik ve otorite zaafına neden olacağı gerekçesiyle biraz daha istisnalara açık olarak uygulanmaya başlanmıştır. Bunun en önemli nedeni de devletin hiçbir düzenleme aracının ceza hukukunun etkiyi verecek düzeyde değildir. Zaten temel hak ve özgürlüklere meşru müdahalenin en açık ve ağır yaşandığı alan olan ceza hukukunun bu karakteri onu en son kullanılması gereken araç olarak nitelendirmiştir. Ancak yukarıda da değinildiği üzere risk toplumunun yapısı devletleri önleyici fonksiyonu öne çıkarmak adına ceza hukuku “*ultima ratio*” olarak değil “*prima vey sola ratio (ilk araç)*” olarak kullanmaya yönlendirmektedir.⁸⁴

Konu ile ilgili Türkiye’den bir örnek vermek gerekirse *Ersoy*, 90’lı yılların başında gerçekleşen TCK değişikliği çalışmalarında bilişim suçlarının düzenlenişinde Ceza

⁸² HILGENDORF, Die deutsche Strafrechtsentwicklung 1975- 2000, sh:369.

⁸³ ÜNVER, Sempozyum Notları, sh: 155’den naklen.

⁸⁴ HASSEMER, Winfried, Absehbare Entwicklungen in Strafrechtsdogmatik und kriminalpolitik, in: Strafrechtprobleme an der Jahrtausendwende (Der: Cornelius PRITTWITZ, Ioannis MANELOKADIS) , 2000, sh: 19.

Hukukunun “*ultima ratio*” niteliğinin ikinci plana atılarak “*prima ratio*” ya dönüştürülmesini şöyle eleştirmiştir:

“Bizim mevzuatımızda öncelikle özel hukuk bakımından bir takım değerlendirmelerin yapılması, bir takım ihlalleri özel hukuk yaptırımlarıyla ve daha da olmazsa idare hukuku yaptırımlarıyla önlemenin aranması ve ancak ondan sonra ceza yaptırımını önlemenin aranması ve ancak ondan sonra ceza yaptırımını gerektiren hallerin ortaya çıkması gerektiren, doğrudan doğruya ceza mevzuatında bir kategori öngörülmesi, uygulanması olmayan veya çok az olan suç kategorisine yol açar.”⁸⁵

1.4.4.- Ceza Hukukunun Yapısal Özelliklerinin Esnekleştirilmesi Eğilimi⁸⁶

Bu noktaya kadar yapılan açıklamalarla modern ceza hukuku morfolojisinin hangi zemin üzerinde şekillendiğini sistematik bir biçimde ortaya konulmaya çalışılmıştır. Bu değerlendirmenin son halkası da tüm bu açıklamaları tamamlayıcı nitelikteki son eğilim olan

⁸⁵ **ERSOY**, Yüksel, Genel Hukuki Koruma Çerçevesinde Bilişim Suçları, in :AÜSBFD, C: 49, S: 3-4; Ankara, 1994, sh: 153.

⁸⁶ Ceza Hukuku’na ilişkin yapıların “esnekleştirilmesi” olarak nitelendirilebilecek eğilimlerle ilgili üç dava oldukça ilgi uyandırmıştır: “Compu- Serve Davası”, “Auschwitz Yalanı Davası” ve “Çocuk Pornografisi Davası”. “Compu- Serve Davası”nın temel sorunu erişim sağlayıcısının internet aracılığıyla pornografinin yayılmasından kaynaklanan sorumluluğudur. Sanık hakim şirket ile birlikte çalışan bağlı şirketin sorumlusu olarak, alman kullanıcıların Amerika’daki hakim şirketin Server’inde kayıtlı olan ve gençler açısından sakıncalı görüntülere ulaşabilmelerini mümkün kılmıştır. Münih Sulh Ceza Mahkemesi Tele- Hizmetler Yasası’nın (THY) 5. maddesinin 2. fıkrası gereğince (bu arada THY, Bilişim ve İletişim Servisleri Yasası ile değişikliğe tabi tutulmuştur.), sanığın sorumluluğunda çocuk pornografisinin yayılmasındaki müşterek faillik nedeniyle herhangi bir sınırlandırmaya gitmemiştir. Buna karşın Münih Eyalet Mahkemesi sanığın THY md. 5/3 gereğince beraatine karar vermiştir. Münih Sulh Ceza Mahkemesi kararını yasanın yürürlüğe giriş tarihi olan 13.06.1997’den sonra tesis ettiği için (karar tarihi 28.05.1998), bu yargılama aracılığıyla bir erişim sağlayıcısının sorumluluğundaki mevcut boşlukların THY aracılığıyla nasıl doldurulacağı görülmüş oldu. İkinci davada, “Auschwitz Yalanı Davası”nda, internet aracılığıyla yabancı bir ülkeden yönlendirilen suç içerikli yayınların yayılması durumu söz konusudur. Bu dava bakımından, bu yolla yabancı bir ülkeden yönlendirilen içeriklerin Alman Ceza Kanunu md. 9’a göre Alman Ceza Hukuku’nun uygulama alanı bulup bulamayacağı sorusu sorulmuştur. 12.12.2000 tarihli kararda Federal Mahkeme ilk defa internet davalarında Alman Ceza Hukuku’nun uygulama alanı üzerinde durmuştur. Her şeyden önce de Federal Mahkeme internet alanında soyut- somut tehlike suçları açısından Alman Ceza Hukukunun uygulanabilirliği sorunu ile meşgul olmuştur. Bu suretle, veri ağlarının uluslar arası niteliğinin, yanıtları uygulamada ve öğretide halen oldukça tartışılan derin dogmatik sorunlara kaynaklık ettiği ortaya konulmuştur. Üçüncü dava, “Çocuk Pornografisi Davası”, internet üzerinden çocuk pornografisinin yayılması ve ulaşılabilirliği ile ilgilidir. Bu dava özellikle internet aracılığıyla çocuk pornografisinin yayılımı ve üretiminin artış içinde olduğu vurgulanmaktadır. Sınırsız “siber alem”in gelmiş olduğu seviye itibariyle pornografinin bu tarzının ilgilileri kendilerini yalnız hissetmemektedirler. Hatta çocuk pornografisi içerikli veriler şifrelendirilmiş formda kolaylıkla bir başka kullanıcıya gönderilebilmektedir. Buna karşılık Federal Mahkeme, Al. C. K. md. 184’ün temel kavramlarını kısmen dahi olsa yeniden tanımlamak suretiyle internet aracılığıyla yürütülecek mücadelenin daha etkili hale getirilmesi hususunda çaba sarf etmiştir. Her üç dava ile ilgili ayrıntılı değerlendirme için bkz. **HONG**, Seung Hee, Compu-Serve Davası, in: Karşılaştırmalı Ceza Hukuku Serisi/7, sh: 323 vd., **HONG**, Seung Hee, Auschwitz Yalanı (Çev:Emin KOÇ), in: Karşılaştırmalı Ceza Hukuku Serisi/ 7, sh: 333 vd.; **HONG**, Seung Hee, Çocuk Pornografisi (Çev:Pınar BACAŞIZ), in: Karşılaştırmalı Ceza Hukuku Serisi/ 7, sh: 343 vd.

ceza hukukunun klasik yapılarının esnekleştirilmesi (*Flexibilisierung*) eğilimidir.⁸⁷ Bu eğilimin mantığını anlamak yukarıdaki açıklamalar dikkate alındığı takdirde hiç de zor değildir. Çünkü klasik ceza hukuku yaklaşımının temel unsurları sayılırken bu yaklaşımın ortaya çıkış serüveni de aktarılmış ve klasik ceza hukukunun temel prensiplerinin aydınlanma dönemi hümanist felsefesinin etkisiyle hazırlandığı, Ortaçağ skolastizminin tanrısal kaynaklı, sınırları muğlak ve hümanist güvencelerden yoksun ceza hukuku uygulamalarına bir tepki olarak ortaya çıkarıldığı kabul edilmektedir. Bu nedenle klasik ceza hukuku yaklaşımıyla öncelik cezalandırma prensiplerinin statik hale getirilmesi ve mutlak güvencelerle insan değerini koruyan bir hüviyete büründürülmesi amaçlanmıştır. Bu bakış açısı Belirlilik, Kanunilik, Kusur, Ultima Ratio ve Şüpheden Sanık/Özgürlük Yaralanır (in dubio pro reo / libertate) prensiplerinin doğumuna neden olmuştur. Ancak modern toplum koşulları içerisinde bu ilkelere mutlak bağlılığın o dönem için geçerli olan faydaların elde edilmesi sonucunu doğurmayacağı kabul edilmeye başlamıştır.⁸⁸

Bu bakış açısı da bazı kurumlarla örneklendirilmektedir. Örneğin her geçen gün bilgi – iletişim teknolojilerinde yaşanan gelişmeler yeni hukuksal değer ihlallerine sebebiyet verecek kaynakları ortaya çıkarabilir. İnternet örneği üzerinden hareket edilecek olursa son 20 yılda en çok gelişim sağlayan bilişim – iletişim teknolojisi olan internette her gün yeni bir hizmet imkanı doğmakta bu hizmet imkanları amacına uygun kullanılmadığı takdirde hukuksal değer ihlallerine sebebiyet vermektedir. Peki bu ihlallerin ceza hukuku görünümüleri açısından nasıl bir değerlendirme yapılacaktır? Kanunilik prensibi gereği kanunda açıkça unsurları belirtilmemiş bir eylemden dolayı kimse cezalandırılmaz. Bugün internette ortaya çıkan yeni bir ihlal modeli ceza kanunlarında açıkça düzenlenmediği takdirde cezai yaptırıma tabi tutulamaz, buna rağmen ortaya zarar neticesi doğuran bir eylem çıkmaktadır. Bu riski önlemek amacıyla genel eğilime paralel ve müstakbel ihlal modellerini kapsayacak biçimde genel düzenlemeler yapıldığı takdir de Belirlilik ilkesi ihlal edilmiş olacaktır⁸⁹. Yine benzer

⁸⁷ Ceza Hukukunda esnekleştirmenin anlamı üzerine ayrıntılar için bkz. **HONG**, Flexibilisierungstendenzen, sh: 91.

⁸⁸ **HILGENDORF**, Die deutsche Strafrechtswirkung 1975 – 2000, sh: 373.

⁸⁹ Bu tespiti bilişim suçları açısından bir örnekle yaklaşmak gerekirse, 765 s. TCK'da düzenlenen bilişim suçlarında en çok tartışılan konulardan biri “diğer herhangi bir unsur” kavramıdır. Bilindiği üzere 765 s. TCK md. 525/a v.d. maddelerinde düzenlenen bilişim suçlarında suç teşkil eden eylemin veri, program veya diğer herhangi bir unsur üzerinde cereyan edeceği kabul edilmekteydi. Özellikle veri ve program kavramları somutlaştırılabilir nitelikte olmalarına rağmen “diğer herhangi bir unsur” kavramı belirsizlik içermekteydi. Kanun koyucunun böyle bir tercih yapmasındaki temel neden o dönemde bilişim teknolojilerindeki gelişmeler sonucu ileride ortaya çıkabilecek ve ne olacaklarının baştan tahmin edilmesi güç olan bilişim sistemi unsurlarının da bu kapsam altında değerlendirilmesine olanak sağlamaktır. Ancak tercih doktrinde çok ciddi eleştirilere maruz kalmıştır. Özellikle bu kavramla neyin anlatılmak istendiği yeterince açık olmadığı bunun da

nitelikli başka bir kurumun düzenlemesi örnek olarak kullanılmak istenirse de Kıyas yasağı ihlali karşımıza çıkacaktır. Bu durumda modern toplumun dinamik yapısı klasik ceza hukuku prensiplerinin güvenceleriyle korunmaktan çok daha büyük risklere ve tehlikelere maruz kalacaktır. Yine *ultima ratio* prensibi ile ilgili dönüşüm örneği yukarıda verilmişti.

Ceza Hukukunda esnekleştirme girişimleri üzerine yapılan tartışmalara Polonya Ceza Hukuku özelinde verilecek örneğin konunun çerçevesini belirme konusunda etkili olabileceği kanaatindeyiz. *Wasek*, Polonyanın geçirdiği totaliter politik sistemin kötü tecrübelerinin kendilerini, ceza normu yaratmak ve uygulanmasında, kanunilik ilkesine riayet etmek bakımından oldukça hassaslaştırdığını ve aradan on yılı aşkın bir sürenin geçmesine rağmen eski politik geçmişlerinin psikolojik baskısını hissettiklerini belirtirken, bu bağlamda kanunilik ilkesinde en ufak bir gevşemeye ciddi hiçbir Polonya ceza hukukçusunun taraftar olamayacağını önemle vurgulamıştır. Aynı şeyin, kanunilik ilkesiyle sıkı ilişki içinde olduğu "fiil ceza hukuku ilkesi" için de geçerli olduğunu belirten yazar, gelecekte de bu ilkeye mutlak bir bağlılığın olması gerektiğini vurgulamıştır⁹⁰. Bu yaklaşım tarzının karşısında *Gostynski*, Kanunilik ilkesinin Polonya hukuk düzeninde egemen ilke olmasına karşılık, bu ilkenin maslahata uygunluk (oportunité) ilkesi altında toplanabilecek önemli istisnaları olduğunu belirtmiş ve kanunilik ilkesinin aşırı anlamda ele alınması durumunda yargı organlarına aşırı yük yükleme tehlikesinin ortaya çıkacağını ifade etmiştir⁹¹.

İşte bu tartışmalar ceza hukukunda güvencelerin esnekleştirilmesi önerilerini ortaya koymaktadır. Nitekim uygulamada bu tarz esnekleştirme eğilimine de rastlamak mümkündür. Ancak tabii ki burada esnekleştirmenin ölçüsü problemi de kendini göstermektedir. Hangi noktaya kadar bu kurumları esnekleştirmek mümkündür? Şayet bu esnekleştirme girişimleri esnekleştirilen kurumların hiçe sayılmasına varacak derecede yapı bozumuna sebebiyet verecekse ceza hukukunda esnekleştirme amacı dışında bir şeye hizmet edilmiş olur. Netice de söz konusu prensiplere mutlak bağlılık modern toplumun dinamiğinde ceza hukukunun etkinliğini sekteye uğratabilecek riskleri içerse de⁹² bu prensiplerin tamamen ortadan kaldırılmasına zemin hazırlayacak bir esneklik daha büyük tehlike ve zararlara neden olur.⁹³

ceza hukukunun temel prensiplerinden kanunilik ve belirlilik ilkelerine aykırılık oluşturduğu üzerinde durulmuştur. Konu ile ilgili eleştiriler için bkz. **DÜLGER**, Murat Volkan, *Bilişim Suçları*, Ankara, 2004, sh: 68; **ÜNVER**, TCK ve Ceza Kanunu Tasarısının Değerlendirilmesi, sh:95; **YAZICIOĞLU**, *Bilgisayar Suçları*, sh: 227.

⁹⁰ **ÜNVER**, Sempozyum Notları, sh:164'den naklen.

⁹¹ **ÜNVER**, Sempozyum Notları, sh: 170'den naklen.

1.5. - Modern Ceza Hukuku Morfolojisi Üzerine Doktrindeki Bazı Görüşler

Modern ceza hukukunun kimlik analizini klasik ceza hukuku anlayışının temel prensipleri ile karşılaştırmalı olarak ortaya koyduktan sonra modern ceza hukuku morfolojine geçmek isabetli olacaktır. Bu noktaya kadar yapılan süreçsel değerlendirmeler ışığında modern ceza hukuku yaklaşımının hangi temel yapılar etrafında tasarlandığı daha isabetli olarak tespit edilebilir. Günümüz ceza hukukunun belki de en dinamik düzenleme alanı olan internet ortamında işlenen suçlar ve internet süljelerinin ceza sorumluluğu ancak böyle bir sistem analizinin ardından ele alınabilir. Çünkü bu sistem analizi aynı zamanda söz konusu suçluluk ve sorumluluk alanlarının hangi ceza hukuku felsefesiyle düzenlenmesi gerektiğini de gözler önüne serme iddiasını taşıyabilir.

1.5.1. - Winfried Hassemer

Hassemer'e göre günümüz modern ceza hukuku dört temel nokta üzerine inşa edilmiştir. Bu dört temel nokta şunlardır: hukuksal değerlerin korunması, önleyici fonksiyonun öne çıkarılması, neticeyle ilişki kurmak ve ceza hukukunun metafizikten ayrılması⁹⁴.

Hassemer hukuksal değerlerin korunmasını modern ceza hukukunun en bariz karakteristiği olarak görmektedir. Ancak buradaki karakteristik özellik yukarıda da değinildiği üzere modern ceza hukukundaki hukuksal değer korumasının hangi bağlamda klasik ceza hukukundan ayrıldığı noktasında kendini göstermektedir. Her şeyden önce şunu dile getirmek gerekir ki, *Hassemer* de hukuksal değerlerin korunması teorisini Aydınlanma dönemi düşünce dünyasının bir ürünü olarak kabul ederken bu teoriyi devletin cezalandırma yetkisinin meşruiyet düzlemi olarak görmektedir. Buradan da anlaşılacağı gibi *Hassemer* hukuksal değerlerin korunması yaklaşımının klasik ceza hukuku anlayışında da var olduğu

⁹² HILGENDORF, Eric/ FRANK, Thomas/ VALERIUS, Brain, Computer und Internetstrafrecht, Berlin – Heidelberg, 2005, sh: 168.

⁹³ Benzer yönde düşünceler için bkz. HASSEMER, Winfried, Symbolische Strafrecht und Rechtsgüterschutz, NSZ, H. 12, 1998, sh: 558.

⁹⁴ ÜNVER, Hukuksal Değer, sh: 442.

kanaatindedir ancak klasik ceza hukukundan modern ceza hukukuna geçişte bu teörinin bir dönüŖüne uğradığını düşünmektedir.⁹⁵

Modern ceza hukuku bireysel nitelikli hukuksal değerlerin korunması ekseninden ayrılarak evrensel hukuksal değerlere (*Universalrechtsgüter*) yönelmiştir. Bu anlamda modern ceza hukukunda artık kurumların korunmasına yönelik bir hukuksal değer korumasından bahsedilmektedir. Yazar bu yaklaşımın doğal sonucu olarak da evrensel hukuksal değerlerin henüz net olarak kavramlaştırılmamasının bir muğlaklığa neden olduğunu, bunun da ceza hukukun büyük ölçüde genişlemesine (*Ausweitung des Strafrecht*) ve soyut tehlike suçlarının somut tehlike veya zarar suçlarına oranla artış göstermesine neden olduğunu savunmaktadır.⁹⁶ Bunu da ceza hukukunun hukuk devleti geleneğinden uzaklaşması anlamına geleceğini ifade etmektedir. Bu durum tespitinin ardından soyut tehlike suçlarının modern ceza hukukunun yapısına ve amaçlarına uygun olduğu üzerinde duran *Hassemer* soyut tehlike suçlarını “*modernitenin suç şekli*” olarak kabul etmektedir.⁹⁷ Yazara göre soyut tehlike suçları, somut insan çıkarlarından ziyade toplumsal kurumların korunmasını amaçlamaktadır. Ancak bu tespitlerle birlikte soyut tehlike suçlarındaki aşırı genişlemenin temel amaç olan hukuksal değerlerin korunmasına hizmet vermenin ötesinde ihlal kaynağı olma ihtimalini de canlı tuttuğunu savunmaktadır. “*Klasik – liberal ceza hukuku bakımından şüpheli olan bu düzenlemelerin, önleme düşüncesine dayandırılmasını da yetersiz bulmaktadır. Bu alanda sembolik ceza hukuku anlayışına başvurulmasının riskli olabileceğini, sembolik ceza hukuku anlayışında hukuksal değerlerin korunması kaygısından çok kanun koyucunun imajının ön planda olduğunu savunmaktadır.*”⁹⁸

Modern ceza hukukunun önleme fonksiyonunu ön plana çıkartması *Hassemer* tarafında modern ceza hukukunun bir diğer karakteristik özelliği olarak kabul edilmiştir. Keza hukuksal değerlerin korunması teorisine ilişkin değerlendirmelerinde sürekli ceza hukukunun artık sadece “*ultima ratio*” değil “*prima veya sola ratio*” olduğu tespitine gönderme yapması modern ceza hukukunun morfolojik yapısında önleme fonksiyonunun ne denli önemli bir yere sahip olduğunu bir göstergesi olarak yorumlanmalıdır.⁹⁹ Öyle ki *Hassemer* modern ceza

⁹⁵ HONG, Flexibilisierungstendenzen, sh: 61.

⁹⁶ HONG, Flexibilisierungstendenzen, sh: 62.

⁹⁷ HONG, Flexibilisierungstendenzen, sh: 62.

⁹⁸ ÜNVER, Hukuksal Değer, sh: 960.

⁹⁹ HASSEMER, Absehbare Entwicklungen, sh:19.

hukukunu önleme ceza hukuku (*Präventionsstrafrecht*) olarak da adlandırmaktadır.¹⁰⁰ Modern ceza hukukuna bu denli içkin bir fonksiyon olarak kabul gören önleme fonksiyonu aslında klasik ceza hukukunda da kullanılan etkili bir fonksiyon olarak görüldüğünü vurgulayan *Hassemer* her iki ceza hukuku düşüncesinin bu kavrama yaklaşımını birbirinden ayırma eğilimindedir. Şöyle ki; klasik ceza hukukunda “*Prävention*” kavramı haksızlık ve kusurlu eylemlere bir karşılık olarak ceza hukukunun tamamlayıcısı niteliğinde bir anlam taşımaktadır. Ancak modern ceza hukuku bakımından bir tamamlayıcı öge olmanın ötesinde bizatihi modern ceza hukukunun baskın amacını teşkil etmekte, gelecekte ortaya çıkması muhtemel suç niteliğindeki hukuk düzenine aykırılıkların önlenmesi amaçlanmaktadır. Bu değerlendirmeden sonra bir hususun altı çizilmelidir. “*Prävention*” kelimesi hem önleme hem de tedbir anlamına gelmektedir.

Hassemer'in yapmış olduğu bu ayırım karşısında klasik ceza hukuku düşüncesi içinde kullanılan “*Prävention*” kavramının nitelik itibariyle karşılık, bedel ve tamamlayıcılık fonksiyonu göz önünde bulundurulduğunda daha çok teknik (sonradan uygulanan) tedbir anlamında kullanıldığı, ve fakat modern ceza hukuku anlayışı içinde kullanılan “*Prävention*” kavramının ise doğrudan önleme anlamında kullanıldığı kabul edilmelidir. Yalnız *Hassemer* bu ilke bakımından da bir takım kaygıları taşımaktadır. Bu kaygıların en önemlisi modern ceza hukukunda önleme fonksiyonun normatif sınırlarının nasıl belirleneceği üzerinedir. Yazar ceza hukukunun önleme fonksiyonunun yoğunlaştırılması sonucu ortaya çıkacak olan tehdit duygusunun hukuk devletinin ceza ve ceza usul hukuku bakımından çizdiği normatif sınırların aşılmasına sebebiyet verip vermeyeceği konusunda tereddütleri vardır.¹⁰¹

Hassemer modern ceza hukukunun neticeye ilişkilendirilmiş bir yapısı olduğu kanaatindedir. Özellikle neticeye yönelimli bir ceza hukuku anlayışının hukuksal değerlerin korunması ve önleme ile çok yakından ilişkili olduğunu kabul etmektedir.¹⁰² Bu ilişkiyi kurarken de ceza hukukunun toplumsal ilişkilerin korunmasında ve toplumsal yaşamın sağlıklı bir şekilde devamlılığında yönlendirici – yönetici bir araç olması özelliğinden hareket etmektedir. Hatta ceza hukukunu halk pedagojisi aracı olarak gördüğünü ifade etmektedir. *Hassemer*, kendi zamanına kadar savunulan hukuksal değer görüşlerini ve onlara dayalı olarak ceza hukukunun ödevinin oluşturulmasına ilişkin görüşleri genel/soyut nitelikte ve

¹⁰⁰ HONG, Flexibilisierungstendenzen, sh: 64.

¹⁰¹ HONG, Flexibilisierungstendenzen, sh: 65.

¹⁰² HONG, Flexibilisierungstendenzen, sh: 66.

uygulamadan uzak olmaları dolayısıyla eleştirmiştir. *Hassemer'e* göre suç birey ile toplum arasındaki iç ilişki sürecinin bir ürünüdür.¹⁰³

Hukuksal değer kavramını toplumsal olarak kanıtlanabilirlik ile paralel görmektedir. Bu bakımdan modern toplumunun sosyolojik niteliklerini modern ceza hukuku morfolojisine de etki edeceğini düşünmektedir. Zaten modern ceza hukukundaki ultima ratio prensibinin geçirdiği evrimi bu yaklaşıma bağlamaktadır. Ceza hukukunun modernleşmesi sürecinin aynı zamanda ceza hukukunun fonksiyonelleşme süreciyle paralel gören *Hassemer* ceza hukukunun fonksiyonelleşmesinin de ceza hukukunun normatif geleneklerinin değişmesi/dönüşmesine etkide bulunduğunu kabul etmektedir. Bu süreçte objektif isnadiyet öğretisi, müdahaleci veya pozitif genel önleme, evrensel hukuksal değerler ve soyut tehlike suçlarının yaratılması eğilimiyle güncel bir suç politikası tercihi ceza hukukunun fonksiyonel hale getirilmesi amacıyla kullanılan araçlar olarak dikkat çekmektedir ki bu durum da fonksiyonel ceza hukukunun hukuk devleti temel ilkelerinden uzaklaştığı anlamına gelmektedir.¹⁰⁴

1.5.2.- Ulrich Sieber

Sieber, günümüzde artış gösteren suçluluk ile modern toplum arasında sıkı bir ilişki olduğunu düşünmektedir. Yazara göre modern toplum bünyesinde birçok riski barındırmaktadır ve bu riskler toplum dinamiklerini şekillendirmektedir.¹⁰⁵ Risk Toplumu veya Risk Altında Yaşayan Toplum olarak belirlediği bu toplum yapısı içerisinde riskin kontrol edilebilirliği ile suçluluk arasında bir ters orantı mevcuttur. Risk ne ölçüde kontrol edilebilirse, suçluluk da buna bağlı olarak bir azalma trendi içerisine girecektir. Ancak risk kaynaklarının kontrolü ne kadar azalır, suçluluk da bir o kadar artacaktır. Bu yaklaşımın ceza hukukunda son dönemde yaşanan toplumsal gelişmelere bağlı olarak etkisini daha da arttırdığını düşünen *Sieber*, bunun en büyük kanıtı olarak günümüz ceza hukukunda önleme düşüncesinin ön plana çıkartılmasını göstermektedir.¹⁰⁶

Yazar, modern toplumun yukarıda özetlenen bu özellikleri dolayısıyla klasik ceza hukuku anlayışı içerisinde belirlenmiş temel ilkelerin bir değişim süreci içerisinde ele alınması gerektiğini savunmaktadır. Bu değişim süreci iki eksen üzerinde şekillenmektedir.

¹⁰³ HONG, Flexibilisierungstendenzen, sh: 66.

¹⁰⁴ HONG, Flexibilisierungstendenzen, sh: 68.

¹⁰⁵ SIEBER, Ceza Hukukunun Sınırları, sh: 174.

¹⁰⁶ SIEBER, Ceza Hukukunun Sınırları, sh: 173.

Birincisi küreselleşme olgusuna paralel olarak sınır aşan suçların işlenmesi için yeni olanaklar sağlanmasıyla ceza hukukunun ülkesel sınırlarının zorlanmasıdır. Buna bağlı olarak da ikinci eksen, “bilgi toplumu/ risk altında yaşayan toplumdaki” gelişmelerin ortaya çıkan suç yapılarında bir karmaşıklaşmaya sebebiyet vermesinden ötürü, klasik ceza hukuku formlarının bu karmaşık yapıları çözmeye ve ceza hukukunun fonksiyonel etkisini hissettirmeye elverişli olamayacağı düşüncesinden hareketle, toplum ve birey özgürlüklerinin korunması kaygısıyla ceza hukukunun yapısal sınırlarının zorlanmasıdır.¹⁰⁷

Küreselleşen toplumda, kişilerin ve eşyaların ülke sınırları dışına doğru hareket edebilir hale gelmesi, sınır ötesinde yapılan hizmetlerin ve bilgisayar verilerinin kolaylıkla sınır ötesine aktarılabilmesi, sınır aşan suçluluğun hızlı bir şekilde artmasına neden olmaktadır. Örneğin teknik olarak bakıldığında, dünya çapındaki veri ağlar suç işlemek için kullanılmakta ve internette mevcut verilere, dünyanın her yerinden ulaşılabilmekte ve bir tıklama ile her yerden bunlara erişilebilmektedir. Ülke sınırlarını aşan erişime açık bu verilerin bir ülke tarafından kendi mülki sınırları içerisinde denetim altına alınması mümkün değildir. Bu gelişmeler karşısında küreselleşmenin suçluluğun artması ve çeşitlenmesi açısından olumsuz etkiler doğurduğunu savunan *Sieber*'e göre, daha önce bağımsızlık fikrine dayanan klasik ceza hukukunun sınırları ülke dışında işlenen suçlar söz konusu olduğunda zorlanmaktadır¹⁰⁸. Ceza hukukunun bu yeni sorunları yenmesi için ülke dışında işlenen suçları da yargılayacak şekilde kapsamının genişletilmesi yani “küreselleşmesi” gerekmektedir.

Sieber, suçların aydınlatılması açısından giderek daha da büyümekte olan risklerin ceza hukukunun görevlerini kimi noktalarda sembolik bir düzeye indirgediğini düşünmektedir. Bireyin özgürlüklerine büyük müdahale yapılsa bile bu alanlarda ceza hukuku etkisiz kalmaktadır. Bu durumun özel olarak gözlemlendiği alanlar, internet suçluluğu, ekonomik suçlar, örgütlü suçluluk ve terör suçlarıdır. Örneğin bu yeni riskler tipik olarak modern bilgi toplumunun bilgisayar sistemlerine giderek daha fazla bağımlı hale gelmesinden kaynaklanmakta ve bunlara dayalı olarak da güvenlik boşlukları ve dünya çapında ağ şeklinde birbiriyle bağlanmış bilgisayarlar içerisinde hareket eden failin, genellikle kolay ele geçmesi sağlanamamaktadır¹⁰⁹.

¹⁰⁷ **SIEBER**, Ceza Hukukunun Sınırları, sh: 175.

¹⁰⁸ **SIEBER**, Ceza Hukukunun Sınırları, sh: 177.

¹⁰⁹ **SIEBER**, Ceza Hukukunun Sınırları, sh: 180.

Son olarak da *Sieber*'in modern ceza hukuku anlayışını klasik ceza hukuku sınırlarının yetersizliği üzerinden değerlendirmesine kısaca bakılmalıdır. Yazara göre, ceza hukukunun modern toplumun sorunlarıyla mücadelesinde klasik ceza hukukunun sınırlarını zorladığı ve yeni arayışlar içerisinde olduğu görülmektedir. Bu arayışlar netice itibariyle devlet açısından ikili bir seçeneği mümkün kılmaktadır. Bunlardan biri özellikle son yıllarda kendini gösteren terör eylemleri neticesinde gündeme gelen bir seçenektir. Bu seçeneğe göre, ceza hukukunun kapsama alanının genişletilmesi ve adeta sınırsız bir ceza hukuku oluşturularak ceza hukukunun yeni bir isim altında güvenlik hukuku adı altında incelemeyi arzu etmektedir.¹¹⁰

İkinci çözüm önerisi ise birinci öneriden farklı olarak, modern toplumun sorunlarının tümünü ceza hukuku kapsamına çekme eğiliminden ziyade ceza hukuku dışında ve hatta hukuk dışı önleyici suç siyaseti tedbirlerine başvurulması şeklindedir.

1.5.3.- Peter Alexis Albrecht

Albrecht modern ceza hukuku düşüncesini *Hassamer*'e benzer nitelikte bir dönüşüm sürecinin ürünü olarak görmektedir. Yalnız *Albrecht* söz konusu yaklaşımını 19. y.y.'ın liberal hukuk devletinin 20. yy.'ın sosyal müdahaleci devletine dönüşümü ile açıklamaya gayret etmiştir.¹¹¹ Bu dönüşüm süreci içinde özellikle belli alanlar ortaya çıkmıştır ki bu alanlardaki suç teşkil eden eylemlere karşı mutlak suretle modern ceza hukuku bakımından önleyici fonksiyonun ön plana çıkmaktadır. Öyle ki *Albrecht* bu alanlara örnek olarak çevre suçlarını ve ekonomik suçları örnek olarak göstermekte, bu alanlarda ortaya çıkan problemlerin çözülmesi adına artan sayıda soyut tehlike suçlarına başvurulduğu hukuk devletinin ceza hukuku için belirlediği prensiplere aykırı tedbirler alınmaktadır. Hatta kanun koyucuların dahi tehlike suçlarının istisnai düzenlemeler olduğu gerçeğini unutup aksine düzenleme esasında kural kabul etmeleri üzerinde durmuştur.¹¹² Ancak *Albrecht* de bu tutumu eleştirmekte ve *Hassamer*'e paralel olarak modern toplumun büyüklü küçüklü tüm problemlerinin ceza hukuku bünyesinde çözmeye çalışmanın isabetli olmadığını ve öz bir ceza hukuku yaklaşımı ile ceza hukuku alanını daraltarak dışarıda kalan problemlere karşı

¹¹⁰ **SIEBER**, Ceza Hukukunun Sınırları, sh: 182.

¹¹¹ **ALBRECHT**, Peter, Alexis, Das Strafrecht auf dem Weg vom liberalen Rechtsstaat zum sozialen Interventionsstaat – Entwicklungstendenzen des materiellen Stafrechts, in KritV 1988, sh: 207.

¹¹² **ALBRECHT**, Peter, Alexis, Die Funktionalisierung des Opfers im Kriminaljustizsystem, in: Die Stellung des Opfers im Rechtssystem (Hrgs: Bernd SCHUHNEMANN, Markus Dirk DUBBER), 2000, sh:49.

diğer hukuk alanlarıyla çözüm getirilmesi gerektiğini savunmaktadır. Netice itibariyle *Albrecht* modern ceza hukuku eğiliminin yapısal unsurların kendince şöyle dile getirmiştir.

- 1- Artan sayıda soyut tehlike suçları,
- 2- İhmal ve taksirle işlenen suçlarda sorumluluğun artırılması ,
- 3-Genel şartlar ve belirsiz maddi unsurların yardımıyla suç isnadının basitleştirilmesi.¹¹³

1.5.4.- Felix Herzog

Felix Herzog ise modern ceza hukuku tehlike ceza hukuku olarak karakterize etmeye çalışmıştır. Kendi belirlenimi içinde temel hareket noktasını yine diğer yazarlara paralel olarak (soyut) tehlike suçlarının kapsamlı kullanılabilirliği oluşturmaktadır. Kendi tasarımında kullandığı tehlike kavramı da *Beck'in Risk Toplumu* çözümlemesinde kullandığı kavramsal açıklamaya özdeş bir içeriğe sahiptir. *Herzog* modern ceza hukukunu tehlike suçlarına dayalı bir ceza hukuku sistemi olarak açıklarken ekonomik ve çevre ceza hukukunu modern ceza hukukunun merkezine yerleştiriyor.¹¹⁴

Bu bağlamda tehlikenin interaktif bir sürecin sonucunda oluştuğunu ve statik bir konum teşkil etmediğini savunmaktadır. Başka bir anlatımla tehlike basit bir şekilde yaratılmaz, aksine toplumsal yapının farklı etkileşim ve yorumlama süreçlerinin neticesinde ortaya çıkmaktadır. Bu da, tehlike unsurunun subjektif ölçütlere göre değişim gösterdiği sonucunu ortaya koymaktadır. Böyle olunca *Herzog* tüm modern ceza hukuku sistematüğını iki temel yapı üzerine inşa ediyor: tehlike unsuru ve buna karşı önlemler. Böyle bir tespiti gelişen dünyada ortaya çıkan yeni buluşlar ya da daha karmaşık haline getirilen sistemler ve yeni yapılandırmalardan yani kısacası ekonomik ve teknolojik alanda yeni büyük gelişmelerden hareketle yapmaktadır. Bu bağlamda *Herzog*'un toplumsal bir ihtiyacın neticesi olarak gördüğü tehlike ceza hukuku, söz konusu riskleri aşmak adına sadece adaleti yeniden sağlamakla yetinmeyerek devletin sağladığı var olma güvencesi sisteminin bir parçası olmak anlamını da taşımaktadır.¹¹⁵

¹¹³ HONG, Seung- Hee, Flexibilisierungstendenzen, sh: 79.

¹¹⁴ HERZOG, Felix, Gesellschaftliche Unsicherheit und strafrechtliche Daseinvorsorge, Heidelberg, 1991, 109 vd.

¹¹⁵ HONG, Flexibilisierungstendenzen, sh: 81- 82.

1.5.5.- Cornelius Prittwitz

Özellikle Risk Toplumu ve Risk Ceza Hukuku üzerine çok yoğun çalışmaları bulunan *Cornelius Prittwitz* modern ceza hukukunu risk toplumunun sistematik yapısını esas almak suretiyle değerlendiriyor. Bu yüzden ona göre modern ceza hukukunu risk ceza hukuku olarak kabul etmektedir. Tarihsel süreç içerisinde ceza hukuku düşüncesinin geçirdiği evrim üzerinde duran *Prittwitz* şüandaki ceza hukukunu endüstri toplumunun önleyici ceza hukukundan risk toplumunun yönlendirici ceza hukukuna (*Grosssteuerungsstrafrecht*) dönüştüğü görüşünü savunmaktadır. Bu noktada *Prittwitz'in* risk toplumunu da tehlike toplumu, güvenlik toplumu ve güvenlikten arındırılan toplum olmak üzere üç modelde ele aldığı da belirtilmelidir.¹¹⁶ Tehlike toplumunu endüstriyel gelişimin bir ürünü olarak ortaya çıkan belirsiz, yeni ve insanlığı tehdit eden tehlikelerin şekillendirdiği toplum olarak niteleyen *Prittwitz*, güvenlik toplumunu da endüstriyelleşme ve modernleşme ile bağlantılı tehlikelerin kontrol altına alınabildiği toplum tipi olarak görmektedir.

Tüm bu açıklamaların ışığında *Prittwitz* modern ceza hukuku tasarımını içinde karakteristik suçluluk alanlarını şu şekilde belirtmektedir.

a- Uyuşturucu, para sahteciliği, otomobil hırsızlığı, insan kaçakçılığı ve insanların cinsel amaçlı pazarlanmasına yönelik organize suçluluk

b- Çevre suçları, ekonomik suçlar, rüşvet, irtikap gibi alanlarda şekillenen organize suçluluk

c- Teknolojik gelişmelere paralel olarak ortaya çıkan suçlar, en önemli örnek olarak bilişim suçları¹¹⁷

Bu suçluluk alanlarına dikkati çeken *Prittwitz*, söz konusu alanlardaki hukuka aykırılıklarla mücadele ederken ceza hukukunun diğer kontrol mekanizmalarının – politika ve diğer hukuk alanları – yetersiz ve etkisiz kaldıkları noktada devreye girmesi gerektiğini de vurgulamaktan geri kalmamıştır. *Prittwitz'in* modern ceza hukukunda risk ekseninde ortaya koyduğu bakış açısının önemli bir boyutunu da riskin derecesine göre getirdiği ayımdır¹¹⁸. Çünkü yazar her türlü riskin ceza hukuku kapsamında değerlendirilmesini isabetli

¹¹⁶ **PRITTWITZ**, Risiken, sh: 52.

¹¹⁷ **HONG**, Flexibilisierungstendenzen, sh: 87.

¹¹⁸ **PRITTWITZ**, Risiken, sh: 60 v.d.

görmemektedir. Çünkü bu takdirde risklerden örülü bir dünyada ceza hukukunun her şeye yetişmesinin mümkün olamayacağını, aksi takdirde yaşamı idame ettirmenin ciddi ölçüde engelleneceğini ifade etmektedir. Bu yüzden ceza hukuku yaptırımını gerektirmeyecek ölçüde, toplumsal düzeni bozmayacak ve yaşamın olağan akışı içinde kaldırılabilir bir takım riskleri “izin verilen risk” çerçevesinde kabul ederek ceza hukukunun uygulama alanı dışında bırakmıştır¹¹⁹.

1.5.6. Eric Hilgendorf

Özellikle modern ceza hukuku tasarımı esnekleştirme eğilimlerinin önemine vurgu yapan *Hilgendorf* ise internet suçluluğunu model suçluluk alanı olarak kabul etmiştir. Çünkü modern toplum olarak kabul gören risk toplumunun tüm unsurlarını bünyesinde bulduran en güncel araç olarak interneti görmektedir. Keza ceza hukukunun esnekleştirilmesi düşüncesinin altında modern toplumun problemlerinin çözülmesi için ceza hukukunun daha rahat uygulanabilir hale getirilmesi adına geleneksel dogmatik yapıların çözülmesi yaklaşımının bulunduğunu savunan *Hilgendorf* çevre suçları ve ekonomik suçlar kadar ve hatta günümüz gelişmeleri ışığında onlardan daha da öncelikli olarak internet suçluluğunun dikkate alınması ve tüm bu tartışmalar için bu suçluluk alanının model teşkil ettiğini ortaya koymuştur.¹²⁰ Bu çerçevede modern ceza hukuku düşüncesine paralel olarak ceza yasalarının aşağıdaki temel prensipler dahilinde şekillendiğini kabul etmektedir.

a- Ceza hukuku hukuksal değerlerin korunması açısından “ultima ratio” değil “prima ratio” olarak anlaşılması.

b- Müphem bir şekilde formüle edilen evrensel hukuksal değerlerin uygulanması / esas alınması

c- Soyut tehlike suçlarıyla ön alanın cezalandırılması.

d- Ceza hukuku dogmatığının esnekleştirilmesi.

e- Mağdur ve hukuksal değer yönelimli çekirdek ceza hukukunun görecelendirilmesi.¹²¹

¹¹⁹ *Prittwitz*'in yaklaşımına yönelik değerlendirmeler bakımından bkz. ÜNVER, İzin Verilen Risk, sh: 10 – 12.

¹²⁰ HILGENDORF/FRANK/VALERIUS, Computer- Internetstrafrecht, sh: 198-199.

¹²¹ HONG, Flexibilisierungstendenzen, sh: 90.

1.5.7. Yener Ünver

Türk doktrininde yaşayan modern ceza hukuku olarak ifade ettiğimiz yaklaşım ile ilgili çalışmalarla ilgili son zamanlara kadar pek sık karşılaşılmadığı görülmektedir. Ancak son yıllarda klasik anlamda idealize edilmiş bir modern ceza hukuku anlayışının yanında yaşayan modern ceza hukukunun temel problemleri de sorunsallaştırılmaya başlanmıştır. Örneğin yukarıda ifade edildiği üzere modern ceza hukukunun görünüm tarzlarından olan Risk Ceza Hukuk, Tehlike Ceza Hukuku, Düşman Ceza Hukuku¹²² gibi anlayışlar yine bu yazar topluluğunun öncülüğünde Türk Literatüründe incelenmeye başlanmıştır. Konu bütünlüğü çerçevesinde Türk doktrinindeki konu ile ilgili bakış açısına örnek olarak *Ünver'in* değerlendirmelerini ortaya koymakta fayda vardır.

Ünver, modern ceza hukuku öğretisinin temelinde hukuksal değer kavramını yerleştirmiştir¹²³. Yazara göre günümüz ceza hukuku öğretisinde ceza hukukunun anlam ve amacının hukuksal değerlerin korunmasıyla oluştuğunu ve geliştiği kabul edilmektedir. Bu yaklaşım tarzı itibarıyla *Hassamer'in* modern ceza hukuku tasarımı gerçekleştirdiği dörtlü ayırımını esasında hukuksal değerlerin korunması öğretisinin bir bütünlük oluşturan parçaların tek tek ifadesi olarak görmekte ve sadece hukuksal değerlerin korunması öğretisinin isabetli bir biçimde ortaya konulmasıyla tüm bu parçaların açıklanabileceğini savunduğu görülmektedir.

Yazar özellikle ceza hukukunun ödevi ile hukuksal değerlerin korunması öğretisi arasında bir ilişki kurmuş ve ceza hukukunun temel ödevinin hukuksal değerlerin tehlikeye ve zarara sokulmasının önlenmesi olduğunu ifade etmiştir. Bu ilişki de beraberinde hukuksal değerlerin korunması öğretisinin kanun koyucuya yönlendirdiği bir eleştirisel fonksiyonunun mevcudiyetini ortaya koymaktadır. Bu noktada *Ünver*, modern ceza hukuku ile klasik ceza hukuku arasındaki ilişkiye bu eleştirisel fonksiyonunun anlaşılma tarzları penceresinden bakmaktadır¹²⁴. Buna göre klasik ceza hukukunda hukuksal değerlerin korunması öğretisinin yüklediği eleştirisel fonksiyonun suç olmaktan çıkartma yönünde bir eğilim gösterirken, modern ceza hukukunda bu eğilimin değişikliğe uğradığı ve kanun koyucuya suç haline getirme bakımından yükümlülük yükleme yönünde olduğu görülmektedir. Bu yönelimin

¹²² Proje Yöneticiliğini Kayıhan İÇEL'in, editörlüğünü Yener ÜNVER'in yaptığı Karşılaştırmalı Ceza Hukuku Serisinin 8. cildi olan "Terör ve Düşman Ceza Hukuku", Türkiye'de bu konunun kapsamlı olarak ele alındığı ilk çalışma olma özelliğini taşımaktadır.

¹²³ ÜNVER, TCK ve Ceza Kanunu Tasarısının Değerlendirilmesi, sh: 51.

¹²⁴ ÜNVER, TCK ve Ceza Kanunu Tasarısının Değerlendirilmesi, sh: 54.

nedeni üzerinde tartışan yazar, toplumsal gelişim süreci içerisinde birey- toplum- devlet ilişkisinin gün geçtikçe değişime uğraması ve bu değişimin yeni bir takım hukuksal değerlerin oluşumuna etki gösterdiği üzerinde durmuştur. Ortaya çıkan her yeni hukuksal değer çoğunlukla beraberinde ceza hukuku korumasını da getirmektedir. Ancak artan sayıda risk ve tehlikelere bağlı olarak hukuksal değer ihlallerin kapsamı ile birlikte cezalandırılabilirlik alanı genişlemekte, buna bağlı olarak cezalandırılabilir hareket sayısı artarak tüm ihlal teşkil eden eylemleri suç haline getirme yönelimi kendini hissettirmektedir. Bunun en önemli göstergelerinden biri olarak soyut tehlike suçlarındaki artışı göstermektedir¹²⁵.

Ancak *Ünver* bu yönelimi açık bir şekilde eleştirmekte ve bunun nedeni olarak da hukuksal değerlerin korunması teorisinin doğru bir şekilde anlaşılması veya yorumlanamaması olarak görmektedir. Yazara göre hukuksal değerlerin korunması öğretisinin temelini bireyin özgürlüğü oluşturmaktadır¹²⁶. Bu özgürlük alanı bireyin toplumda huzur ve güven içinde yaşamak gereksiniminin zorunlu bir unsuru olsa da, bu özgürlük toplumun diğer bireylerinin eş özgürlük alanlarını ihlal edemez. Başka bir ifade ile bireyler arasında bu özgürlüğün karşılıklı sınırlandırılmasını gerektirir. Bu sınırlandırma da hukuksal meşruiyeti haiz bir tarzda, yani kanun koyucu inisiyatifine bağlı olarak gerçekleşmelidir. Kanun koyucunun anılan özgürlük kullanımlarına ilişkin müdahaleleri olarak adlandırılacak düzenlemeleri, hukuksal değerleri koruma gerekçesiyle dahi olsa, liberal devlet anlayışıyla ve insanın otonom yapısı ve özgürlüğü göz önünde tutularak yapılmalıdır. Aksi bir tutum, *Jakobs'un* saptamalarını gündeme getirecek, hukuksal değerlerin aşırı, olağan sınırlar aşarak korunmak istenmesiyle, hukuksal değer ihlallerinin özneleri hukuksal değerlerin düşmanı sayılacak ve bir “düşman ceza hukuku” oluşumuna yol açacaktır. Bu açıklamaların ardından yazar, ceza hukukunu sınırlı bir hukuk alanı olarak görüp bu tür sınırlamaların temel ilkeler yanında, toplumsal yaşam dinamikleriyle de uyumlu olmasına özen gösterilmesi gerektiğini düşünmektedir¹²⁷.

Ünver yukarıda aktarılan edilen eleştiriyi internet aracılığıyla ilenen suçları değerlendirirken naklen şu şekilde ifade etmiştir.

¹²⁵ ÜNVER, Hukuksal Değer, sh:958-959.

¹²⁶ ÜNVER, Hukuksal Değer, sh: 1058.

¹²⁷ ÜNVER, Hukuksal Değer, sh:1059.

“Kanun koyucu suç tiplerini yaratırken şüphesiz bireyin hukuksal değerleri, bu değerlerden yararlanması kadar, onun toplum içindeki yaşam alanını, izin verilen hareket serbestisi alanını da göz önünde tutmak zorundadır. Bir taraftan (ceza hukukundaki teknik ihlal anlamı dışında) hukuksal değerleri ihlal veya ihlal riski yaratan, diğer yandan ise bireyin toplumsal yaşamı açısından hukuksal değeri koruyan tipik ihlal modellerinin çizdiği “koruma alanları” ile izin verilen risk alanları arasında dengeli “doğru alanlar” in nasıl belirlenebileceği hem anayasa hem de ceza hukukunun en önemli sorunlarından birisidir. Çünkü toplumsal yaşamın durağan hale getirilmesinin de bazen dinamik, yüksek teknolojiyle iç içe yaşayan bir toplumsal yaşam biçimi gibi bazı hukuksal değerler hakkında ceza hukukunun dışındaki anlamıyla ihlal veya ihlal riski yaratabileceği kabul edilmektedir. ... Günümüzde artık, ceza hukukunun amacı yalnızca çok önemli hukuksal değerleri ve bunları da yalnızca bazı ihlal modellerinden korumaktır. Cezaya liyakat ve cezaya muhtaçlık ölçütleri suç politikası açısından kanun koyucuya bu konuda yol gösterici ve onu sınırlayıcı ölçütlerdir. Hukuksal değerlerin ceza hukukuyla layıkıyla korunmaları ve dinamik bir toplumsal yaşam modeli arasında iyi bir denge kurulmalı, bu denge değişen toplumsal yaşam biçimi ve koşullarına göre de sürekli gözden geçirilmelidir.”¹²⁸

Bahsedilen bu dengenin en önemli unsurlarından biri de tüm hukuksal değer ihlallerini ceza hukuku kapsamına sokmadan sadece katlanılmaz hukuksal değer ihlallerinin cezalandırılmasıdır. Yazara göre hukuk bireyin hukuksal değerlerini korumalıdır; ancak koruma alanları yaratırken, özellikle de bu alanda ceza hukuku aracına başvurulurken hiç göz ardı edilmemesi gereken bir husus ise, hukukun toplumsal değişim ve gelişimi durduramayacağı, durdurma veya yavaşlatmaya girişmemesi gerektiğidir.

1.5.8.- Görüşlerin Değerlendirmesi

Görüşleri yansıtılan yazarların modern ceza hukuku anlayışını nasıl yorumladıklarına bakılacak olursa, bazı noktalar açısından ortak bir bakışın varlığı kabul edilebilir. Her şeyden önce modern ceza hukuku, modern toplumunun sorunları üzerinden şekillenen ve insanların bu toplum yapısı içinde huzurlu, barış ve güven içerisinde yaşamalarını mümkün kılacak koşulların güvencesi olarak düşünülmektedir. Dolayısıyla ceza hukuku ve toplum dinamikleri arasında bir ilinti kurulmuştur. Bu ilintinin taraflarından biri olan modern toplum ise bilim ve teknolojinin gelişmesi ile birlikte daha da karmaşık hale gelen bir risk toplumu olarak

¹²⁸ ÜNVER, TCK ve Ceza Kanunu Tasarısının Değerlendirilmesi, sh: 60.

tasarlanmıştır. Böylece modern ceza hukuku anlayışı, risk toplumunun karmaşıklaşan yapısı içinde ortaya çıkan sorunların çözülmesine elverişli ve fonksiyonel bir ceza hukukuna ulaşma kaygısıyla şekillendirilmeye çalışılmıştır¹²⁹.

Bu kaygı temelinde *Hassamer, Sieber* ve *Hilgendorf* da görüldüğü üzere klasik ceza hukuku formlarının söz konusu sorunları çözmeye yeteri kadar elverişli olmadığı, dolayısıyla klasik ceza hukukunda bir takım yapısal değişikliklere gidilmesi gerektiği düşünülmektedir. Özellikle dünyada terörle, uyuşturucu ve insan kaçakçılığı ile birlikte siber suçlar alanında son yıllarda konun koyucu iradesinin cezalandırılabilen alanın genişletilmesi veya başka bir ifade ile cezalandırılabilirliğin öne çekilmesi, soyut tehlike suçlarındaki artışı ve ceza hukuku normlarının risk kaynaklarıyla etkin mücadelede ilk araç olarak kullanılması yönünde bir eğilime yönelmesini bu duruma bağlamaktadırlar. Ancak bu noktada da *Hassamer, Prittwitz* ve *Ünver*'in çekinceleri de mutlak suretle hatırlanmalıdır. Öyle ki, *Hassamer* ceza hukukunun etkililiğini ön plana çıkartmaya çalışan bu yönelimlerin ceza hukukunu hukuk devleti ekseninden kaydıracağını ifade ederken, *Prittwitz* ve *Ünver* de aynı yönde bir temellendirmeye ceza hukukunun sorunu çözebilecek bir sihirli değnek olarak görülmemesi gerektiğini, bir hukuksal değer ihlalinin cezalandırılabilirliğinin cezaya liyakat ve cezaya muhtaçlık koşullarını gerçekleştirmeye elverişli olmasının aranmasını ifade etmişlerdir. Kanaatimizce bu yöndeki düşünceleri, her iki yazarın da modern risk toplumunda “izin verilen risk” teorisine verdikleri önemden kaynaklanmaktadır. İzin verilen risk ile ilgili dördüncü bölümde internet süjelerinin ceza sorumluluğu değerlendirilirken ayrıntılı bir biçimde ele alınacaktır.

Son olarak da, çalışma konusuyla ilişkinin ortaya konulması anlamında hemen hemen tüm yazarlar modern toplumun dinamiğini ve bir ölçüde de modern ceza hukukunun gelişim seyrini belirleyen temel risk kaynakları içinde bilişim – iletişim teknolojisindeki gelişmeye ve dünyanın git gide bilgisayar sistemlerine bağımlı hale gelmesine paralel olarak bilişim sistemlerini ve özellikle de interneti öncelikli olarak değerlendirmektedirler. Bunun kaynağında da internetin sınır aşan etkisi, kontrol edilemezliği ve hayatın tüm alanlarına nüfuz etmesi yatmaktadır.

1.6.- Modern Toplumun Temel Dinamiklerinden Olan İnternet Teknolojisinin Gelişim Seyri

¹²⁹ **HILGENDORF**, Strafrechtliche, sh: 45 v.d.

Bilgi ve iletişim teknolojilerinde özellikle 20. yüzyılın ikinci yarısından itibaren yaşanan ve her geçen gün hızını arttırarak devam eden gelişim ve değişim sosyal, siyasi, ekonomik alanda birçok dinamiğin yeniden tanımlanmasına ve buna bağlı olarak yeni anlam içerikleriyle zenginleştirilmesine neden olmuştur.¹³⁰ Bu gelişimin en bariz örneği ve itici güçlerinden biri hiç şüphesiz bilgi – iletişim teknolojisinin özellikle de internet teknolojinde yaşanan gelişmelerdir.

İnternet, insanların her geçen gün gittikçe artan "üretilen bilgiyi saklama/paylaşma ve ona kolayca ulaşma" istekleri sonrasında ortaya çıkmış bir teknolojidir. Bu teknoloji yardımıyla pek çok alandaki bilgilere insanlar kolay, ucuz, hızlı ve güvenli bir şekilde erişebilmektedir. Bilgi ve iletişim teknolojilerinin bu anlamda günümüzde en önemlisi hiç şüphe yok ki internet teknolojisidir. İnternetin sağladığı sanal paylaşım ortamı ile sınırlar ortadan kalkmakta ve 21. yüzyılın temel kaynağı olan bilginin her türüne rahatlıkla ulaşılabilir. Bilindiği üzere internet, iletişim teknolojilerinin mümkün kıldığı, bilgisayarlar vasıtasıyla insanları birbirine bağlayan, fiziksel mekandan bağımsız sanal bir iletişim, bilgi, ticaret, eğlence ve paylaşım ortamıdır.¹³¹ İnternet dünya üzerindeki milyonlarca bilgisayarın birbirine bağlanmaları ile oluşan global bir bilgisayar ağları sistemini ifade edilirken aynı zamanda da dünyada üzerindeki bilgisayar ağlarının aralarında tekrar bağlantı kurmaları ile büyüyen bir "ağlararası ağ" niteliği internetin en önemli karakteristiğini yansıtmaktadır.¹³² Keza Amerikan Yüksek Mahkemesi İnterneti "*... birbirleri ile bağlı bulunan bilgisayarlardan oluşan uluslar arası ağ ... bireylerin dünya çapında haberleşmesi için tamamen yeni ve benzeri olmayan bir ortam ...*" şeklinde tanımlamıştır.¹³³ Yine Amerikan Yüksek Mahkemesi de 28.09.1995 tarihli Whirlpool Financial Corporation v. GN Holdings davasında verdiği kararda, internetin tarama yapılarak bilgiye erişimin sağlanması dolayısıyla, herkesin kullanımına ve erişim sağlamasına açık olması ölçüsünde bir bilgi ve iletişim aracı olduğu yönünde bir tanımlamaya gitmiştir¹³⁴. *Akgül* de interneti bir bilgisayar ağının ötesinde, insanları ve insanlığı düşünce ve kültür ürünlerini kapsayan bir ağ olarak görürken internet üzerinde 1.4 milyar insan olduğunu ifade etmiştir. Ayrıca yazarın

¹³⁰ Bkz. Giriş, sh: 5 v.d.

¹³¹ **YALÇIN**, Sosyolojik, sh: 78.

¹³² **SINAR**, İnternet, sh: 21.

¹³³ **YAZICIOĞLU**, Yılmaz, Bilgisayar Marifetiyle İşlene Suçlar: Sanal Suçlar, in: Panel – Bilişim Suçları (Adalet Bakanlığı Hakim ve Savcı Adayları Eğitim Merkezi Başkanlığı), Ankara, 2001, sh: 32.

¹³⁴ **KAPLAN**, Yavuz, İnternet Ortamında Fikri Hakların Korunmasına Uygulanacak Hukuk, Ankara, 2004, sh: 23.

verdiği bir başka istatistiğe göre 570 milyon bilgisayar internet alan adı sistemi DNS'e kayıtlı durumdadır¹³⁵.

İnternet ilk olarak ABD'de askeri amaçlı bir proje ile ortaya çıkmıştır. 1960'lı yıllarda soğuk savaş döneminin nükleer çatışma tehdidi yüzünden savunma amaçlı projelere büyük harcamalar yapılmaktaydı. ABD tarafından geliştirilen ve ARPANET (Advanced Research Projects Authority Net) adı verilen proje, ülke savunmasını birbirine bağlı bilgisayarlarla kurulacak iletişimle koordineli bir biçimde sağlamak amacıyla 1969 yılında geliştirilmiştir. Projeye göre herhangi bir bilgisayarın devre dışı kalması ağa bağlı diğer bilgisayarları etkilemeyecek ve iletişim devam edecekti. Ağ düzenleyen ya da denetleyen herhangi bir merkez bulunmadığından sürekli ve kesintisiz bir iletişim mümkün olabilecekti. Bugünkü İnternet'in temelini oluşturan bu projede daha sonra aynı ağa başka yeni bilgisayarların eklenmesiyle ağ üzerinden iletişim giderek arttı ve çok sayıda kullanıcının yararlandığı elektronik mektup, tartışma listeleri, forumlar, dosya transfer hizmetleri gibi yeni kullanım alanları ortaya çıktı.¹³⁶

ARPANET'ten başka bilimsel amaçlı NSFNET (National Science Foundation) 1986 yılında, ticari amaçlı Comuserve gibi yeni ağlar da kullanıma açıldı. İlk olarak 1973 yılında birbirinden farklı ağların aralarında veri iletimi sağlayabilecekleri, ortak bir dil oluşturularak birleştirilmeleri kararlaştırılmıştır¹³⁷.

Bu amaçla geliştirilen TCP/IP (Transmission Control Protocol / Internet Protocol) kullanılmaya başlandı. TCP/IP, İnternet üzerinde yer alan farklı özellikte bilgisayarların ve ağların birbirleriyle sağlıklı bir şekilde iletişim kurabilmelerini sağlayan ortak bir dil olarak geliştirilmiştir. İnternet'in gelişmesindeki son aşama ise WWW'in (World Wide Web)

¹³⁵ **AKGÜL**, Mustafa, İnternet Yasakları ve Hukuk, in: TBB, Sayı:78, Ankara, 2008, sh: 354.

¹³⁶ Konu ile ilgili detaylı Açıklamalar için bkz. **İÇEL**, Kayıhan/**ÜNVER**, Yener, Kitle Haberleşme Hukuku, 7. Baskı, İstanbul, 2006, sh: 469 v.d.; **SINAR**, İnternet, sh: 22.

¹³⁷ **ÖZDİLEK**, Ali Osman, İnternet ve Hukuk, İstanbul, 2002, sh: 19.

geliştirilmesidir.¹³⁸ WWW İnternet kullanımını ve kullanıcılarının artmasında sağladığı kolaylıkla önemli bir işlevi yerine getirmiştir.¹³⁹

İnternet teknolojisinin geçirmiş olduğu evrimi tarihsel süreçteki yansımalarını esas alarak üç aşamaya ayıran *Floridi* bu aşamaları sırasıyla “*buluş*”, “*reform*” ve “*yayılma*” olarak belirlemiştir.¹⁴⁰ Birinci aşama olan “*buluş*” yukarıda ortaya konulduğu şekliyle 1968 yılında ABD’nin ARPANET olarak adlandırılan bir projeyi destekleme kararı alması ve askeri amaçlarla kullanılması tasarlanan bilgi - iletişim ağının işlerlik kazanması çerçevesinde bir anlam kazanmaktadır. Burada bahsi geçen ve internetin primitif halini teşkil eden bilgi - iletişim ağı dönemin soğuk savaş şartları içinde güvenlik kaygılarının bir neticesi olarak, bir savaş durumunda askeri ve idari kurumların birbirleriyle olan iletişimini sağlıklı olarak kurulması amacıyla tasarlanmıştır. Bu bağlamda tasarlanan ARPANET projesinin temel hedefi, ciddi yapısal zarar verici eylemlere rağmen güvenilir ve hızlı bilgi akışını sağlayacak bir iletişim sisteminin, bir ağın oluşturulması olmuştur. “*Bu dönem içerisinde bilgisayar sistemlerinin birbiriyle bağlantı kurabilmesini sağlayan teknolojilerin gelişimi, TCP/IP protokolü, enformasyonun gönderildiği hedefe ulaşabilmesi amacıyla küçük paketlere ayrılması ve öngörülen hedefe bu şekilde gönderilmesi anlamına gelen paket anahtarlama teknolojisi, alan adı sistemi bugünkü anlamıyla internetin altyapısının oluşturulması anlamında önemli adımları oluşturmaktadır.*”¹⁴¹

Yazarın “reform” aşaması olarak ifade ettiği aşama 1984-95 yılları arasını kapsayıp, bu aşamayla artık internetin sadece askeri amaçlara özgülenmiş bir bilgi – iletişim ağı olmanın ötesinde daha geniş alanlarda kullanılmaya bağlı olarak sosyal ve özellikle de ekonomik hayatta kullanılmaya başlaması ile geçirdiği değişimi kastetmektedir. 1990’lı yıllarda ticari ve eğitim amaçlı internet servis sağlayıcıların ortaya çıkması, 1995 yılında NSFNET aracılığıyla yürüten alan adları hizmetlerinin serbest bırakılması bu süreci tamamlayan bir unsurlardır. Böylece internet dar veya kapalı alan ağ sistemi olmanın ötesine geçerek özellikle de

¹³⁸ **AKGÜL**, Mustafa, Bilgi Toplumuna Göre İnternet, <http://bid.ankara.edu.tr/start/Internet/bil-toplum.html> (Erişim Tarihi: 19.09.2007, Saat:16:00).

¹³⁹ Bu gelişmeleri, günümüzde de çok yoğun olarak kullanılan ve İnternet ortamında gezintiyi olanaklı kılan “browser” adı verilen programlar (İnternet Explorer, Netscape, Mozilla vb.) izledi ve internetin popülaritesine önemli ölçüde artmıştır. Bu programlarla sadece metinlere, resimlere, ses ve videolara ulaşım gittikçe kolaylaştırılarak çok fazla eğitim gerektirmeksizin pek çok insanın İnternet’e erişimi sağlanmış ve bu anlamda büyük dönüşümler yaşanmıştır. Konu ile ilgili detaylı bilgi için bkz. **YALÇIN**, Sosyolojik, sh: 78-79.

¹⁴⁰ **KETİZMEN**, Muammer, Türk Ceza Hukukunda Bilişim Suçları, Ankara, 2008, sh:21.

¹⁴¹ **KETİZMEN**, Bilişim Suçları, sh: 21.

ekonomik kaynak desteğinin etkisiyle küreselliğe uzanan bir etki ve kullanım genişliğine sahip olmuştur. Bu gerçeğin fark edilip içselleştirildiği bu dönem bu bakımından bir ara dönem özelliği taşımaktadır.

İnternetin gelişim süreci içerisinde tamamlanmayan ve bundan sonraki süreçte dinamizmini koruyacağı öngörülen son aşama ise “yayılma” aşamasıdır. Bu aşama internetin yayılmış olduğu veri aktarımı ve iletişim hizmetlerinin toplumsal yaşama tartışılmaz katkılarının geniş kitlelere ve küresel ölçekte yayılması ve insanların bu teknolojiyi yaygın bir biçimde kullanması sürecini ortaya koymaktadır. Aslında bu son aşama itibariyle internetin hukuk ve bilhassa ceza hukuku alanına çekilmesi durumu söz konusu olmaktadır.

İfade edildiği üzere bilgisayarın her toplumsal kesimden insan tarafından ulaşılabilir ve kullanılabilir olmasıyla interneti kullananların sayısı artmış ve bu artışla da internetin doğrudan ya da dolaylı olarak etkisinin hissedilmediği hiçbir alan kalmamıştır. Bu durum da internet'in sosyal bir olgu olarak tartışma konusu edilmesine zemin hazırlamıştır. Şöyle ki, her geçen yıl internet kullanıcılarının hızla arttığı bir durumda¹⁴² bu sanal ortam mevcut yaşam koşullarını geliştirme ve yeni imkanlar yaratma adına bilgiye ulaşımı mümkün kılacak amaçlar dışında, toplumsal düzeni zedeleyecek nitelikte değer ihlallerine (mal varlığı değerleri, şahıs varlığı değerleri, kamusal barış... v.b.) de kaynaklık teşkil etmesi madalyonun diğer yüzünü oluşturmaktadır. Özellikle son on yıl içinde internetin araç olarak kullanılması suretiyle gerçekleştirilen hukuka aykırı eylem ve işlemlere yönelik çalışmalar ortaya koymaktadır ki, bilgi ve iletişim teknolojisi alanındaki devrimsel gelişim ve dönüşüm sadece modern toplumun morfolojik yapısını şekillendirmemekte buna bağlı olarak toplumsal düzenin kaynağı olan hukukun yeniden ve zamanın koşullarına uygun olarak sistematize

¹⁴² Türkiye genelinde yapılan bir ankete göre, Türkiye'de internet kullanıcılarının sayısı 2000'de yedi katına çıktı. Araştırma, geri kalmış olarak kabul edilen Doğu ve Güneydoğu Anadolu'da bile her 10 kişiden birinin internet kullandığını gösterdi. IBS Araştırma ve Danışmanlık Şirketi'nce Türkiye genelinde 5 binin üzerinde ev dolaşarak yapılan ankette, 12-17, 18-34 ve 35 yaş üstü olmak üzere üç ayrı yaş grubu esas alınmış. Araştırmadan elde edilen sonuçlar şöyle: 3. 5 milyon kişi internette n Doğu Anadolu ve Güneydoğu Anadolu Bölgesi'ndeki her 10 kişiden biri internet kullanıcısı. Türkiye'deki 3 milyon 600 bin internet kullanıcısının yüzde 9.7'si Doğu Anadolu, yüzde 9.4'ü ise Güneydoğu Anadolu'da bulunuyor. Yüzde 609'luk artış n Türk internet abonelerinin sayısı 2000 yılı içinde yüzde 609 oranında artmış. * Katılanların yüzde 45'i internetin hayatını etkilediğini belirtiyor. Deneklerin yüzde 43'ü internet kullanmaya başladıktan sonra daha az televizyon seyrettiğini ifade ederken, yüzde 58'i daha az gazete okuduğunu 'itiraf' ediyor. 'Chat' ilk sırada n Kullanıcıların yüzde 75'i interneti 'chat' yapmak, yüzde 65'i e-posta hizmetleri için kullanıyor. * E-posta hizmetinden yararlananların yüzde 64'ü e-postayı tanıdıklarıyla haberleşmek için kullanıyor. 'Chat' yapanlar arasında 12-17 yaş grubunda 'chat'leşme oranı yüzde 90 iken 35 yaş ve üstünde bu oran yüzde 63'e iniyor. Kullanıcıların sadece yüzde 16'sı banka işlemlerini internetle yaparken, e-alışverişçilerin oranı yüzde 6. İngilizceden sonra Kürtçe n 1509 kullanıcının yüzde 51.5'i İngilizce bilirken, onu yüzde 9.3 ile Kürtçe izliyor. Daha sonra sırasıyla Almanca, Fransızca, Arapça, İspanyolca ve İtalyanca gibi dünyanın sıklıkla kullanılan diller gelmektedir. Kaynak: http://www.haberturk.com/look.asp?N_Id=10640 (Erişim Tarihi: 15.10.2007, Saat: 15:00)

edilmesini zorunlu kılmaktadır. Günümüzde çocuk pornografisi, ırkçılık ve yabancı düşmanlığına ilişkin fiiller internetin kullanımının yaygınlaşmasıyla birlikte dünya gündemine girmiştir. Zaten bu konular özellikle son yıllarda başta Avrupa Konseyi Siber Suçlar Sözleşmesinin ve ek protokolü olmak üzere birçok uluslar arası düzenlemelerin konusu haline gelmiştir.

1.7. – İnternetin Bir Suçluluk Alanı Olarak Normatif Ceza Hukuku Alanına Dahil Edilme Süreci

İnternetin ceza hukukunun bir düzenleme alanı haline gelmesi yukarıda yaşanan gelişmelerin sosyal yansımalarına paralel olarak gelişmiştir. Bu sebeptendir ki, internete dair ceza hukuku düzenlemeleri üzerinde analizler yapılırken temsil ettiği toplum modeli ve bu modelin şekillendirdiği ceza hukuku anlayışının farkındalığı ile hareket etmek gerekmektedir. Geçmişe bakıldığında internetin ceza hukuku alanında düzenlenmesi serüveni tabi ki öncelikle bilgisayar ve ilk bilişim sistemlerinin atfedilen hukuksal değerlerin korunmasında diğer hukuk disiplinlerinin yetersiz kalması ve son araç olarak (ultima ratio) ceza hukukun kullanılması ile başlamıştır¹⁴³. Bazı devlet ve uluslar arası kuruluşlar 70’li yılların ikinci yarısından itibaren bilgisayar kullanımının yaygınlaşması ve farklı sosyal yaşam alanlarında kullanılmaya başlanması sebebiyle ortaya çıkan sorunların çözümüne yönelik çalışmalar yapmışlardır.

Bu anlamda bilişim suçlarına yönelik ilk toplantılardan biri 13 Mayıs 1974’de Parlamentolar Arası Çalışma Birliği’nin Bonn’da yaptığı toplantıdır. Bu toplantıda bilişim sistemlerinden yararlanan insanların, bilişim sistemlerinin kötüye kullanılmasından doğan tehlikeler ve bilişim sistem ihlalleri hakkında bilgi eksikliğine sahip olmaları, bilişim sistemlerinin kötüye kullanılması ve ihlallerinin önlenmesi için gerekli yüksek bütçeli yatırımlardan çekinildiği gözler önüne serilmiştir. Ayrıca toplantı esnasında kötüye kullanma ve ihlallerin önlenmesi için kanun zoru ile alınması gereken asgari tedbirler de tartışılmıştır. Ancak teklif, bilişim sistemleri üreticileri ve bilişim sistemleri kullanıcıları tarafından işletmenin iç organizasyonuna müdahale sayıldığı için reddedilmiştir¹⁴⁴.

¹⁴⁴TIEDEMANN, Klaus Bilgisayarla (Kompüter) İşlenen Suçların Ceza Hukuku Yönünden İncelenmesi (Çev.: Feridun Yenisey), İÜHFİM, C.:XLI, S.:1-2, İstanbul, 1975, sh: 331,332.

Avrupa Konseyi 1970’li yıllarda elektronik bilgi bankalarında işlenen veriler dolayısıyla, bireylerin özel hayatının korunması amacıyla yönelik bir dizi çalışma başlatmıştır. 1973 ve 1974 yılında Avrupa Konseyi Bakanlar Komitesi, elektronik veri bankalarında uygulanacak ilkeleri kapsayan 2 tavsiye kararı kabul etmiştir. Bu tavsiye kararı uyarınca başta Almanya olmak üzere Avusturya, Fransa, Danimarka, Norveç gibi ülkeler 70’li yılların sonunda “Verilerin Korunması” konusunda özel yasaları hukuk mevzuatlarına dahil etmişlerdir¹⁴⁵.

Bu girişimlerin devamında dönemin Avrupa Topluluğu tarafından 1981 yılında İspanya’da gerçekleştirilen toplantıda “bilgisayar teknolojisi ile çevrelenen toplumda yaşanan ihlaller” konusu tartışılmıştır¹⁴⁶. İletişim sistemlerinde meydana gelen gelişmeler ve veri iletişim hızlarının ülkelerarası çok yüksek hızlarda yapılması karşısında elektronik veri bankalarında saklanan, kişilerin özel hayatlarına ilişkin verileri koruma konusunda Avrupa Konseyi üyesi ülkelerin mevzuatlarının yetersiz kalmasından dolayı, konuyu uluslar arası boyutta ele almak ve uluslar arası bir sözleşme ile düzenlemek gereği doğmuştur. “*Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması*”na ilişkin 108 sayılı sözleşme, 28 Ocak 1981 tarihinde imzaya açılmış ve aynı tarihte Avrupa Konseyi üyesi ülkelerle birlikte Türkiye tarafından da imzalanmıştır.

Bilişim suçları alanında karşılaştırmalı olarak ceza yasalarının birbiri ile uyumlaştırma çalışmalarına ilk kez 1983 yılında OECD ülkelerinde başlanmıştır. Bu çalışmalar 1986 yılında sonuçlanmış ve “Bilgisayarla İlgili Suç: Hukuki Politikaların Analizi” raporu ile üye ülkelere birtakım ihlalleri müeyyide ile karşılamak için gerekli düzenlemeleri yapmaları tavsiye edilmiştir. OECD tarafından hukuki düzenleme altına alınması tavsiye edilen ihlaller şunlardır;

- Bilgisayar yoluyla dolandırıcılık
- Bilgisayar yoluyla sahtecilik,
- Bilgisayar program ve verilerinde değişiklik yapılması,
- Bilgisayar programlarının telif haklarına aykırı olarak kopyalanması, çoğaltılması ve dağıtılması,

¹⁴⁵ **DEĞİRMENCİ**, Bilişim Suçları Alanında Yapılan Çalışmalar ve Bu Suçların Mukayeseli Hukukta Düzenlenişi, Kaynak: <http://www.caginpolicisi.com.tr/37/59-60-61-62-63-64.htm> (Erişim Tarihi: 08.11.2007, Saat: 00:15).

¹⁴⁶ **YAZICIOĞLU**, Bilgisayar Marifetiyle, sh: 26.

- Telekomünikasyon sistemlerinin, bilgisayarın diğer fonksiyonlarının ve iletişiminin değişikliğe uğratılması¹⁴⁷.

Yine 1985 yılında Suç Problemleri Avrupa Konseyi'nce "bilgisayar suçları hakkında çeşitli araştırmalar yapmak ve bu suçluluk türüyle savaşta başarılı olmak için" uzmanlar komisyonu oluşturmuştur.¹⁴⁸ Bununla birlikte aynı konuya angaje olmuş olan Birleşmiş Milletler Teşkilatı da 1985 Milano, 1988 Küba toplantılarıyla internet de dahil olmak üzere bilgisayar ağları vasıtasıyla işlenen suçlara karşı savaşımın temel prensipleri üzerinde tartışılmıştır.

Bu arada gerek geniş anlamda bilişim suçları gerekse özelde internet aracılığıyla ilenen suçlar küresel etki alanı dolayısıyla özellikle ekonomik anlamda ciddi zarar neticeleri doğurmaktadır. Hal böyle olunca bu suçluluk alanı sadece belli uluslar arası örgütlerin değil konuyla bir şekilde ilgilen tüm kurum ve kuruluşun dikkatin çekmiştir ve çekmeye devam etmektedir. Keza Uluslar Arası Ticaret Odası da 1988 yılında üyelerinin bu tür suçluluğa karşı korunması için " *Computer Related Crime and Criminal Law and International Business Wiew*" başlıklı bilgisayar suçları ve hukukuna ilişkin raporunda şu sonuçlara varmaktadır.¹⁴⁹

1- *Bilgisayarın yetki dışı kullanılmaları veya müdahalelere maruz kalmaları telematik sistemler bakımından önemli saldırı teşkil etmektedir.*

2- *Bu nevi sistem (bilişim ve bilişimi gerçekleştiren telekomünikasyon sistemleri) sahipleri veya kullanıcıları, ceza hukuku tarafından, büyük değer arz eden verilerin etkili korunmasına ihtiyaç duyulmaktadır.*

3- *Mevcut kanunlar bilişim konusuna uygun kaleme alınmadıklarından, ya bu konulara tatbik edilememekte ya da tatbik edilmeye çalışılsa bile hem içerik hem de ceza yönünden yetersiz kalmaktadır.*

¹⁴⁷ **DEĞİRMENCİ**, Bilişim Suçları Alanında Yapılan Çalışmalar.

¹⁴⁸ Bu komite Avrupa Konseyi tarafından kurulmuş ve yasal sorunlar üzerinde daha ayrıntılı tartışmalardan sonra 9 sayılı tavsiye kararını oluşturmuştur. Bu tavsiye kararı 13 Eylül 1989 tarihinde Avrupa Konseyi tarafından kabul edilmiştir. Tavsiye kararında bilişim suçlarıyla ilgili olarak yapılacak yasal düzenlemelerde tek düze bir ceza politikası için gerekli suçlar listesi ve ayrıca tercihe bağlı bir liste yer almıştır. Bunu takiben de 1995 yılında 13 numaralı "Bilişim Teknolojilerinin Kullanılması Sebebiyle Ortaya Çıkan Ceza Usul Hukuku Problemleri" konulu tavsiye kararlarını yayınlamıştır. Ayrıntılı bilgi için bkz. **KARAGÜLMEZ**, Ali, Bilişim Suçları ve Soruşturma – Kovuşturma Evreleri, Ankara, 2005, sh: 81 – 82.

¹⁴⁹ **YAZICIOĞLU**, Bilgisayar Marifetiyle, sh: 27.

4- Her geçen gün uluslar arası nitelik göstermek suretiyle büyüyen bilişim suçlarına karşı milli sınırlar içerisinde uygulamak amacıyla düzenlenmiş bir ceza usulü yargılaması yeterli olmamaktadır.

Uluslar Arası Ticaret Odasının yayınladığı bu rapor doğrultusunda, dönemin Avrupa Ekonomik Topluluğu, bünyesindeki devletlerin yasama organlarına hitaben, bir çok tavsiyede bulundu, buna göre,¹⁵⁰

1- Bütün tecavüzleri önleyebilmek için öncelikle ulusal ceza kanunları etkili hale getirilmeli.

2- Bilişim suçlarına ilişkin yargılama usulü ve hükümler ulusal düzeyde etkili olmalı.

3- Ulusal hükümetler ile uluslar arası organizasyonlar, sınır ötesi işlenen bilişim suçlarını takip edebilmek ve bunlarla ilgili mücadelede etkin olabilmek için birlikte hareket etmeli.

Bu dönemlerde Birleşmiş Milletler Küba'daki 8. toplantısında bilgisayar ve bilişim sistemleri aracılığıyla işlenen suçların hızlı artışı, bu suçların ortaya çıkarılmasındaki güçlükler, buna karşın işlenmelerindeki kolaylık, süratle ekonomik suçlara olan ilişkilerinin altı çizilerek üye devletlere aşağıdaki tespitleri tavsiye kararı olarak sunmuştur.¹⁵¹

a- Bilgisayar suçları ve bilgisayar destekli suçlarla yapılan savaşta mücadele arttırılarak bu husustaki ceza mevzuatı geliştirilmeli.

b- Bilişim konusundaki güvenlik tedbirlerine yönelik çalışmalar başlatılmalı.

c- Bilgisayar ve sistemleri aracılığıyla işlenen suçlar ve bunların önlenmesi konusundaki toplumun, hukuki mercilerin ve araştırmacıların dikkatini çekecek tedbirler alınmalı.

d- Hakim ve araştırmacılara bu konuda gerekli eğitim verilmeli.

e- Bilgisayar kullanımına ilişkin etiğin tespiti¹⁵² ile bu hususun bilgisayar eğitiminin bir parçası olarak verilmesi konusunda bu konularda çalışan kuruluşlarla işbirliği içine girilmeli.

¹⁵⁰ YAZICIOĞLU, Bilgisayar Marifetiyle, sh:27.

¹⁵¹ YAZICIOĞLU, Bilgisayar Marifetiyle, sh: 28-29.

¹⁵² "Türkiye'de de bu ahlak kuralları için bir çalışma Türkiye Bilişim Derneği tarafından yapılmış ve internet'in ahlak kuralları yazılı olarak yayımlanmıştır: Bu kurallar şu şekilde özetlenebilir:

f- Bilgisayar suçlarıyla mücadelede uluslar arası işbirliği artırılmalı

Bilişim suçlarına ilişkin en kapsamlı düzenleme Avrupa Konseyi bünyesinde gerçekleştirilen “Avrupa Siber Suç Sözleşmesi”dir. Bu sözleşmeyle birlikte internetin bilişim suçları bakımından önemli bir unsur olmaya başlamasının da normatif olarak ifade edildiği görülmektedir. Avrupa Konseyi Suç Sorunları Komitesi, 1997’de başladığı çalışmaları sonucunda Siber Suçlar Sözleşme Taslağı ile açıklayıcı raporu Avrupa Suç Sorunları Komitesi’ne Haziran 2001’de sunmuştur. Taslak, 8 Kasım 2001’de Avrupa Konseyi Bakanlar Komitesinde kabul edilerek, 23 Kasım 2001’de Budapeşte’de düzenlenen Siber Suçlar Uluslar Arası Konferansında imzaya sunulmuştur. Sözleşmeye 26 Avrupa Konseyi üyesi ülke ile beraber ABD, Japonya, Kanada ve Güney Afrika imza koymuşlardır. Siber Suç Sözleşmesi, sözleşmenin amacını, göz önünde bulundurulmuş çalışma ve ilkeleri açıklayan bir giriş bölümü ile beraber 4 bölüm ve 48 maddeden oluşmaktadır. “Ulusal Düzeyde Alınacak Önlemler” başlıklı II. Bölüm,; maddi ceza hukuku, usul hukuku ve yargı yetkisine ilişkin düzenlemeleri içermektedir¹⁵³.

-
- *Kişi açık kimliğini geçerli bir gerekçe olmadıkça gizlememeli,*
 - *Kişi kimliğini saklayabileceğini umarak gerçek yaşamda benimsemediği davranışları sergilememeli,*
 - *Düşünceler düz ve yalın, sadece ne demek istendiğini belirtecek bir şekilde iletilmeli,*
 - *Düşünceleri dile getirirken olumlu olunmalı ve nazik ifadeler kullanılmalı,*
 - *Elektronik bülten, tartışma listesi (mailing list) veya haber listesi (news) gibi ortamları kullanırken bu listelerin genel kurallarına uyulmalıdır.*
 - *Özellikle tartışma listelerinde kişiler kendi düşüncelerini kabul ettirmede ısrarcı olmamalı,*
 - *Tartışmaların kişiselleşmesine izin verilmemeli,*
 - *Gereksiz yere veya anlamını bilmeden büyük harfler kullanarak yazısmaktan, sıkça özel simgeler kullanmaktan, espirili veya alaycı anlatımdan kaçınılmalı,*
 - *Anlamsız sayılacak gereksiz iletiler gönderilmemeli,*
 - *Kişilerin istemleri dışında (spam) eposta olarak rahatsız olmalarına neden olunmamalı,*
 - *İleti trafiğini yoğunlaştıran gönderimde bulunanlar uyarılmalı, bu tavrı devam ettirmekte ısrarcı olanlara karşı yasal önlemlerin oluşturulmasına ve yaptırımlar uygulanmasına destek olunmalı,*
 - *İnsanları duygusal yönden rahatsız edici iletiler yayılmamalı,*
 - *İyelik haklarını zedelememeye özen gösterilmelidir. Başkasının veri kaynaklarını, düşüncelerini ve yazılımlarını kişinin kendisininmiş gibi sahiplenilmeye kalkışılmamalı,*
 - *Kişileri karalayıcı ve kişilik haklarına zarar verici hareketlerden kaçınılmalı,*
 - *İnternet ortamını kullanarak hırsızlık, başkalarının çalışmalarını engelleme gibi kötü kullanımlara yol açılmamalı ve göz yumulmamalıdır.” ÇELİK/ERASLAN’den naklen (Erişim Tarihi: 18.09.2007, Saat: 14:10).*

¹⁵³ DEĞİRMENCİ, Bilişim Suçları Alanında Yapılan Çalışmalar.

Bu genel çerçeve ile ortaya konulmaya çalışılan hassasiyetin normatif alana yansımalarının ne ölçüde gerçekleştiği konusunda bazı önemli uluslar arası belgeler ile Türk Ceza Hukuku bakımından tasarılarla birlikte 765 ve 5237 sayılı TCK düzenlemelerinin kısaca hatırlanması yerinde olacaktır.

1.7.1.- Uluslar arası Düzenlemeler

1.7.1.1.- Avrupa Konseyi Siber Suç Sözleşmesi

23. 11. 2001 tarihinde Macaristan'ın başkenti Budapeşte'de imzaya açılan Sözleşme ve Türkiye tarafından da imzalanmıştır. 48 maddeden oluşan Sözleşme, 1.07. 2004 tarihinde yürürlüğe girmiştir.

Sözleşmede, bir bilişim sistemi olarak bilgisayar sistemlerinin ceza hukukuna etkisi ve ortaya çıkardığı sorunlar, hem maddi ceza hukuku açısından hem de ceza yargılaması açısından ele alınmış ve bu alanlarda bilgisayar sistemlerinin kullanılması merkezinde ortaya çıkan sorunlara ilişkin çözümler getirilmek istenmiştir¹⁵⁴. Bu sözleşmeye A.B.D., Kanada, Japonya ve Güney Afrika'nın da dahil olmalarıyla ve sözleşmenin mahiyetini önemseyerek sözleşmeyle oluşturulmaya çalışılan ortak hareket etme inisiyatifine katılmalarıyla sözleşme sadece Avrupa Birliğini ilgilendiren ve kapsayan bir sözleşme olmaktan çıkmış, küresel bir nitelik kazanmıştır¹⁵⁵. Ancak *Von Bubnoff*, Sözleşmenin önceleri Avrupa Birliği ülkeleri esas alınarak hazırlanmasına rağmen daha sonra farklı kültürel ve politik düşünce eksenlerinde hareket eden ülkelerin bu Sözleşmeye katılımını, uygulama problemlerinin yaşanması ve ancak "en küçük ortak payda" da buluşulabilmesi bakımından sorunlu görmektedir¹⁵⁶. Bu tespiti şöyle bir örnekle geliştirmektedir. A.B.D.'de düşünce özgürlüğünün koruma alanı oldukça geniştir. Özellikle Sözleşmenin imzalandığı dönemden sonra ırkçı ve yabancı düşmanlığı içeriklerinin internette yayımlanması hususunda, A.B.D. ile Avrupa Birliği arasında bu konuda kapsam belirleme farklılıkları yaşanmıştır. Keza bu farklılıkları ortadan

¹⁵⁴ Avrupa Konseyi Siber Suç Sözleşmesi'nin tarihsel oluşum süreci konusunda daha ayrıntılı bilgi için bkz. **SCHWARZENEGGER**, Christian, Die internationale Harmonisierung des Computer- und Internetstrafrechts durch die Convention on Cybercrime von 23 November 2001, in: Strafrecht, Strafprozessrecht und Menschenrechte – Festschrift für Stefan **TRECHSEL** zum 65. Geburtstag (Hrsg.: Andreas **DONATCH**, / Marc **FORSTER** / Christian **SCHWARZENEGGER**), Zürich, 2002, sh: 308 v.d.

¹⁵⁵ **HILGENDORF**, Tendenzen, sh: 268.

¹⁵⁶ **HILGENDORF**, Tendenzen, sh: 268.

kaldırmak amacıyla 28 Şubat 2003 tarihinde ırkçı ve yabancı düşmanlığı etkinliklerinin engellenmesi adına Siber Suç Sözleşmesine (SSS) ek bir protokol kabul edilmiştir¹⁵⁷.

Sözleşmenin ikinci kısmını oluşturan ulusal düzeyde alınacak tedbirler maddi ceza hukuku ve usul hukuku olmak üzere iki bölüme ayrılmış ve birinci bölümde taraf devletlerin ceza kanunlarında siber uzayda gerçekleştirilecek belirli davranışların suç haline getirilmesi beklenmektedir. İkinci bölümde ise, ceza yargılamasına yönelik düzenlemelerle delillerin elde edilmesi, korunması ve saklanmasına ilişkin olarak ortaya çıkan sorunlara çözüm getirilmek istenmiştir¹⁵⁸.

Anılan iki bölümün ardından, birinci bölümde ayrıntılarıyla ortaya konulmuş tartışmaların ve kaygıların Avrupa Konseyi'nce de paylaşıldığı görülmekte ve bilişim suçlarının, bilişim ağları ile işlenmesinin yaygın bir hal alması ve internetin hızla yaygınlaşması, bu suçlara ilişkin sorunların ulusal bir sorun olmaktan çok uluslar arası bir sorun haline gelmesi gerçeğinden hareketle üçüncü bir kısma yer verilmiştir. Bu kısmın konusu ise, Sözleşmeye taraf devletlerin birbirleri arasında adli yardımlaşmaları ve suçluların iadesidir¹⁵⁹.

Bu yapı üzerinden sözleşmenin amaçları *İçel*'in yaptığı belirlemeyle şöyle ortaya konulmuştur ,

1. *Siber suçlarla ilgili ceza sorumluluğunun sınırlarının çizilmesinde başta düşünce özgürlüğü olmak üzere tüm temel hak ve özgürlüklerin gereklerine uyulması;*
2. *Bilgisayarlarla işlenen veya bilgisayarla ilişkili suçların belirlenip düzenlenmesinde*

¹⁵⁷ Değerlendirme farklılıklarının ayrıntıları için bkz. **VON BUBNOFF**, Eckhart, Krimineller Missbrauch der neuen Medien im Spiegel europäischer Gegensteuerung, in: Strafrecht und Kriminalität in Europa (Der:Frank ZIESCHANG/ Eric HILGENDORF / Klaus LAUBENTHAL), IUS EUROPÆUM, B: 23, Baden – Baden, 2003, sh: 93 v.d.

¹⁵⁸ Siber Suç Sözleşmesinin ceza yargılamasına ve özellikle delillerin elde edilmesi, korunması ve saklanmasına ilişkin hükümler hakkında bkz., **KESKİN**, Serap Avrupa Konseyi Siber Suç Sözleşmesinde Ceza Muhakemesine İlişkin Hükümlerin Değerlendirilmesi, in: İHFM, C. LIX, S. 1-2, İstanbul, 2001, sh. 162. vd.

¹⁵⁹ **HELVACIOĞLU**, Aslı Deniz, Avrupa Konseyi Temel Siber Suç Sözleşmesi Temel Hükümlerinin İncelenmesi, in: İnternet ve Hukuk (Der: Yeşim ATAMER), İstanbul, 2004sh: 294 v.d.

ortak minimum standarda uyulması; 3. Eylemin hukuka aykırı olması gerektiğinin kabulü; 4. Eylemin kasten işlenmesinin kabulü ¹⁶⁰.

Sözleşmede yer ver verilen suçlarda ortak amaç, bu tür suçlara ilişkin olarak taraf devletlerin ceza mevzuatlarında uyum sağlamadır. Sözleşmede yer alan suçlar, daha önceki dönemlerde çeşitli ülkelerin ceza mevzuatları içerisinde düzenlenmiş olan suçların uluslar arası düzeyde ele alınması şeklinde olmuştur. Aşağıda bu suçlara genel olarak değinilecektir.

Sözleşmenin ikinci kısım birinci başlık altında yer alan “ *Bilgisayar Veri ve Sistemlerinin Gizliliğine, bütünlüğüne ve Erişilebilirliğine karşı suçlar*” kapsamında yetkisiz erişim (2. madde) yetkisiz müdahale (3. madde), verilere müdahale (4. madde), sisteme müdahale (5. madde) ve aygıtların kötüye kullanılması (madde 6) suçlarına yer verilmiştir.

Sözleşmenin 2. maddesine göre “*Yasadışı erişim*”, kasten ve hukuka aykırı bir şekilde bir bilgisayar sisteminin tamamına veya bir kısmına girilmesidir. Aynı maddede, yetkisiz erişim suçunun taraf devletlerin ceza mevzuatlarında düzenlenirken, güvenlik önlemlerinin ihlal edilmesi suretiyle işlenebileceğine, verinin elde edilmesi ya da diğer gayri meşru bir niyetle sisteme girilmesi ya da bilgisayar ağları vasıtasıyla birbirine bağlı bilgisayar sistemleri aracılığıyla işlenebileceğine ilişkin ek unsurları getirebilecekleri belirtilmiştir.

“*Yasadışı müdahale*” ise Sözleşmenin 3. maddesinde düzenlenmiş olup buna göre, bilgisayar sisteminden elektromanyetik dalgalar yayılması da dahil olmak üzere, kamuya açık olmayan bilgisayar verilerinin iletimi sırasında, bunlara teknik yöntemler kullanılmak suretiyle müdahale edilmesinin suç haline getirilmesi öngörülmüştür. Dolayısıyla bu madde bağlamında “kamuya açık olmayan bilgisayar verisi yayını” kapsam dahilindeki suçlar için belirleyici özellik taşımaktadır. Ayrıca bu maddeye göre taraf devletler anılan suçu sahtekarlık amacı güden bir fiil şeklinde veya başka bir bilgisayar sistemine bağlı bir bilgisayar sistemini esas alarak da tanımlayabilmektedirler¹⁶¹.

Sözleşmenin 4. maddesinde veriye müdahale, 5. maddesinde sisteme müdahale düzenlenmiştir. Sözleşmenin 4. maddesinde göre, veriye zarar verilmesi, verinin bozulması, değiştirilmesi veya ortadan kaldırılmasının suç olarak düzenlenmesi gerekmektedir. Madde incelendiğinde, verinin bilgisayar içinde bulunması ya da herhangi bir saklama aygıtı içerisinde olması arasında fark yaratılmadığı görülmektedir. Aynı maddenin ikinci fıkrasında,

¹⁶⁰ İÇEL, Kayıhan Avrupa Konseyi Siber Suç Sözleşmesi Bağlamında “Avrupa Siber Suç Politikasının Ana İlkeleri, in: İHFM, C. LIX, S. 1-2, İstanbul, 2001, sh. 3 vd.

¹⁶¹ HELVACIOĞLU, Avrupa Siber Suç Sözleşmesi, sh: 283.

taraf devletlerin söz konusu suçun gerçekleşmesi için ciddi zararın varlığı şartına yer verebilecekleri ifade edilmiştir.

Beşinci maddede ise sisteme müdahale düzenlenmiştir. Sözleşmenin 5. maddesinde sistemin işleyişinin ciddi olarak engellenmesinin suç haline getirilmesi gerektiği belirtilmiştir. Sistemin işleyişinin engellenmesine ilişkin müdahaleler ise sisteme veri yoluyla müdahale edilmesi ya da sistem içerisindeki verilere müdahale edilmesi esas alınarak düzenlenmiştir¹⁶². Bu açıdan fiziki müdahaleler sözleşmede sistemin işleyişine müdahale kapsamında değerlendirilmemiştir.

Sözleşmenin 6. maddesinde ise birtakım hazırlık hareketlerinin suç olarak düzenlenmesi yoluna gidildiği görülmektedir. Nitekim 6. maddenin 1. fıkrasına göre Sözleşmenin 2-5. maddelerinde düzenlenen suçların işlenmesi için öncelikli amacının söz konusu suçların işlenmesine yönelik tasarlanmış ya da uyarlanmış olan program da dahil cihazların (m. 1/a.i); söz konusu suçların işlenmesi amacıyla, bir bilgisayarın tamamına ya da bir kısmına erişimi sağlayabilecek bir bilgisayar şifresinin, erişim kodunun ya da benzer verinin (m. 1/a.ii), üretiminin, satışının, kullanılmak için tedarikinin, ithal edilmesinin, dağıtılmasının ya da diğer şekilde erişilebilir kılınmasının taraf devletlerce suç olarak düzenlenmesi hükmüne yer verilmiştir¹⁶³.

Aynı maddenin “b” bendinde, Sözleşmenin 2 ila 5. maddeleri arasında düzenlenen suçların işlenmesi amacıyla, “a” bendinde sayılan hususların elde bulundurulmasının suç olarak düzenlenmesi gerektiği ifade edilmiştir. Elde bulundurmanın suç sayılabilmesi için taraf devletlerin yukarıda sayılanların belirli bir sayıda olmasına ilişkin ek şart getirebilecekleri hükmüne yer verilmiştir.

Maddenin 2. fıkrasına göre yukarıda sayılan hükümler, bu tür aygıt ya da programların, bir bilgisayarın korunması ya da test amacı gibi Sözleşmenin 2 ila 5. maddelerinde belirtilen suçların işlenmesi amacını gütmeyen meşru amaçlar için üretimi, satışı, kullanılmak için tedariki, ithal edilmesi, dağıtılması ya da diğer şekilde erişilebilir kılınmasını cezalandıracak şekilde yorumlanamaz¹⁶⁴.

¹⁶² TAŞKIN, Şaban Cankat, Bilişim Suçları, Bursa, 2008, sh: 40.

¹⁶³ KETİZMEN, Bilişim Suçları, sh: 58.

Aynı maddenin son fıkrasında ise, bilgisayar şifreleri, erişim kodlarının ya da benzer verilerin satışının, dağıtımının ya da diğer şekillerde erişilebilir kılınmasının cezalandırılabilmesine ilişkin hükümler saklı tutulmak kaydıyla, taraf devletlerin ceza mevzuatları içerisinde birinci fıkrada düzenlenen hususları kapsam dışı bırakabileceği belirtilmiştir.

Sözleşmenin 7. ve 8. maddelerinde, bilgisayar aracılığıyla sahtekarlık ve bilgisayar aracılığıyla dolandırıcılık fiilleri düzenlenmiştir. Yedinci maddeye göre bilgisayar aracılığıyla sahtekarlık, *“verilerin açıkça okunabilir ya da anlaşılabilir olup olmadığına bakılmaksızın Bilgisayar verilerinin hukuki açıdan orijinal verilermiş gibi değerlendirilmesi ya da hareket edilmesi amacıyla verilerin orijinalliğinin bozulması sonucunu doğuran, bilgisayar verilerine yeni veriler ilave etme ve bilgisayar verilerini değiştirme, silme veya erişilemez kılma ve böylece orijinal verilerden farklı veriler meydana getirme, fiillerin hukuka aykırı olarak kasten işlenmesi”* şeklinde tanımlanmıştır. Devamında md. 8’de düzenlenen bilgisayar aracılığıyla dolandırıcılık, sistemin işleyişine ekonomik bir yarar sağlanması amacıyla müdahale edilmesi ve yarar sağlanması şeklinde tanımlanmış ve maddede sisteme yeni veri yerleştirilmesi, verinin değiştirilmesi, silinmesi veya erişilmez kılınması, bunların yanında sistemin işleyişine diğer herhangi bir müdahale seçimlik hareketler olarak düzenlenmiştir.

Sözleşmenin 9.maddesinde ise içerikle ilgili suçlar başlığı altında çocuk pornografisinin yasaklanmasına ilişkin hükümler getirilmiştir. Bu kapsamda yasaklanan fiiller, bilgisayar sistemleri aracılığıyla dağıtmak amacıyla çocuk pornografisinin üretilmesi (m. 9/1.a), sunulması veya temin edilebilir hale getirilmesi (m. 9/1.b) ; dağıtılması ya da iletilmesi (m. 9/1.c); kendisi ya da başkası için bilgisayar sistemi aracılığıyla elde edilmesi (m.9/1.d); son olarak, bilgisayar sistemi içerisinde ya da bilgisayar veri depolama ortamında çocuk pornografisi bulundurulmasıdır (m. 9/1.e). Maddede çocuk pornografisi, bir küçüğün cinsel içerikli bir eylemde kullanılması, küçük gibi görünen bir kişinin cinsel içerikli bir eylemde kullanılması ya da bir küçüğün cinsel içerikli bir eylemde yer aldığını temsil eden gerçekçi

¹⁶⁴ Avrupa Konseyi Siber Suç Sözleşmesi'nin üzerinde en çok durulan hükümlerinin başında çocuk pornografisiyle mücadeleyi içeren 9. madde gelmektedir. Özellikle internet teknolojisindeki gelişim çocuk pornografisi içerikli yayınlara olan talebi arttırmış, bununla birlikte bu yayınların dağılımı, yayılımı konusunda birçok alternatif ortaya çıkmıştır. İnternette çocuk pornografisi ile mücadele ve bu konuda Avrupa Konseyi Siber Suç Sözleşmesi md. 9'un değerlendirilmesi ile ilgili bkz. **KÖNIG**, Sabine, Kinderpornographie im Internet, sh: 239 v.d., Kaynak: http://deposit.ddb.de/cgi-bin/dokserv?idn=971602565&dok_var=d1&dok_ext=pdf&filename=971602565.pdf (Erişim Tarihi: 13.04.2009, Saat: 09:09)

imaj olarak tanımlanmıştır. Maddeye göre, küçük 18 yaşından küçükleri ifade etmekte, taraf devletlerin 16 yaşına kadar indirilebilmelerine imkan tanınmaktadır.

10. maddede ise, telif hakları ve bağlantılı hakların korunmasına ilişkin uluslar arası düzenlemelerde yer alan hükümlerin etkin bir şekilde uygulanabilmesi ve de ihlallerin cezalandırılabilmesine ilişkin cezai hükümlerin getirilmesi düzenlenmiştir¹⁶⁵.

1.7.1.2.- Irkçı ve Yabancı Düşmanlığı Eylemlerine İlişkin Siber Suç Sözleşmesi Ek Protokolü

“Bir Bilişim Sistemi Aracılığıyla İşlenen Irkçı ve Yabancı Düşmanlığı İçerikli Eylemlerin Suç Kapsamına Alınmasına Yönelik Siber Suç Sözleşmesinin Ek Protokolü”¹⁶⁶ Strassburg’da 28 Şubat 2003 tarihinde kabul edilmiştir. Bu süre zarfında İsviçre’nin de 9 Ekim 2003 tarihinde taraf olduğu bu sözleşmeye 23 ülke imza atmıştır.

Ek Protokol’ün 2. maddesinde “ırkçı ve yabancı düşmanlığı içerikli materyal” kavramını tanımlamış ve bir kişiye veya gruba karşı kin, ayrımcılık veya şiddeti destekleyen, teşvik eden, bunu alenen ilan eden düşünce veya teoriye ait her türlü yazı, resim ve diğer tüm temsil araç ve imkanların bu tanım altında anlaşılması gerektiğini ortaya koymuştur. Bu tanıma bağlı olarak yukarıda belirtilen durumların ırk, ten rengi, soy, ulusal veya coğrafi kökenden kaynaklanmış olması da gerekmektedir. “Soy (*Abstammung*)” kavramından, Ek Protokol’ün Açıklayıcı Raporu’na göre; zarar gören tüm kişi veya gruplarda var olmasa bile, belirli bir grubun üyelerine özgülenen karakteristik özellikler anlaşılmaktadır (Örneğin ırk veya ten rengi gibi)¹⁶⁷.

Ek Protokol’ün 3/1 maddesine göre taraf devletlere, ırkçı ve yabancı düşmanlığı içerikli materyallerin bilişim sistemleri aracılığıyla kasten aleni bir şekilde yayılmasının cezalandırılması ile yükümlülük atfedilmiştir. Bu bağlamda “ulaşılabilir kılma” kavramı materyalin kullanım amacıyla internete yüklenilmesi anlamına gelirken, “yayma” bu

¹⁶⁵ Ayrıntılı değerlendirmeler için bkz. **BAŞPINAR**, Veysel/ **KOCABEY**, Doğan, İnternette Fikri Hakların Korunması, Ankara, 2007, sh: 178- 179.

¹⁶⁶ Bilgisayar Sistemleri Aracılığıyla İşlenen Irkçılık ve Yabancı Düşmanlığı Eylemlerinin Suç Kapsamına Alınmasına İlişkin Siber Suç Sözleşmesi Ek Protokolü, Avrupa Anlaşmalar Serisi No: 189, <http://convention.coe.int/Traty/Commun/QueVoulezVous.asp?NT=189&CM=1&DF=29/09/04&CL=ENG>.

¹⁶⁷ **NIGGLI**, Marcel Alexander, Irk Ayrımcılığı ve İnternet (Çev:İlker TEPE), in: CHD, Yıl: 2 Sayı:1, 2007, sh: 247 v.d.

bağlamda doğrudan aktif bir dağıtımı kapsamaktadır. Hiper linklerin kurulum veya birleştirilmesi de “ulaşılabilir kılma” kapsamında değerlendirilmelidir. “Ulaşılabilir kılma”, bilgisayar sistemleri aracılığıyla yapılan özel iletişimler hariç olmak üzere bilgilerin kamu tarafından rahatlıkla erişilebilir hale getirilmesini ifade etmektedir.¹⁶⁸

Suç unsuru taşıyan bilgilerin sohbet odalarında değişimi ve haber gruplarına veya tartışma formlarına yüklenmesi, kamusal ulaşılabilirlik olarak anlaşılmaktadır. Her ne kadar bu bilgilere erişim için bir şifre kullanmak gerekli olsa da, bu şifrenin herkese veya belli özellikleri haiz olan kimselere istedikleri zaman verilmesi durumunda söz konusu bilgi kamusal olarak kabul edilir. Ancak bu bağlamda zarar gören kişiler arasındaki ilişkinin tarzı da önemsenmelidir. Ek Protokol’ün 4. maddesine göre taraf devletler bir bilişim sistemi aracılığıyla kişi veya kişi gruplarına ırkları, ten renkleri, soyları, ulusal ve etnik kökenleri nedeniyle tehditlere maruz kalmaları durumunda, bu eylemlerin tehdit suçunun ağırlaştırılmış hali olarak cezalandırılması yükümlülüğünü atfetmiştir.

5. madde ise taraf devletlerden , bir bilişim sistemi kullanılarak bir kişi veya kişi grubuna karşı, Ek Protokol md. 2’de tanımlanan bir gruba aidiyetleri dolayısıyla kasten ve hukuka aykırı olarak alenen gerçekleştirilen hakaret /aşağılama eylemlerinin cezalandırılmasını talep etmektedir. Bu düzenleme açısından da dinin sadece diğer belirtilen faktörlerden birinin gerçekleştirilmesi için bir vesile/bahane olarak kullanılması durumunda maddenin koruma alanı kapsamına alınacağı açıkça belirtilmiştir. Bu çerçevede “hakaret” kavramından bir kişinin onur ve şerefini ilgilendiren hor görücü, aşağılayıcı ifadeler anlaşılmaktadır.¹⁶⁹

Ek Protokol 6/1 maddesinde taraf devletlerden, bilgilerin bir soykırımı veya insanlığa karşı suçların inkarını, basitleştirilmesini, onaylanmasını veya hukuka uygun kabul edilmesini içermesi durumunda söz konusu içeriklerin bir bilişim sistemi aracılığıyla kasten ve hukuka aykırı olarak alenen yayılmasının veya bunların kamu açısından ulaşılabilir kılınmasının cezalandırılması istenmektedir.¹⁷⁰

¹⁶⁸ NIGGLI, Irk Ayrımcılığı, sh: 255.

¹⁶⁹ NIGGLI, Irk Ayrımcılığı, sh: 260.

¹⁷⁰ NIGGLI, Irk Ayrımcılığı, sh: 261.

Son olarak Ek Protokol 7. maddesinde taraf devletlere suç işleme kastıyla yukarıda belirtilen suçlara yardımın cezalandırılması yükümlülüğünü atfetmiştir. Açıklayıcı Rapor net bir biçimde – sözleşmeden farklı olarak – teşebbüsün bu kapsamda değerlendirilmediğini belirlemiştir. Ek Protokol 7. maddesi, Açıklayıcı Rapor’da da belirtildiği üzere, kastın yanında suç işleme bilincini de aradığı için, servis sunucularının kendi ağları veya bilişim sistemleri üzerinden transfer edilen veya buralara kaydedilen içeriklerin aktif bir biçimde izlenmeleri bu kapsamda olmadığı gibi bu yönde bir yükümlülükleri de söz konusu değildir.¹⁷¹

1.7.1.3.- Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşme

İnternet de dahil olmak üzere tüm bilişim sistemlerini kapsayacak şekilde kişisel verilerin korunması açısından ilk önemli belge olan Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşme 28.01.1981 tarihinde Straburg’da kabul edilmiştir¹⁷². Anılan sözleşme otomatik bilgi işleme konu teşkil eden kişisel nitelikteki verilerin sınırlar ötesi akışının yoğunluk kazanması karşısında bilhassa özel yaşama saygı hakkını korumak ve ona saygı göstermek adına haber alma özgürlüğünün sınırlarını da göz önünde bulundurarak özel yaşama saygının ve halklar arasındaki serbest bilgi akımının temel değerler olduğu temelinden hareket etmektedir.

Avrupa Konseyinin 108 nolu Verilerin Korunması Sözleşmesi, gerek kamusal gerekse özel sektörde geçerli olmak üzere verilerin korunması alanında kabul edilmiş olan uluslar arası hukukun ilk bağlayıcı sözleşmesidir. Bu sözleşme esas olarak üye devletler içerisinde verilerin korunması için temel ilkeleri ortaya koymaktadır. Sözleşme her sözleşmeci devlette uyruğu ve ikametgahı ne olursa olsun tüm gerçek kişilerin temel hak ve özgürlüklerini ve özellikle kendilerini ilgilendiren kişisel nitelikli verilerin otomatik işleme tabi tutulması karşısında özel yaşamın güvence altına alınmasını yani kişisel verilerin korunmasını amaçlamaktadır. Sözleşme sadece kişisel verilerin işlenmesi sırasında gerçek kişilerin korunması ile sınırlıdır. Bunak karşılık yasa koyucular tarafından sözleşmenin kapsamına tüzel kişilerin ve kişi toplulukların dahil edilmesine engel bulunmamaktadır. Sözleşmede

¹⁷¹ NIGGLI, Irk Ayrımcılığı, sh: 261.

¹⁷² Sözleşmenin tam metni için bkz. http://www.avrupakonseyi.org.tr/tur/...ma/aas_108.htm (Erişim Tarihi: 15.01.2008, Saat: 23:33)

kişisel nitelikli verilerin tanımına da yer verilmiştir. Sözleşmeye göre kişisel nitelikli veriler kimliği belirtilen veya belirtilebilen gerçek kişiyle ilgili tüm bilgileri ifade etmektedir. Sözleşmede otomatik işlem kavramı da tanımlanmıştır. Buna göre otomatik işlem, tamamı veya bir kısmı otomatik yöntemlerle gerçekleştirilen verilerin kaydı bu verilere mantıksal ve/veya aritmetik işlemlerinin uygulanışı, verilerin değiştirilmesi, silinmesi, çıkarılması veya dağıtılması anlaşılır¹⁷³.

Sözleşmenin 1. maddesinde bu temel yaklaşıma paralel olarak sözleşmenin amacı uyruğu veya ikametgahı ne olursa olsun tüm gerçek kişilerin, temel hak ve özgürlüklerini ve özellikle kendilerini ilgilendiren kişisel nitelikteki verilerin, otomatik bilgi işleme tabi tutulması karşısında özel yaşam haklarını güvence altına almak olarak vurgulanmaktadır. Sözleşmenin 2. maddesinde ise kişisel veri de dahil olmak üzere sözleşmenin önemli kavramları tanımlanmıştır.

Sözleşmenin 5. maddesinde otomatik bilgi işleme konu teşkil eden verilerin niteliği hakkında bir takım esaslar kabul etmektedir. Buna göre otomatik bilgi işleme konu teşkil eden kişisel nitelikteki veriler:

- (a) Meşru ve yasal yoldan elde edilmeli ve işleme tâbi tutulmalıdır;
- (b) Belli ve meşru amaçlar için kaydedilmeli ve bu amaca aykırı şekilde kullanılmamalıdır;
- (c) Uygun ve elverişli olmalı ve kaydedildikleri amaca göre aşırı olmamalıdır;
- (d) Doğru ve icabında güncel olmalıdır;
- (e) İlgili kişilerin kimliklerini belirtecek bir biçim altında ve kaydedildikleri nihai amaç için gerekli görülen süreyi aşmayacak bir süre için muhafaza edilmelidir.

Otomatik bilgi işleme tabi tutulacak olan verilerin niteliği üzerinde durulduktan sonra hemen 6. maddede hangi verilerin otomatik işleme tabi tutulamayacağı açık bir biçimde dile getirilmektedir. İç hukukta uygun güvenceler sağlanmadıkça, ırk menşeyini, politik

¹⁷³ ŞİMŞEK, Oğuz, Anayasa Hukukunda Kişisel Verilerin Korunması, İstanbul, 2008, sh: 22.

düşünceleri, dini veya diğer inançları ortaya koyan kişisel nitelikteki verilerle sağlık veya cinsel yaşamla ilgili kişisel nitelikteki veriler ve ceza mahkumiyetleri, otomatik bilgi işlemine tâbi tutulamazlar.

Sözleşmede ilgili kişiler lehine de bir takım ek güvenceler öngörülmüştür. 12. madde hükmüne göre herkes:

(a) Kişisel nitelikteki verilerin otomatik işleme tâbi tutulduğu fişiyelerin¹⁷⁴ mevcudiyetini, temel amaçlarını, fişiyeye yöneticisinin kimliğini ve mutad ikâmetgâhı ile esas müessesesini öğrenmek;

(b) Makul aralıklarla ve süreye bağlı olmaksızın veya aşırı masrafa girmeden kendisi ile ilgili kişisel nitelikteki verilerin otomatik fişiyede bulunup bulunmadığının teyidini yaptırmak ve bu bilgilerin anlaşılır bir biçim altında bildirilmesini sağlamak;

(c) Gerekli olan durumlarda, bu verileri düzelttirmek veya bunların, bu Sözleşmenin 5 ve 6 ncı maddelerinde belirtilen temel ilkelere işlerlik sağlayan iç hukuk hükümlerinin ihlali suretiyle işleme tâbi tutulması hallerinde, söz konusu verileri sildirtmek.

(d) Teyit talebinin veya gerekli durumlarda bu maddenin b ve c fıkralarında öngörülen, bildirim, düzeltme veya silme talebinin yerine getirilmemesi halinde Kanun yoluna başvurma hakkından yararlanmak; hakkına sahiptir.

1.7.1.4.- A.B. Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Konusunda Bireylerin Korunmasına Dair Yönerge

Avrupa Parlamentosu ve Avrupa Birliği Konseyi tarafından 24 Ekim 1995 tarihinde kabul edilen yönerge ile kişisel verilerin özellikle gelişen bilişim – iletişim teknolojisi karında daha etkili bir şekilde korunabilmesi için Avrupa Birliği inisiyatif ortaya konulmuştur. Bu yönergeyi devamında 15Aralık 1997 tarihinde Telekomünikasyon Sektöründe Kişisel Verilerin İşlenmesine ve Gizliliğin Korunmasına Dair Yönerge, 18 Aralık 2000 tarihli Kişisel Verilerin Topluluk Kurumları ve Organlarınca İşlenmesi ve Bu Verilerin Serbest Dolaşımı

¹⁷⁴ Sözleşmenin 2. maddesinde yapılan tanıma göre otomatik fişiyeye, otomatik işleme konu teşkil eden bilgilerin tümüdür.

Konusunda Bireylerin Korunmasına Dair Düzenleme ile 12 Eylül 2002 tarihli Elektronik Komünikasyon Sektöründe Kişisel Verilerin İşlenmesine ve Gizliliğin Korunmasına Dair Yönerge kabul edilmiştir. Anılan bu düzenlemelerin çıkış noktası olarak inceleme konusu yönerge gösterilebilir¹⁷⁵.

24 Ekim 1995 tarih ve 95/46/EC sayılı yönerge çerçevesinde kişisel veriler ancak açıkça ve hukuka uygun bir amaç doğrultusunda toplanabilir ve işlenebilir olmalıdırlar. Toplama ve işleme işlemlerinin hukuka uygunluğu amacın kesin bir şekilde ortaya konulmasıyla birlikte değerlendirilmelidir. Kişisel verilerin hukuka uygun olarak toplanmış olması toplanıp kayıt altına alınan kişisel verilerin daima muhafaza edilmesi anlamına gelmemektedir. Bu veriler ancak toplama ve işleme amacına bağlı olarak makul bir süre için muhafaza edilebilirler. Buna paralel olarak ilgili yönerge, kişisel verilerin toplanmasını ve işlenmesini ancak bu verilerin toplanma ve işleme amacıyla aralarında bir nedensellik bağı olduğu ölçüde kabul edilebilir olduğunu kabul etmektedir.

Kişisel verilerin işlenmesinde hukuka uygunluğun ilk adımı, kaynak kişinin söz konusu kişisel verinin toplanıp işlenmesine göstereceği rızadır. Bunun dışında müşterek veya iç hukukun kaynak kişinin rızası alınmaksızın bir kişisel verinin toplanması ve işlenmesi ile ilgili düzenlemeleri de bu çerçevede hukuka uygunluğun bir çerçevesini çizmektedir. Ancak bu hallerde kişisel verisi toplanıp işlenen kaynak kişi menfaatleri ile söz konusu düzenlemelerde yazılı menfaatler arasında dengenin sağlanabilmesi için ölçülülük ilkesine riayet edilmesi de ek olarak aranmıştır¹⁷⁶.

Son olarak da yönergenin hassas kabul ettiği ve işlenmesinin yasaklandığı kişisel veriler hakkında bir açıklama yapmak yerinde olacaktır. 95/46/EC sayılı yönerge, düşünce özgürlüğünün bir gereği ve unsuru olan veriler ile geniş anlamda sağlık bilgilerini içeren verileri hassas veri kategorisinde değerlendirmiş ve bu verilerin toplanmasını ve işlenmesini yasaklamıştır. Bu kategori içindeki hassas veriler açılacak olursa kişinin siyasi, felsefi, dini kanaatleri veya geniş anlamda kabul edildiği için kişinin sağlık durumuna ilişkin aktüel veya potansiyel iyileşme, hastalık veya risklere ilişkin bilgiler yer almaktadır¹⁷⁷. Ancak bu işlem yasağı mutlak bir yasak hükmünde olmayıp, kaynak kişinin hayati menfaatleri, yine kaynak

¹⁷⁵ ER, Biyometrik Yöntemler, sh: 86.

¹⁷⁶ ER, Biyometrik Yöntemler, sh: 87.

¹⁷⁷ ER, Biyometrik Yöntemler, sh: 88.

kişinin açık rızası ile toplanması ve işlenmesinde ölçülülük ilkesine uygun olmak koşulu ile kamu yararı güdülen hallerde üye devletlerce belirlenen istisnalar Avrupa Komisyonu'na bildirmek şartıyla bu işlem yasağından muaf tutulabilirler.

1.7.1.5.- B.M. Çocuk Haklarına Dair Sözleşmeye Ek Çocuk Satışı, Çocuk Fahişeliği Çocuk Pornografisi İle İlgili İhtiyari Protokol

Çocuk Haklarına Dair Sözleşmeye Ek Çocuk Satışı, Çocuk Fahişeliği ve Çocuk Pornografisi İle İlgili İhtiyari Protokol, kaynak sözleşme olan Çocuk Haklarına Dair Sözleşme'nin, çocukları cinsel veya ekonomik istismardan ve çocuklar açısından tehlike doğurabilecek, onların sağlığına, fiziksel, zihinsel, ruhsal, ahlaki ya da sosyal gelişimine zarar verebilecek herhangi bir işte çalışmaktan koruduğundan hareketle çocuk satışı, çocuk fahişeliği ve çocuk pornografisi amacıyla yapılan kayda değer ve giderek artan uluslararası çocuk istismarının önüne geçebilmek için hazırlanmıştır¹⁷⁸. Söz konusu Protokol'de özellikle internet teknolojisinin gelişmesiyle birlikte çocuk pazarlıklarının daha sık ve uluslar arası düzlemde daha kolay gerçekleşmesi, bunun yanında çocuk pornografisinin internette ve diğer gelişen teknolojiler üzerinde artan erişebilirliğinden doğan tehlikeler karşısında çocuk pornografisinin üretiminin, dağıtımının, ihracatının, naklinin, ithalatının, kasıtlı zilyetliğinin ve reklamının tüm dünyada suç olarak kabul edilmesi için hükümetler ile internet endüstrisi arasında daha yakın işbirliği ve ortaklığın önemini vurgulanmaktadır. Böyle bir işbirliğinin küresel ölçekte vereceği pozitif etki ile çocuk satışına, çocuk fahişeliğine ve çocuk pornografisine olan tüketici talebini azaltmak ve kamuoyundaki bilinci arttırmak amaçlanmaktadır. Bu amaçlar çerçevesinde anılan Protokol'ün temel yapısını oluşturan kapsamlar yine Protokol'ün 2. maddesinde şöyle tanımlanmıştır.

a) Çocuk satışı, herhangi bir şahıs veya bir grup şahıs tarafından, ücret ya da başka herhangi bir şey karşılığında bir çocuğun başka birine devredildiği herhangi bir fiil veya işlem anlamına gelmektedir.

b) Çocuk fahişeliği, bir çocuğun ücret veya başka herhangi bir şey karşılığında cinsel faaliyetlerde kullanılması demektir.

¹⁷⁸ Özellikle çocuk pornografisine yönelik Avrupa Birliği bakış açısıyla ilgili bkz. **STILO**, Leo, Çocuk Pornografisine Karşı Avrupa Birliği Müdahalesi: 22 Aralık 2003 Tarihli 2004/ 68 GAI Konseyin Çerçeve Kararı Hakkında Bir Yorum (Çev: Vesile Sonay EVİK), in: KGCHS/ 4 "Çocuklar ve Suç- Ceza" (Der: Yener ÜNVER), Ankara, 2005, sh: 469.

c) Çocuk pornografisi, çocuğun gerçekte veya taklit suretiyle bariz cinsel faaliyetlerde bulunur şekilde herhangi bir yolla teşhir edilmesi veya çocuğun cinsel uzuvlarının, ağırlıklı olarak cinsel amaç güden bir şekilde gösterilmesi anlamına gelir.

Protokolün 3. maddesi taraf devletlere bir çocuğun cinsel veya ekonomik açıdan her türlü istismarının sağlanması amacıyla çocuk pornografisinin üretimini, dağıtılmasını, yayılmasını, ithalini, ihracını, sunumunu, satışını veya zilyetliğinin, eylemin vehametiyle orantılı bir şekilde cezalandırılabilir suç haline getirilmelerini bir gereklilik olarak ortaya koymaktadır.

Protokol'ün 10. maddesi bir bakıma, internetin sınır aşan kimliğinin yarattığı kontrol edilemezlik durumunun etkisiyle birlikte, bu düzenlemenin önleyici fonksiyonunu da ortaya koymaktadır. Söz konusu maddeye göre taraf devletler çocuk satışı, çocuk fahişeliği, çocuk pornografisi ve çocuk seks turizmini içeren faaliyetlerden sorumlu olanların önlenmesine, meydana çıkarılmasına, soruşturma, kovuşturma ve cezalandırılmasına yönelik uluslararası işbirliğini çok taraflı, bölgesel ve iki taraflı düzenlemelerle güçlendirmek için gerekli olan bütün adımları atacaklar ve kendi makamları, ulusal ve uluslararası sivil toplum kuruluşları ve uluslar arası örgütler arasındaki uluslararası işbirliği ve eşgüdümü geliştireceklerdir. Buna paralel olarak çocukların, satış, fahişelik, pornografi uygulamaları ve çocuk seks turizmine karşı zaafiyetini arttıran yoksulluk, az gelişmişlik gibi temel nedenleri ele almak amacıyla uluslararası işbirliğinin güçlendirilmesini teşvik edeceklerdir. Bu tespit gerçekten önem arz etmektedir. Nitekim internet üzerinden yayılan çocuk pornografisi veya çocuk satışı eylemlerine bakılacak olursa sosyal, ve ekonomik gelişmişlik düzeyinin tek başına olmasa da belirleyici bir kriter olduğu söylenebilir.

Özellikle Tayland ve Filipinler gibi az gelişmiş ülkelerde üretilen çocuklara yönelik cinsel istismarın görüntülendiği filmler önemli rol oynamaktadır. Ancak son zamanlarda özellikle eski sosyalist ülkelere gelen pornografi içerikli malzeme bu piyasada ciddi bir yer kaplamaktadır. Ancak bu değerlendirmenin tek başına mutlak bir kriter olmadığı dünyanın gelişmişlik düzeyi olarak en önde bulunan ülkelerinde yapılan operasyonlarla anlaşılmıştır. Örneğin 2003 yılında Almanya'da Marcy Operasyonu çerçevesinde Almanya'da yaklaşık 500 ev baskını yapılırken kurulan uluslar arası bağlantılarla toplam 166 ülkede 26.500 kişi soruşturmaya tabi tutuldu. Yine Almanya'da Aydınlatılmış alanlardaki olaylar [Çocuk Pornografisinin Bulundurulması ve Temini (Alman C.K. §184/5)] ve şüpheli ifadelerinden hareketle elde edilen Polis Suç İstatistiği verilerine göre, çete halinde gerçekleşen ve ticari

amaçlı çocuk pornografisine ilişkin malzemenin imali ve yayılması (Alman C.K. § 184/4) aynı zaman diliminde 191 ve 344 olaylar arasında değişirken ve 2002’de 108 olaya gerilemesine rağmen 1996 – 2002 yılları arasında çocuk pornografisine ilişkin malzemenin temin ve elde bulundurulması ile ilgili tespit edilen olayların sayısında yıllık 663’den 2002’ye bir artış gözlemlenmektedir¹⁷⁹. Bu veriler de ortaya koymaktadır ki, çocuk pornografisinin yaygınlaşmasında teknolojik gelişmeler özellikle de bilişim teknolojilerindeki gelişmeler önemli bir etken haline gelmiştir.

1.7.2.- Türk Ceza Hukukunda İnternet de Dahil Olmak Üzere Genel Anlamda Bilişim Suçlarına İlişkin Normatif Düzenleme Süreci

Türk Ceza Hukukunda interneti de kapsar nitelikte bilişim suçlarına ilişkin düzenlemelerin oluşum süreçleri incelendiğinde hiç şüphe yok ki, sadece 765 ve 5237 sayılı TCK düzenlemeleri değil 1989 yılından itibaren oluşturulan Tasarılar ve nihayet 5651 sayılı Kanunun getirdikleri de göz önünde bulundurulmalıdır.

1.7.2.1.- - 1989 TCK Ön Tasarısı

1984 yılında bir komisyon yeni bir Ceza Kanunu tasarısı hazırlamak için bir araya gelmiş ve çalışmalarını tamamlayarak tasarıyı 1987 yılında ortaya çıkarmışlardır. Fakat oldukça eleştiri toplayan bu tasarı ikinci bir komisyonla yeniden ele alınmış ve 1989 yılında yeni tasarı tamamlanmıştır.¹⁸⁰ 1989 TCK Ön Tasarısı olarak adlandırılan bu tasarının bilişim suçları bakımından önemi, ilk kez bu tasarıyla bilişim suçları Türk Hukuk Sistemine alınmış olmasından kaynaklanmaktadır. Söz konusu suçlar “Topluma Karşı Suçlar” başlıklı ikinci kısmının dokuzuncu bölümünde yer almıştır ve toplam beş maddeden oluşmaktadır. Bu maddeler 1989 TCK Ön Tasarısında düzenlenen haliyle özetlenecek olursa;

¹⁷⁹ NEUBACHER, Frank/ ROLLO, Giorgia, Çocuk Pornografisi ve İnternet – Karşılaştırmalı Hukuk Çerçevesinde Genel Bir Bakış (Çev: İlker TEPE), in: KGCHS/ 4, sh: 653.

¹⁸⁰ HAKERİ, Hakan. Tötungsdelikte Im Türkischen Stgb-Entwurf 1997,(Kaynak: http://www.akader.info/KHUKA/7_2000_ekim/totungsdeligte.htm, Erişim Tarihi: 08.07.2007)

“*Hile ile bilgi elde etme ve bunları haksız kullanma*” başlıklı 342. maddesinde bilgileri otomatik işleme tabi tutmuş bir sistemden programları, verileri veya herhangi bir unsuru hukuka aykırı olarak ele geçirme ve bilgileri otomatik işleme tabi tutulmuş bir sistemde yer alan bir programı, verileri veya diğer herhangi bir unsuru başkasına zarar vermek üzere nakletme ve çoğaltma fiilleri suç olarak düzenlenmiştir.¹⁸¹

“*Yarar sağlama, zarar verme*” başlıklı 343. maddesi başkasına zarara verme veya kendisine yarar sağlamak amacıyla bilgileri otomatik işleme tabi tutmuş bir sistemi veya verileri veya diğer herhangi bir unsuru kısmen veya tamamen tahrip etme veya değiştirme veya sistemin işlemesine engel olma ile bilgileri otomatik işleme tabi tutmuş bir sistemi kullanarak kendisi veya başkası lehine hukuka aykırı yarar sağlama fiillerini düzenlemiştir.¹⁸²

“*Sahtecilik*” başlıklı 344. maddesinde ise, delil olarak kullanılmak amacıyla sahte bir belgeyi oluşturmak için bilgileri otomatik olarak işleme tabi tutan bir sisteme, verileri veya diğer unsurları yerleştirme veya var olan verileri, diğer unsurları tahrif etmek veya bunları kullanma fiili suç olarak düzenlenmiştir.¹⁸³

“*Feri cezalar*” başlıklı 345. maddesinde, 342 ve 343. maddelerde belirtilen suçları işleyen failler hakkında öngörülen cezalara ek olarak, kamu hizmetinden veya sanat veya ticaretten yasaklanma, suçtan meydana gelen şeylerin müsaderesi, suçun işlenmesinde kullanılan kurumların veya teşebbüsün kapatılması öngörülmüştür.¹⁸⁴

“*Tüzel kişiler ve teşebbüs hali*” başlıklı 346. maddesinde bütün bölümü kapsayacak bir hüküm getirerek, bu bölüme giren suçlardan dolayı tüzel kişilerin de sorumlu olduğu, teşebbüs halinde ise tamamlanmış suçun cezasının verileceğinin belirtildiği görülmektedir.¹⁸⁵

1.7.2.2.- 3756 Sayılı Kanunla Gerçekleştirilen Düzenleme

¹⁸¹ YAZICIOĞLU, Bilgisayar Suçları, sh: 208.

¹⁸² YAZICIOĞLU, Bilgisayar Suçları, sh: 208.

¹⁸³ KURT, Levent. Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Hukukundaki Uygulaması, Ankara, 2005, sh:120.

¹⁸⁴ KURT, Bilişim Suçları, sh: 120.

¹⁸⁵ KURT, Bilişim Suçları, sh: 120 – 121,

Kanun koyucu 14.06.1991 tarih ve 3756 sayılı Kanunla 1989 TCK Ön Tasarısı kısmen de olsa 765 sayılı TCK'ya eklenmiştir. Ön Tasarının bilişim suçlarına ilişkin maddeleri 525. madden sonra gelmek üzere “Bilişim Alanında Suçlar” başlığı ile on birinci bölüm olarak eklenmiştir. Anılan Kanun ile yapılan düzenlemeler kısaca özetlenecek olursa;

TCK md. 525/a olarak kanun metnine aktarılan düzenleme 1989 TCK Ön Tasarısının 342. maddesinde öngörülen düzenlemeye (“Hile ile bilgi elde etme ve bunları haksız kullanma”) karşılık gelmektedir. Cezanın miktarı ve gerekçesi de dahil olmak üzere aynen aktarılmıştır.¹⁸⁶

Aynı şekilde TCK md. 525/b 1989 TCK Ön Tasarısındaki 343. maddeye denk gelen düzenlemenin (“Yarar sağlama, zarar verme”) gerekçesi de dahil olmak üzere aynıdır.¹⁸⁷

TCK md. 525/c maddesi ise kendisine karşılık gelen 1989 TCK Ön Tasarısı'nın 344. maddesi (“Sahtecilik”) ile bazı yönleriyle farklıdır. “*Yerleştirme ve tahrif etmenin*” cezası Ön Tasarıyla aynı tutulmuştur. Ancak Ön Tasarıda “*kullanma*”ya da aynı cezayı öngörmüşken, 3756 sayılı Kanunda tahrif edilmiş olan verileri kullanmanın cezası için daha az bir ceza öngörülmüştür.¹⁸⁸ Bunun yanında Ön Tasarısından farklı olarak, tahrif edilmiş veri veya diğer unsurları kullanmanın “*bilerek*” yapılması hususu vurgulanmıştır.¹⁸⁹

Feri Cezalarla ilgili 525/d maddesinde Ön Tasarının 345. maddesinden farklı müsadere ve kurum kapatma yer almamıştır.¹⁹⁰ Ayrıca bu bölümdeki suçlardan tüzel kişilerin de sorumlu olduğuna ve teşebbüsün tamamlanmış suç gibi cezalandırılacağına ilişkin 1989 tarihli Öntasarının 346. maddesi alınmamıştır.¹⁹¹

¹⁸⁶ **KARAGÜLMEZ**, Bilişim Suçları, sh:126 vd.; **YENİDÜNYA/DEĞİRMENCİ**. Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları, İstanbul, 2003, sh: 54.

¹⁸⁷ **KURT**, Bilişim Suçları, sh: 122.

¹⁸⁸ **DÜLGER**, Murat Volkan. Bilişim Suçları, Ankara, 2004, sh: 207

¹⁸⁹ **YAZICIOĞLU**, Bilişim Suçları, sh: 284.

¹⁹⁰ **KURT**, Bilişim Suçları, sh:124; **DÖNMEZER**, Kişiler ve Mala Karşı Cürümler, sh: 623.

¹⁹¹ **YAZICIOĞLU**, Bilgisayar Suçları, sh: 209.

1.7.2.3.- 1997 TCK Ön Tasarısı

1997 TCK Ön Tasarısı'nda yer alan bilişim alanındaki suçlar ile ilgili düzenleme 1994 Fransız Ceza Kanununu düzenlemesinden esinlendiği ve Fransız Ceza Kanununun 323-1 ile 323-7 maddesindeki suçlarla bir olduğu söylenebilir.¹⁹²

Tasarının 347. maddesi “*Bilişim sistemine girme, verileri tahrip ve bozma*” başlıklı olup maddenin birinci fıkrasında, bilişim sistemine hukuka aykırı olarak girme veya orada kalmaya devam etme suçu düzenlenmiş, ikinci fıkrasında ise bu fiil nedeniyle sistemin içerdiği verilerin yok edilmesi veya değiştirilmesi durumu ağırlaştırıcı neden olarak belirtilmiştir. Girme veya orada kalma fiili nedeniyle sistemin içerdiği bilgilere zarar verilecek olursa ayrıca birinci fıkradaki hükümden daha ağır bir ceza ile karşılanmaktadır. Üçüncü fıkrada sisteme hukuka aykırı olarak girmeye teşebbüs edilmesi halinde suç tanımlanmış bir suç gibi kabul edilmektedir. Söz konusu düzenlemenin ceza hukukunun suça teşebbüs edilmesi halinde, tamamlanmış suçtan daha hafif cezalandırılması yönündeki genel prensibi ile uyum içinde olmadığı kabul edilmiştir.¹⁹³

İlk kez bu tasarıda “*bilgileri otomatik olarak işleme tabi tutmuş sistem*” kavramı yerine “*bilişim sistemi*” kavramı kullanılmıştır.

Tasarının “*Sistemi engelleme, bozma, haksız yarar sağlama*” başlıklı 348. maddesinin birinci fıkrasında bir bilişim sisteminin işleyişini engelleme, bozma ve bilişim sistemlerinden haksız yarar sağlama, ikinci fıkrasında da bilişim sistemine hukuka aykırı olarak veriler sokma veya sistemin içerdiği verileri yok etme, veya değiştirme suç olarak düzenlenmiştir. Üçüncü fıkrasında, bu fiillerle failin başkasının zararına ve kendisinin yararına haksız bir menfaat elde etmesi halinde cezanın ağırlaştırılacağı, son fıkrasında ise bu suçlara teşebbüs halinde faile tamamlanmış suçun cezasının verileceği belirtilmiştir.¹⁹⁴

“*Sahtecilik*” başlığı taşıyan 349. maddesinde ise, hukuk alanında bir neticeye ulaşmak amacıyla sahte bir belge oluşturmak için bilişim sistemine veriler yerleştirme veya var olan verileri tahrif etme fiillerinde, ikinci fıkrasında ise belirtilen sahte belgeyi kullanma suçu

¹⁹² YAZICIOĞLU, Yeni Türk Ceza Kanunundaki Bilişim Suçlarının Değerlendirmesi, in: YÜHFD, C. II, S 2, İstanbul, 2005, s: 394

¹⁹³ KURT, Bilişim Suçları, sh:124.

¹⁹⁴ KURT, Bilişim Suçları, sh:125-126.

düzenlenmiştir. Bu anlamda madde ile düzenlenen alan ile 3756 sayılı kanunla yapılan düzenleme arasında bir farklılık yoktur. Tek fark, “bilişim sistemi” kavramının yerine “bilgileri otomatik olarak işleme tabi tutmuş sistem” ifadesinin yerine kullanılması ve belgeyi düzenleyen ile kullanan arasında kanunda var ceza farkının ortadan kaldırılmasıdır.¹⁹⁵

“Feri cezalar” başlıklı 350. maddesine yeniden müsadere eklenmiştir. “Tüzel kişilerin sorumluluğu” başlıklı 351. maddesinde ise, 347 ve 348 maddelerinde düzenlenen suçlardan tüzel kişilerinde sorumlu olduğu kabul edilmiştir. “Suç işlemek için örgütlenme” başlığı taşıyan 1997 TCK Ön Tasarısının 352. maddesinde, yukarıda maddelerde öngörülen suçları işlemek için oluşturulan bir örgütü kuran veya buna katılan kişilere işlemek istedikleri suçlardan en ağırının cezasının verileceği hükme bağlanmıştır. Bu şekilde düzenlemede ilk defa getirilmiştir.

1.7.2.4.- 2000 TCK Ön Tasarısı

2000 tarihli TCK Ön Tasarısında bilişim suçları, tasarının İkinci Kısımının “Bilişim Alanında Suçlar” kenar başlığı Dokuzuncu Bölümünde, 346 – 352 maddeleri arasında düzenlenmiştir.

1997 Ön tasarısının maddeleri 2000 Ön tasarısına bir takım değişiklikler ve para cezalarındaki güncellenmesi dışında gerekçeleriyle dahil olmak üzere olduğu gibi aktarılmıştır. Yalnızca ferî cezaların düzenlendiği 348. maddede, suçta kullanılan veya suçtan meydana gelen şeylerin müsadereyi “veya mülkiyetin devlete geçirilmesi” ifadesi kullanılmıştır.¹⁹⁶

2000 Ön tasarısında getirilen en önemli yenilik “*Banka ve Kredi Kartlarının Kötüye kullanımı*” başlıklı 349. maddesidir. Bu maddenin birinci fıkrası ile başkasına ait veya diğer bir kişiye verilmesi gereken bir kredi kartını herhangi bir şekilde ele geçiren veya bulunduran bir kişinin kart sahibinin rızası olmaksızın kullanarak veya kullandırarak kendisine veya başkasına haksız kazanç sağlaması suç olarak düzenlenmiştir. İkinci fıkrasında ise aynı fiilin

¹⁹⁵ KURT, Bilişim Suçları, sh: 127.

¹⁹⁶ ÖZEL, Cevat. Bilişim Suçları İle İletişim Faaliyetleri Yönünden Türk Ceza Kanunu Tasarısı, in: İBD, C: 75, S: 7,8,9, sh: 862.

banka veya kredi kartını tahrif ederek veya bunu sahtecilik suretiyle meydana getirerek işlendiğinde ceza ağırlaştırılmıştır.¹⁹⁷

Tüzel kişilerin sorumluluğuna ilişkin düzenleme 1997 Ön Tasarısından bir fark dışında aynen düzenlenmiştir. 1997 Ön Tasarısında tüzel kişilerin sorumluluğu bilişim sistemine girme, verileri tahrip ve bozma, sistemi engelleme, bozma, haksız yarar sağlama fiilleri ile sınırlandırılmasına rağmen bu tasarıda tüzel kişilerin bu bölümdeki tüm suçlardan sorumlu olduğu düzenlenmiştir.¹⁹⁸

1.7.2.5.- 2003 TCK Ön Tasarısı

2003 TCK Ön Tasarısında İkinci Kitabın “Topluma Karşı Suçlar” başlıklı İkinci Kısımının “Bilişim Alanında Suçlar” başlıklı 9. bölümünde bilişim suçları düzenlenmiştir.

Bu bölünme yer alan 346. maddesinde bilişim sistemine girme, verileri tahrip ve bozma, 347. maddesinde sistemi engelleme, bozma, haksız yarar sağlama, 348. maddesinde sahtecilik, 349. maddesinde ferî cezalar, 350. maddesinde banka veya kredi kartının kötüye kullanılması, 351. maddesinde suç işlemek için örgütlenme, 352 maddesinde tüzel kişilerin sorumluluğu düzenlenmiştir. 2000 TCK Ön Tasarısındaki 346, 347, 348 . maddeleri gerekçeleri de dahil olmak üzere 2003 tasarısına aynen alınmış ,sadece zamanın şartlarına uygun olarak para cezası miktarları güncellenmiştir. 349 hiçbir değişiklik olmadan aynen alınmıştır. Suç işlemek için örgütlenme başlıklı 351. maddesinde ise, aynı başlık altında temelde aynı olmakla birlikte tek farkla 2003 tasarısına alınmıştır. Bu fark madde metninden “varlığı bir veya birden çok maddi nitelikteki hazırlıklardan anlaşılan” ifadesi çıkarılmıştır.¹⁹⁹

350 ve 352. maddeler bakımından her iki Ön Tasarısında (2000 ve 2003) düzenleme farklılığı görülmemiştir.

¹⁹⁷ AKINCI,Hatice/ALIC, A.Emre/ER, Cüneyt. Türk Ceza Kanunu ve Bilişim Suçları, in: İnternet ve Hukuk (Der: Yesim ATAMER), İstanbul, 2004, sh: 266.

¹⁹⁸ AKINCI/ ALIC/ ER, Türk Ceza Kanunu ve Bilişim Suçları sh: 272-273.

¹⁹⁹ KURT, Bilişim Suçları, sh: 132.

5237 sayılı TCK'da bilişim suçları İkinci Kitabının Üçüncü Kısımının Onuncu Bölüm başlığı altında “*Bilişim Alanında Suçlar*” özel bir bölümde düzenlenmiştir. Bilgisayar ve bilgisayar aracılığıyla gerçekleştirilen iletişim de bir üst başlık olarak bilişim alanı kapsamı altında değerlendirilmiştir. Bu sebeple “Bilişim Alanında Suçlar” başlığı, bir yandan bilgisayarı, unsurlarını ve bunlarda gerçekleştirilen işlemleri kapsarken bir yandan da internet de dahil olmak üzere bilgisayar marifetiyle veri iletişimi ve naklini de koruma altına almaktadır.²⁰⁰

1.7.2.6.- 5237 Sayılı TCK

5237 sayılı TCK'de internet de dahil olmak üzere bilişim araçları ile ve/veya bilişim alanında işlenen suçlara ilişkin normatif düzenlemeler, üçüncü bölümde ayrıntısıyla ele alınacağı için bu bölümde özel olarak bir değerlendirme yapılmamıştır.

1.7.2.7.- 5651 Sayılı “İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Hakkında Kanun”

5237 sayılı TCK'nin yürürlüğe girdiği 2005 yılından sonra bilişim suçlarına ilişkin mevcut düzenlemelerin internetin gün geçtikçe artan kullanım oranına paralel olarak ortaya çıkan yeni suç tipleriyle mücadele etmek bakımından yetersiz kaldığı düşüncesiyle, sadece internet ortamında işlenebilecek suçlarla mücadeleyi mümkün kılacak bir yasal düzenlemenin gerekliliği üzerinde yoğun tartışmalar yaşanmıştır. Bu tartışmaların neticesinde 04.05.2007 tarihinde 5651 sayılı “İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Hakkında Kanun” yürürlüğe girmiştir. Bu kanunla ilk amaçlan husus, internet sükelerinin yani içerik sağlayıcı, erişim ağılayıcı, yer sağlayıcı ve toplu kullanım sağlayıcının ceza hukuku bakımından yükümlülük ve sorumluluk alanlarının belirlenmek ve böylece özellikle internet ortamında işlenebilen içerik suçlarının önüne geçmektir. Bu Kanunla özellikle, fonksiyonları ve sorumlulukları tartışmalı olan internet sükelerine ilişkin tek tek tanımlamalar ve sorumluluk alanları belirleme yoluna gidilmiştir²⁰¹.

²⁰⁰ YAZICIOĞLU, Yeni Türk Ceza Kanununda Bilişim Suçları, sh: 403; KARAGÜLMEZ, Bilişim Suçları, sh:37; DÜLGER, Bilişim Suçları, sh: 66.

²⁰¹ 5651 sayılı Kanunun internet sükelerine ilişkin düzenlemeleriyle ilgili değerlendirmeler için bkz. YETİM, Servet, İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkındaki Kanun ile Kamu Bilgi İşlem Merkezi Yöneticilerine Getirilen Yükümlülükler, in: Terazi, S:32, Ankara, 2009, sh: 85 v.d.

Keza bu düzenlemelere ikinci bölümde değinilecektir. Ancak söz konusu Kanunun en çok tartışılan iki düzenlemesi hiç şüphe yok ki internet erişiminin engellenmesi kararının verilebilmesi için oluşturulan katalog suçlar ve erişimin engellenmesi sürecidir.

Erişimin engellenmesi kararı ve yerine getirilmesinin düzenlendiği 8. maddede, bir internet içeriğinin erişiminin engellenmesi için, bu içeriğin 5237 sayılı TCK'de düzenlenen intihara yönlendirme, çocukların cinsel istismarı, uyuşturucu ve uyarıcı madde kullanımını kolaylaştırma, sağlık için tehlikeli madde temini, müstehcenlik, fuhuş, kumar oynanması için yer ve imkan sağlama suçları ile 25/7/1951 tarihli ve 5816 sayılı Atatürk Aleyhine İşlenen Suçlar Hakkında Kanunda yer alan suçların işlendiği yönünde yeterli şüphenin söz konusu olması gerekmektedir.

İkinci sorunlu husus olan erişimin engellenmesi kararı ve icrası ise, gerek bu tedbire sık başvurulması dolayısıyla internetin, kendi doğasıyla örtüşmeyen bir yasaklar ortamına dönüşmesi, ayrıca belirtilen suçları oluşturan yayınların içerik veya yer sağlayıcısının yurt dışında bulunması halinde veya içerik veya yer sağlayıcısı yurt içinde bulunsa bile, içeriği 8. maddenin birinci fıkrasının (a) bendinin (2) ve (5) numaralı alt bentlerinde yazılı suçları – yani çocukların cinsel istismarı, müstehcenlik- oluşturan yayınlara ilişkin olarak erişimin engellenmesine ilişkin kararın re'sen bir idari kuruluş olan Telekomünikasyon Başkanlık tarafından verilebilir olmasının bir güvence olmasından ziyade bir tehdit olarak algılanmasıdır. Keza anılan Kanun yürürlüğe girdikten sonra uygulanan erişimin engellenmesi kararlarının yarattığı sonuçlar bu endişelerin yersiz olmadığını ortaya koymuştur.

1.8.- İnternet Bakımından Modern Ceza Hukuku Anlayışının Normatif Alana Yansımına Örnek Olarak Federal Alman Anayasa Mahkemesinin 27.02.2008 Tarihli “Online-Araştırma” Kararı²⁰²

Modern ceza hukuku anlayışının yukarıda özetlenen çerçevesi ve eğilimleri sadece teorik düzelmeye tartışılabilir gelen bir yapıyı ihtiva etmemekte, doğrudan yasa koyucu inisiyatifine ve dolayısıyla bu inisiyatifin somut yansımaları olan normatif düzenlemelerin birinci dereceden muhatabı olan yargıya da sirayet etmektedir. Bunun en güncel

²⁰² Kararında incelenen ve sonuçlanan bu konuyla ve diğer şikayetlerle ilgili olarak orijinal metin için bkz. http://www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007.html (Erişim Tarihi: 10.01.2009, Saat: 20:00)

örneklerinden biri de Federal Alman Anayasa Mahkemesinin “Online Araştırmalar” ile ilgili verdiği karardır²⁰³.

Federal Alman Anayasa Mahkemesinin 27.02.2008 tarihli kararına esas teşkil eden dava anayasa şikayeti kurumu işletilerek açılmıştır ve davaya konu anayasa şikâyetlerinin kaynağının Anayasayı Koruma Makamlarına verilen farklı veri elde etme süreçlerine başvurma (özellikle bilgi teknolojisi sistemlerinden) ve elde edilen verilerle münasebet kurmaya ilişkin yetkilerin düzenlendiği Kuzey Ren- Vestfalya Eyaleti Anayasayı Koruma Kanununun (AKK) bazı maddeleri oluşturmaktadır.

Dava konusu düzenlemeler, özellikle 20 Aralık 2006 tarihli Kuzey Ren Vestfalya Eyaletinde Anayasanın Korunmasına İlişkin Kanunda Değişiklik Öngören Kanun ile eklenmiş veya değişikliğe tabi tutulmuştur. Buna göre anayasayı korumayla görevli birimlere iki tür soruşturma tedbirini uygulama imkanı sağlanmaktadır. Bunlardan birincisi internet içeriklerinin gizli olarak takip edilmesi ve aydınlığa kavuşturulması (1. alternatif), diğeri ise bilgi teknolojisi sistemlerine (devamında bilişim sistemleri olarak kullanılmıştır) gizli olarak erişimin sağlanmasıdır (2. alternatif). Dava konusu düzenlemede (AKK md. 5/2 -11) yer alan her iki tedbir türü arasındaki fark bilişim sistemlerine teknik erişimin dışı yansıyan görünüşü itibarıyla ortaya konulmaktadır. İnternet içeriklerinin gizli olarak açığa çıkartılması başlığı altında, anayasayı korumakla görevlendirilmiş makamların internet iletişim içeriklerini teknik olarak öngörölmüş yollarla bilgileri dahiline almaları / edinmeleri anlaşılmaktadır²⁰⁴.

Buna karşın bir bilişim sistemine gizli bir şekilde erişimden kastedilen şey ise, hedef sistemin güvenlik boşluklarının kullanıldığı veya bir casus yazılım programının kurulumu üzerinden neticeye ulaşılan teknik bir sızma (sisteme gizlice nüfuz etme) eylemidir. Hedef sisteme sızma tekniği bu sistem kullanıcısının izlenmesine, sisteme ilişkin veya sistemde bulunan kayıtlarının incelenmesine ya da sistemin uzaktan kontrol edilmesine imkan vermektedir.

²⁰³ İnceleme konusu Federal Anayasa Mahkemesi kararından önce Federal Yüksek Mahkemenin aynı konuda 2006’da vermiş olduğu karara yönelik değerlendirmeler için bkz. **KUDLICH**, Hans, Zur Zulässigkeit strafprozessualer Online – Durchsuchungen, Kaynak: <http://www.humboldt-forum-recht.de/deutsch/19-2007/index.html> (Erişim Tarihi: 04.04.2009, Saat: 13:00)

²⁰⁴ Bkz. Online Araştırmalar Kararı, prg. 5.

Md. 5/2-11'in birinci cümlesinde ilk alternatif olarak yer alan ve internet içeriklerinin gizli yöntemlerle açığa çıkarılmasına yetki veren düzenleme çerçevesinde öncelikle Anayasayı Koruma Makamlarını tarafından genel olarak erişimi mümkün iletişim içeriklerinin edinilmesi söz konusu olmaktadır. Bu duruma örnek olarak web tarayıcılar aracılığıyla erişim güvenliği tesis edilmemiş web sitelerine erişip oralardan bilgi toplama etkinliği gösterilebilir. Dava konusu edilen maddenin bulunduğu yasanın gerekçesi incelenecek olursa, bunların yanında ilgili madde Anayasayı Koruma Makamlarına anayasal düzenin tesisi ve muhafazası açısından özel öneme sahip bilgileri edinmek amacıyla elektronik posta adreslerine veya erişim güvenliği tesis edilmiş web sitelerine erişimi mümkün kılmak için bu konuyla iştigal eden muhbirler veya Key Logging adı verilen yazılım temelli bazı programlar kullanmak suretiyle hedefe gizli teknik yöntemler kullanılmasına da yetki vermiştir²⁰⁵.

Md. 5/2-11'de ikinci alternatif tedbir olarak düzenlenen bilişim sistemlerine teknik sızma yöntemleri kullanılmak suretiyle erişim konusu "Online Araştırma" başlığı altında yakın geçmişte gerek hukuk gerekse siyaset mecralarında sıkça tartışılmıştır. Bu tarz yöntemler dava konusu edilen madde hükmünün tesisine kadar federal makamlarca herhangi bir özel yasal yetkilendirme söz konusu olmaksızın münferiden uygulanmaktaydı. O zamana kadar gerçekleştirilen bu uygulamaların neticesi ve uygulama yöntemlerine ilişkin olarak yeterli bilgiye ulaşılamamaktadır. Yukarıda da değinildiği üzere anayasa şikayetine konu edilen eyalet düzenlemesi, alman makamlarının "online- araştırma" tedbiri bakımından yetkilendirilmeleri konusunda atılmış ilk somut adım olma özelliğini taşımaktadır. Ancak bu düzenlemeyle birlikte hangi makamın hangi koşullar altında bu tedbire başvurma konusunda yetkilendirilmesi gerektiği husus tartışma yaratmıştır. Özellikle günümüzdeki tartışmalar, söz konusu tedbirin uygulanması konusunda yetkilendirmenin federal emniyet teşkilatı için uluslar arası terörizm tehlikesiyle mücadele amacına yönelik oluşturulduğu/düşünüldüğü üzerinde yoğunlaşmaktadır²⁰⁶.

Online- araştırmalar, özellikle radikal ve terörist örgütlenme içinde yer alan faillerin suç teşkil eden eylemlerinin hazırlanış ve icra ediliş aşamasına ilişkin diğer örgüt üyeleriyle bilişim teknolojisi araçlarını bilhassa da interneti kullanarak iletişime geçmeleri nedeniyle yaşanan soruşturma güçlükleri göz önünde bulundurularak düzenlenmişleridir. Sözlü olarak

²⁰⁵ Bkz. Online Araştırmalar Kararı, prg. 6.

²⁰⁶ Bkz. Online Araştırmalar Kararı, prg. 8/aa.

bilgilerine başvuru Federal Emniyet ve Anayasanın Korunmasıyla Görevli Federal Birim Başkanları, terörist şiddet eylemlerinin hazırlanışında teröristlerin küresel ölçekte haberleşmelerini sağlamak amacıyla bilişim teknolojileri sistemlerini kullandıkları, radikal ve terörist çevrelerin mensuplarının yasa dışı eylemlerine ilişkin olarak kayıt altına aldıkları verileri de özel şifreleme yöntemleri kullanarak dış ve yetkisiz erişime kapatmaları için bu hazırlık veya eylemlere yönelik gerçekleştirilecek operasyonlarda klasik soruşturma yöntem ve tedbirlerinin yani örnek olarak bilişim sistemine el koyma ya da ay temelli iletişimin dinlenmesi tedbirlerinin çok zorlanacaklarını ve hatta kimi zaman bunların soruşturmayı yürütme bakımından kullanılmasının imkansızlaşacağını ifade etmişlerdir²⁰⁷.

Md. 5/2'de düzenlenen tedbirler prensip olarak aynı kanunun 7. ve 3. maddelerinden hareketle, istihbari nitelikli veri teminini gerekli kılacak koşullar altında yapılması öngörülmüştür. Buna göre, bu tedbirler uygulanmak suretiyle elde edilen veriler ya anayasanın korunması bakımından önem arz eden girişim veya eylemlerle ilişkili bilgilerin ya da bu bilgilere ulaşımı mümkün kılacak kaynakların edinimi sağlanacaktır. Dava konusu edilen maddedeki tedbirler Anayasanın 10. maddesinde yer alan posta, mektup ve telekomünikasyon gizliliğine yasal müdahalelerle aynı çerçevede değerlendirildiği üzere, online arama ve internet içeriklerinin açığa çıkarılması gibi tedbirlerin uygulama tarz ve ağırlıkları ile ilgili posta, mektup ve telekomünikasyon gizliliğinin sınırlanmasına ilişkin kanun (10. madde kanunu) da öngörülmüş ölçütlerin geçerli olduğu ifade edilmiştir.

Anayasa şikayetinde bulunanların kim olduğuna ve hangi çerçevede başvurduklarına gelince, başvuruçulardan biri bir gazetecidir ve internet ortamında sunulan bir yayın için yazılar yazmaktadır. Mesleki faaliyetleri çerçevesinde, anayasal düzene muhalif kişi ve örgütlerce işletilen internet sitelerini ziyaret etmektedir. Bireysel olarak verilerin korunması hukukunun sorunlarıyla ilgilenen bu gazeteci başkalarıyla birlikte www.stop1984.com web sitesini işletmektedir. Bu web sitesi bünyesinde dileyen herkesin chat adı verilen sohbetlere katılabileceği ortamlar mevcuttur ve bu imkandan hukuk sisteminde radikal addedilen kişiler de kullanmışlardır. Bu kişilerin bilgileri kaydedilmiştir. Kaydedilen bu bilgiler başvuruçunun özel amaçlarla da kullandığı bilgisayarında mevcuttur.

Diğer şikayetçi ise Kuzey Ren Vestfalya eyaleti anayasayı koruma birimlerince faaliyetleri gözlem altında tutulan, DIE LINKE partisinin aynı eyaletteki örgütlenmesinin

²⁰⁷ Bkz. Online Araştırmalar Kararı, prg. 7.

aktif görev alan bir üyesidir. Bu kişi siyasi faaliyetlerini internet bağlantısı da bulunan kişisel bilgisayarından gerçekleştirmektedir. Yukarıda aktarılan şikayetçide olduğu gibi bu bilgisayar aynı zamanda şikayetçinin özel münasebetlerini kurduğu, interaktif bankacılık sistemlerinden yararlandığı bilgisayardır.

Nihayet son başvuruçular bir avukatlık bürosunun iki mensubudur. Bu kişilerden biri avukat olarak özellikle göçmenler ve ilticacılar üzerinde yoğunlaşmaktadırlar ve müvekkileri arasında Kuzey Ren Vestfalya eyaleti anayasayı koruma birimlerinde tehlikelilikleri nedeniyle etkinlikleri gözlem altına tutulan yasa dışı bir terör örgütünün (PKK) lider kabul edilen bir üyesi de bulunmaktadır. Bahsi geçen avukat gerek evinde gerekse ofisinde internet bağlantısı bulunan bilgisayar ağlarını kullanmaktadır. Ofiste kullandığı ağ aynı zamanda diğer şikayetçi tarafından da özel ya a genel amaçlara yönelik kullanılmaktadır.

Yukarıda belirtilen şikayetçiler tarafından dava konusu edilen md. 5/2-11'den hareketle, söz konusu normla Federal Anayasanın 1/1, 10/1 ve 13/1. maddelerinin atfıyla md. 2/1'in ihlal edildiği iddia edilmektedir.

Söz konusu maddede düzenlenen tedbirlere internet araçları vasıtasıyla kurulan bir iletişime gizli dahil/ taraf olma durumu söz konusu olduğundan, bu tedbirlerin haberleşme gizliliğine bir müdahale olarak düzenlendiği görülmektedir. Şayet aynı şekilde erişilen bilişim sistemi bir konutta bulunuyorsa, dava konusu edilen uygulamalar, mekansal olarak dış müdahaleye kapatılmış bir alana müdahale olmak anlamında, federal anayasanın 13. maddesinde düzenlenen konut dokunulmazlığı güvencesine de bir ihlal niteliği taşımaktadır. Her iki durumda uygulamaların muhatabı açısından genel kişilik hakkının zarara uğratılması söz konusu olabilir²⁰⁸.

Madde 5/2'ye göre belirlenen tedbirlerin Federal Anayasanın 13. maddesine bir ihlal olarak değerlendirilebilmeleri halinde, söz konusu tedbirleri düzenleyen maddenin anayasaya aykırılığı ortaya çıkacaktır. Çünkü federal anayasanın 13 maddesinde güvenceye alınan konut dokunulmazlığı güvencesine getirilen sınırlandırmaların düzenlendiği 2 ila 7. fıkralarda bu yönde bir koşul bulunmamaktadır. Bu durum aynı zamanda federal anayasanın 19. maddesinin birinci fıkrasının 2. cümlesi bakımından da sorun teşkil etmektedir.

²⁰⁸ Bkz. Online Araştırmalar Kararı, prg. 220.

Bunların yanı sıra md. 5/2 normun açıklığı kuralını da zedelemektedir. Maddenin 2. cümlesinde yer alan ve anayasanın 10. maddesine ilişkin kanunu işaret eden yollamada ne koşullar ne de kapsam belirlenmemiştir. Ayrıca özel yaşamın çekirdek alanında bireysel gelişimin korunmasına ilişkin olarak normatif koşulların eksikliği de göze çarpmaktadır. Nihayet bu düzenleme ile ölçülülük ilkesi de zedelenmiştir. Çünkü getirilen tedbirlerde müdahalenin ağırlığı/ sınırına yönelik yasal bir kayıt bulunmamaktadır. Bunun yanında usul hukuku çerçevesinde online- araştırma veya internet içeriklerinin açığa çıkarılması tedbirlerinin uygulanmasına ilişkin olarak muhatapın hakkını koruma anlamında, örneğin bir hakim kararı gibi, güvencenin getirilmemiş olması da bir eksiklik²⁰⁹.

Anayasa aykırılığı iddia edilen bu düzenlemelere ilişkin federal makamlardan alınan değerlendirmelere de kısaca bakmakta yarar vardır. Anayasa şikayetlerine ilişkin olarak Federal Hükümet doğrudan şikayet konusu normlara ilişkin olmaksızın genel çerçevede bilişim sistemlerine teknik araçlarla gizli erişiminden kaynaklanan anayasa hukukuna dair sorunları müzakere etmiştir.

Federal Hükümete göre bu tür tedbirler Federal Anayasanın 10. maddesinde düzenlenen iletişimin dinlenmesi tedbirinden farklı olarak telakki edilmelidir. Bu kapsamda öngörülen güvencelerin dışında tedbirlerin yapısına uygun güvenceler tesis edilmelidir. Anayasanın korunması amacına hizmet eden nitelikli bir araç olarak kabul edilen bir bilişim sistemine teknik imkanlar kullanmak suretiyle gizli erişim usul hukukuna bakımından özel bir takım güvenlik önlemlerine ihtiyaç duymaktadır. İlgili makama ya da birimlerce belli arama parametreleri çerçevesinde önem arz eden enformasyonların kopyalanması ya da üzerinde oynanması söz konusu olmadan, sadece bu makamların kayıtlarında yer alan verilerin yüzeysel olarak incelenmesinde dahi, bireylerin özel yaşamlarını idame ettirme haklarının çekirdek alanının korunması şarttır. Yine konut içi arama veya dinleme tedbirinde olduğu gerçekleştirilecek erişimin bir hakim kararına dayandırılması beklenebilir. Ayrıca prensip olarak bu tedbire muhatap olan bireylerin bilgilendirilmeleri bir yükümlülük olarak öngörülmelidir. Nihayet online arama tedbirleri bakımından, tedbirin ağırlığı dolayısıyla yüksek bir ölçülülük değerlendirmesi yapılmalıdır. Anayasayı koruma makamları için bu tedbirlerin hayata geçirilmesi, başka hiçbir tedbirin neticeye ulaşmak bakımından yeterli

²⁰⁹ Bkz. Online Araştırmalar Kararı, prg. 128.

imkanı sağlamadığı hallerde son araç olarak kullanılması koşuluna bağlanmalıdır(ultima ratio)²¹⁰.

Kuzey Ren Vestfalya Eyalet Hükümetine göre md. 5/2’de öngörülen tedbirler federal anayasanın 13. maddesinde düzenlenen konut dokunulmazlığı hakkını ihlal etmemektedir. Bu temel hak, ancak somut olarak mekan haline getirilmiş, yani mekansal açıdan sınırları aşılması halinde ihlal edilebilir. Bu düzenlemede böyle bir durum söz konusu değildir. Ayrıca internet içeriklerinin açığa çıkartılması tedbiri e- posta trafiğinin veya Internet üzerinden kurulan telefon görüşmelerinin dinlenmesi/izlenmesi tedbirinde olduğu gibi anayasanın 10. maddesi kapsamında tesis edilmiş bir tedbirdir²¹¹.

Görüşlerine başvuru olan başka bir kurum olan Federal Yüksek İdare Mahkemesi ise bilişim sistemine gizli yöntemlere erişim konusunda yetkilendirmeyi içeren md. 5/2 konusunda anayasal hukuka dair bir takım endişelerin söz konusu olduğu açıklamıştır. Mahkemeye göre Federal Anayasanın 13. maddesinin hem lehine hem de aleyhine olmak üzere nitelikli argümanlar ortaya konulmuştur. Her durumda düzenlenen erişim bir enformasyona dayalı otonomi hakkına müdahale anlamına gelmektedir. Ayrıca söz konusu müdahalenin ölçülü olup olmadığı konusunda tereddütler vardır. Tedbirin yoğunluğu dolayısıyla online aramanın ancak belli hukuksal değerler için somut tehlike halinde işletilmesi gerekmektedir. Fakat kanun özel yaşamın idamesini ilgilendiren çekirdek alanın korunmasına ilişkin herhangi bir önlem tesis etmemiştir²¹².

Anayasa şikayetleri ayrıntılı olarak temellendiren Federal Anayasa Mahkemesi, AKK md. 5/2- 11 ‘de düzenlenen her iki alternatif de anayasaya aykırı bulunmuş ve yok hükmünde olduğuna karar vermiştir.

Buna göre bir bilişim sistemine gizli olarak erişim olarak tanımlanan “Online Araştırma”yı düzenleyen md. 5/2-11’in ikinci cümlesi bilişim sistemlerinin bütünlüğü ve güvenilirliğinin korunmasını bekleme hakkı olarak ifade edilebilecek özel görünüm dahilinde genel kişilik hakkını ihlal etmektedir²¹³.

²¹⁰ Bkz. Online Araştırmalar Kararı, prg. 130.

²¹¹ Bkz. Online Araştırmalar Kararı, prg. 133.

²¹² Bkz. Online Araştırmalar Kararı, prg. 138.

Genel kişilik hakkının bu görünümü bilişim sistemlerini yöneltilem müdahalelere, Federal Anayasa md. 10, md. 13 veya bunlarla birlikte enformasyon üzerindeki otonomi hakkı gibi diğere temel hakların koruma güvencesi tesis etmedikleri hallerde, karşı koruma getirmektedir. Sorun dava konusu şikayetler bakımından ele alınacak olursa, tesis edilen tedbirlere gerçekleştirilen müdahalelerin anayasa hukuku açısından hukuka uygun olmadığı sonucuna varılmaktadır. Şöyle ki; md. 5/2 normun açıklığı kuralına, ölçülülük ilkesinin şartlarına uygun olmamakla birlikte özel hayatın idamesi açısından gerekli çekirdek alan korumasını da ortaya koymaktan uzaktır. Bu çerçevede inceleme konusu norm yok hükmündedir ve diğere temel haklar ölçüsünde ek bir incelemeye ihtiyaç bulunmamaktadır.

Md. 5/2, bilişim sistemlerinin bütünlüğü ve güvenilirliğinin korunmasını bekleme hakkı olarak ifade edilebilecek özel görünüm dahilinde genel kişilik hakkına müdahalelerde bulunma yetkisi vermektedir. Bu temel hakkın enformasyon üzerindeki otonomi hakkı, ve Federal Anayasa md. 10 ve 13'de sunulan özgürlük güvenceleri gibi diğere somutlaşmış görünümleri, bu müdahaleler karşında hiç veya yeteri kadar güvence sağlayamamaktadır.

Genel kişilik hakları kişiliğin, başka bir temel hak ve özgürlük alanı tarafından koruma garantisi altına alınmayan ancak kişiliğin yapısal anlamı bakımından göz ardı edilemeyecek unsurlarını güvence altına almaktadır. Böylesi bir torba güvence, özellikle bilim ve teknolojinin gelişmesi ya da yaşam koşullarındaki sair değişikliklerin neden olacağı yeni tehlikelerin ve tehditlerin önlenmesi amacıyla öngörülmüştür.

Bilişim teknolojilerinin kullanımı geçmişte kişiliğin geliştirilmesi sürecinde fazla göz önünde bulunan ve bu süreçler üzerinde etki sahibi olan bir konumda bulunmamaktaydılar. Modern iletişim teknolojilerinin gelişmesiyle birlikte birey birçok yeni imkana kavuşmakla birlikte bu teknolojiler aynı zamanda bireyin kişiliği üzerinde yeni tarz ve şekillerde tehlikelerin de temelini oluşturmuştur.

Bilgi iletişim teknolojisinde son zamanlarda yaşanan gelişmeler, bilişim sistemlerinin hayatın her alanına sirayet ettiği ve birçok kişi tarafından merkezi bir yaşam unsuru haline gelmesi sonucunu doğurmuştur.

²¹³ Bkz. Online Araştırmalar Kararı, prg. 165.

Bu durum öncelikle, yapılan arařtırmalara göre Federal Almanya'da net bir çoğunluęun sahip olduęu kiřisel bilgisayarlar için geçerlidir. Bu biliřim aygıtının faaliyet yeteneęi, ana bellek ve buna baęlı kayıt cihazlarının kapasitesinin arttırılmasıyla geliştirilmiř ve çok farklı amaçlara hizmet etmeye müsait hale getirilmiřtir. Böylece kiřisel bilgisayarların kiřilik gelişimi sürecindeki rolü daha da artmış ve çok ciddi bir anlam kazanmıştır. Bilgisayarların yaygınlaşması ve bir aę baęlantısı dahilinde kullanılmaya başlamalarıyla birlikte biliřim sistemlerinin imkanları münferit bilgisayarlara nazaran daha geniř kitlelere ulařmaya başlamıştır. Buna baęlı olarak da biliřim teknolojilerindeki gelişmeler fonksiyon arttırma odaklı bir seyir izlemeye başlamıştır ve bu süreç her geçen gün yeni eklenen fonksiyonlarla devam etmektedir. Bilgisayarlar arası iç içe geçmiş bir aę olarak kabul edilen internet bu gelişim sürecinin önemli bir sonucudur. İnternetin kullanılmasıyla birlikte bir bilgisayardaki veriler dięer bir bilgisayara bir aę üzerinden kolaylıkla aktarılabilmesi saęlanmıştır. Bunun yanında internet aktif sosyal münasebetlerin kurulduęu ve geliştirildięi birçok haberleşme hizmetlerini de kullanıma sunmuştur. Böylece artık internetin iletiřim imkanları sunduęu kolaylıklar dolayısıyla klasik iletiřim araçlarının ikinci plana itilmesine zemin hazırlamıştır²¹⁴.

Bir aę baęlantısı dahilinde kullanılan biliřim sistemlerinin çoęalması bireyin kiřilięini özgürce geliřtirmesi konusunda bir çok imkan saęlarken, bunların yanında da kiřilięe karřı yöneltilecek birçok yeni tehlikeyi de beraberinde getirmektedir. Bu tehlikeler aęrlıklı olarak kiřisel bilgisayarlar gibi karmařık bilgi iletiřim sistemlerinin sunduęu kullanım imkanlarındaki geniř skaladan kaynaklanmaktadır. Öyle ki bu imkanların verilerin üretimi, işlenmesi, kaydedilmesi ve aktarılması şeklinde kendini göstermektedir. Burada söz konusu olan sadece sistem kullanıcısının bilgisi dahilinde işlenen ve kayıt altına alınan veriler deęildir. Veri işleme süreçleri çerçevesinde biliřim sistemleri tarafından otomatik olarak üretilen ve kullanıcının hareketleri ve özelliklerine iliřkin deęerlendirme imkanı vermeye muktedir veriler de buna dahildir. Biliřim sistemlerin internet veya dięer aęlar vasıtasıyla sosyal iletiřime ve sair ortak kullanıma açılmasıyla birlikte bu verilerin üçüncü kiřiler tarafından edinilmeleri imkan dahiline girmiř ve bir tehlike olarak kendini hissettirmeye başlamıştır²¹⁵.

Daha çok bir şekilde ifade etmek gerekirse, sistemin üçüncü kiřilerle baęlantı kurmaya olanak tanıyan bir aę dahilinde kullanılmaya başlaması, sistem içinde yer alan verilerin temini

²¹⁴ Bkz. Online Arařtırmalar Kararı, prę. 179.

²¹⁵ Bkz. Online Arařtırmalar Kararı, prę. 180.

veya manipüle edilmeleri amacıyla kullanılacak kullanıcı isteği dışında erişim imkanlarını ortaya çıkarmıştır. Bu tür erişimlere karşı nispeten koruma tedbirleri almak mümkündür ancak internetin sosyal yapılanma içinde gelmiş olduğu konum, sistemin yüksek karmaşıklık derecesi bireysel koruma önlemlerinin bir takım güçlüklerle karşılaşmasına neden olabilmektedir. Öyle ki, bu tarz sızma veya manipülasyon girişimlerine karşı kullanılan şifreleme veya hassas verilerin gizlenmesi tedbirleri de üçüncü kişiler tarafından etkisiz hale getirilebilmektedir. Son olarak şunu ifade etmek mümkündür ki, bilişim teknolojisindeki gelişimin hızı, kullanıcıların gelecekte kendilerini teknik olarak korumalarını sağlayacak hangi imkanların söz konusu olacağı konusunda bir öngörünün oluşmasını engellemektedir.

Bu bağlamda bilişim sistemlerinin kullanılmasıyla bağlantılı olarak kişiliğin geliştirilmesi ve bunun karşındaki tehlikeler temel ve önemli bir koruma ihtiyacının da beraberinde getirmiştir. Bireyler devletten engellenemez nitelikte bir hak olan kişiliğin geliştirilmesi perspektifinden yaklaşıldığında bu amaca hizmet eden bu tür sistemlerin bütünlüğünü ve güvenilirliğini güvence altına alınması yönünde haklı bir talebi ileri sürebilirler. Federal Anayasa Mahkemesinin şu zamana kadar vermiş olduğu kararlar da kendini gösterdiği üzere bilişim teknolojilerinin gelişimiyle birlikte Federal Anayasanın 10. ve 13. maddeleriyle tesis edilen ve genel kişiliğin gelişimini mümkün kılan temel hak korumalarının yukarıda anılan koruma gereksinimini karşılar nitelikte olmadıkları görülmektedir.

Federal Anayasa Mahkemesinin bundan önce verdiği kararlarda genel kişilik haklarına ilişkin belirlenimler, özellikle de özel alanın korunmasının veya enformasyona dayalı otonomi hakkının güvenceye alınması, enformasyon sistemlerinin kullanılmasından kaynaklanan koruma gereksinimini yeterli ölçüde karşılamaya elverişli değildir. Örneğin özel alanın korunması olarak ortaya konulan belirlenim içerisinde bireyin genel kişilik hakları mekan ve konu olarak belirli bir çerçeve içerisinde telakki edilmektedir. Fakat bir bilişim sisteminin kullanılmasının yaratacağı koruma gereksinimi sadece bireyin özel alanını ilgilendiren verilerle sınırlandırılmaz. Çünkü sisteme sızılmasıyla birlikte artık sadece özel nitelikli veriler hedef alınmamakta, aksine hedef sistem kullanıcısı hakkında kapsamlı bir resim çizebilmeyi mümkün kılan tüm verilere ulaşılabilmektedir²¹⁶.

²¹⁶ Bkz. Online Araştırmalar Kararı, prg. 167.

Enformasyon üzerindeki otonomi hakkı ise kişiye özel alanın korunmasını aşan bir karaktere sahiptir. Bu hakkın tesisi ile getirilmek istenen güvence, bireyin kendisini ilgilendiren kişisel verileri üzerinde kendi inisiyatifıyla tasarrufta bulunabilmesini sağlamaktır. Enformasyon üzerindeki otonomi hakkı aynı zamanda mahremiyetin ve istenç özgürlüğünün korunması ile desteklenmekte ve geliştirilmektedir. Bireyin, kontrolü ve bilgisi dışında icra edilen veya önlem alamayacağı bir şekilde kişiliğiyle ilgili verilerin kullanılması ve diğer verilerle ilişkilendirilmesi halinde bu temel hakkın ihlal edildiği sonucuna ulaşılabilmektedir.

Ancak enformasyon üzerindeki otonomi hakkı da bireyin bilişim teknolojilerini kullanmak suretiyle kişiliğini geliştirmesi çevreleyen ve bu sistemde yer alan verilerin güvenilirliğine ya da bizatihi sistemi kullanırken herhangi bir şüpheye kapılmadan hareket etmeye yönelik yeterli bir güvenceyi ortaya koyamamaktadır. Çünkü mahsus bilişim sistemine erişimle birlikte aktüel olarak kişisel verilerin ilgisinin rızası hilafına işleme tabi tutulması söz konusu olmaksızın, salt bu sisteme erişimle veriler üzerinde kapsamlı potansiyel bir güvenlik zaafının ortaya çıktığı görülmektedir. Dolayısıyla bu tarz erişimler, enformasyon üzerindeki otonomi hakkının güvenceye aldığı, ilgilinin kişiliğini ilgilendiren münferit veri teminden daha üst bir korumayı gerektirir²¹⁷.

Genel kişilik hakkının boşluk doldurucu fonksiyonu göz önünde bulundurularak bahsi geçen koruma gereksinimi bilişim sistemlerinin bütünlüğünün ve güvenilirliğinin teminat altına alınmasıyla karşılanabilir. Bir hak olarak Bilişim sistemlerinin bütünlüğünün ve güvenilirliğinin korunması, enformasyon üzerindeki otonomi hakkı gibi Federal Anayasa md. 1/1 atıfla md.2/1'e dayanmaktadır. Bu hak ile temel hak öznelerinin kişisel ve özel yaşam alanlarının bir parçası olarak bilişim teknolojilerine, sadece iletişime sürecine veya kaydedilmiş verilere yönelik olmaksızın, devlet kanalı ile erişimin önlenmesi düşünülmektedir.

Bilişim sistemlerinin güvenilirliklerinin ve bütünlüklerinin güvence altına alınması temel hakkı sınırsız bir hak değildir. Bu hakka gerçekleştirilecek müdahaleler gerek yasal tedbir amaçları gerekse soruşturma koşullarına bağlı olarak hukuka uygun hale gelmektedir. Birey, temel hak sınırlaması niteliğinde olan ve anayasa uygunluk içerisinde gerekli yasal düzenlemelerce ortaya konulmuş bu tür durumlara rıza göstermek mecburiyetindedir. Dava

²¹⁷ Bkz. Online Araştırmalar Kararı, prg. 207.

konusu düzenleme bakımından yapılan bir incelemede anayasayı koruma makamlarına verilen yetkinin ve uygulamaların bununla bağdaşmadığı gözlemlenmektedir. Bir bilişim sistemine gizli olarak erişimin sağlanması tedbirinin düzenleyen madde ölçülülük ilkesi paralelinde de incelendiği takdirde, ilgili hükmün ölçülü bir düzenlemeyle ele alınmadığı da görülecektir. Bilindiği üzere ölçülülük genel olarak, bir temel hakka müdahalede meşru bir amaca ulaşmak bakımından amaçla uyumlu ve meşru araçların gerektiği oranda kullanılması üzerinden dile getirilmektedir. Kurulmuş bir barış ve güven ortamı olarak devletin güvenliğinin sağlanması ve vatandaşların vücut bütünlüğünün, yaşamlarının ve özgürlüklerine yönelik tehlikelerin bertaraf edilmesi diğer hukuksal değerlerle aynı koruma seviyesinde bulunan anayasal değerlerdir. Bunların temeli Federal Anayasa md. 2/2 c.1 ve md. 1/1 c.2’de yerini almıştır. Elektronik veya dijital iletişim araçlarının artan bir oranda kullanılmaları ve bunların tüm yaşam alanına sirayet etmesi, anayasayı koruma makamlarının görevlerini icra etmelerinde ciddi güçlükler ortaya koymaktadır. Bu bakımdan bu kurumların radikal ve terörist örgütlenmelerle mücadelelerinde modern iletişim araçlarını onlar gibi kullanmaları ve anayasal düzen muhalifliği niteliğinde suç teşkil eden eylemlerin önüne geçmeleri bakımından kabul edilebilir bir durumdur. Keza bilişim sistemlerine gizli olarak erişim de bu amaca hizmet ettiği oranda elverişli ve gerekli bir yöntem olarak kabul edilebilir²¹⁸.

Ancak bir bilişim sistemine gizli olarak erişimin ölçülülük ilkesi bakımından sorunları mevcuttur. Her şeyden önce böylesi bir tedbirin uygulanması yukarıda zikredilen amaçlara ulaşılmasının dışında sistem kullanıcısı tarafından ciddi bir potansiyel risk taşımaktadır. Çünkü sızma yöntemiyle, sistem kullanıcısının bilgisi olmaksızın sistemine erişim ve oradan bilgi temini esnasında, tedbirin amacının dışında ilgilinin genel profili hakkında da bir çok veriyi temin etme imkanı söz konusudur. Bu da ciddi bir genel kişilik hakkı ihlali anlamına gelmektedir ki, amaç ile araç arasındaki ölçülülüğün kaçırılmasına zemin hazırlamaktadır. Bunun ötesinde böyle bir tedbirin kullanılabilir olması durumunda, ilgililer bilişim sistemlerini kullanmak suretiyle girişecekleri iletişimlerde sürekli bir izlenme korkusuyla hareket etmek durumunda kalacak ve her ne suretler olursa olsun uhdelerinde bulunan verilerin devlet makamlarınca dilekleri zaman temin edilecekleri endişesiyle doğrudan özgür hareket edebilme iradesinde ciddi engellemeler söz konusu olacaktır²¹⁹.

²¹⁸ Bkz. Online Araştırmalar Kararı, prg. 220.

²¹⁹ Bkz. Online Araştırmalar Kararı, prg. 227.

Ölçülülük bakımından yapılacak bir başka değerlendirme noktası da böyle bir tedbirin uygulanmasının ancak müdahale edilen temel haktan daha üstün bir hakkı korumaya yönelik olarak somut tehlike durumlarında uygulanabileceğinin belirlenmiş ve bu ilke doğrultusunda düzenlenmiş olması gerekliliğidir. Bu bağlamda bir tehlikenin gerçekleşebilme olasılığının derecesinin somut tehlike koşulunu gerçekleyen bir niteliğinin olması beklenmelidir. Dolayısıyla somut tehlike koşulunun belirlenmesinde şu üç hususun gerçekleşmiş olması aranması gerekmektedir. Öncelikle somut bir tehlikenin kabulü için tek başına bir olay veya durumun söz konusu olması gerekmektedir. Ardından bu tehlikenin yakın bir zaman içerisinde gerçekleşme ihtimalinin yüksek olası ve son olarak da tehlike kaynağı olarak belli bir kişiyle söz konusu tehlikenin ilişkilendirilebilir olması gerekmektedir. Bu şartlar gerçekleştiğinde ortada somut bir tehlikenin varlığı kabul edilmektedir. Somut tehlike belirlenimi gerçekleştiikten sonra ise bu tehlikenin önlenmesi için bir temel hakka, dava konusu itibariyle bir bilişim sisteminin güvenilirliğinin ve bütünlüğünün korunması, gerçekleştirilecek müdahalenin hukuka uygun olması için, müdahale ile korunması amaçlı hukuksal değer kendisine müdahale edilen temel haktan daha üstün bir hak olması gerekmektedir. Fakat dava konusu edilen her iki tedbir açısından da hem somut bir tehlikenin varlığı aranmaksızın anayasayı koruma makamlarınca duyulan şüphenin ilgili tedbirlerin uygulanması için yeterli kabul edilmesi hem de somut durumda anayasayı koruma makamlarınca kişiler tarafından kullanılan bir bilişim sistemine sızma veya diğer teknik yollarla gizli erişim sağlanması ve veri temininin Federal Anayasa md. 1/1 c.2 ve md. 2/2 c.1 temelinde şekillenen bir temel hakka müdahale olması bakımından daha üstün bir hukuksal değer korunması amacının zikredilmemiş olması hasebiyle ölçülülük ilkesinin göz ardı edildiği sonucu ortaya çıkmaktadır. Böylece söz konusu temel hakkın tüm müdahalelerden uzak çekirdek alanına da tecavüz edilmiş olmaktadır. Zira bu durum temel haklarda öz garantisinin de çiğnendiği sonucunu doğurmaktadır.

1.9.- Değerlendirme: Modern Ceza Hukuku Teorisinde İnternet Suçluluğunun Yeri ve Türk Hukukundaki Yansımaları

Modern toplumun bilgi toplumu olarak telakki edildiği günümüzde bilişim- iletişim teknolojilerindeki gelişmeler toplumsal hayatın sistemli bir şekilde devamlılığı hususunda çok önemli bir yere sahiptir. Özellikle yaygınlaşan bilgisayar ağları ve veri transferi imkanıyla dünyanın herhangi bir noktasında herhangi başka bir noktasına ulaşım çok hızlı ve az maliyetli olarak mümkün hale gelmiştir. Bu bağlamda bilişim – iletişim teknolojileri arasında

en etkin rolü hiç şüphe yok ki internet üstlenmektedir. Öyle ki artık internetin oluşturduğu sanal dünya, gerçek dünyanın sunduğu tüm olanakları barındırmakta ve bu dünyanın sakinleri yani internet kullanıcılarını “*net citizen veya netizen*” kimliği altında bir araya getirmektedir.

İnternet modern toplumun temel unsuru olan bilgiye erişim ve kullanım alanında hiçbir iletişim aracının ulaşamadığı bir etkinliğe sahip olmuştur. İnternet kullanıcıları artık arama motorları vasıtasıyla edinmek istedikleri verilere dünyanın neresinde olursa olsun saniyeler hatta saliseler içinde erişebilmektedir. Bunun dışında günlük hayatta çok zaman alan işler internet aracılığıyla sağlanan hizmetlerle aynı şekilde çok kısa zamanda tamamlanmaktadır. Klasik iletişim araçları olarak nitelendirilebilecek olan telgraf, telefon, mektup artık internet sayesinde çok sık kullanılmaz olmuş, bunların yerini e- posta, eş zamanlı görüntülü ve/veya sesli iletişim imkanı veren programlar almaktadır. Artık basın kuruluşları yatırımlarını kullanıcının isteği ve beklentisi doğrultusunda gazete, dergi v.b. kitle haberleşme araçlarına değil internete yapmaktadırlar. Çünkü bilgi toplumunda bilgiye erişim hızı çok önem arz etmektedir. Örneğin gazeteler internet ortamında hazırladıkları web siteleri aracılığıyla gelişmeleri anında kamuoyu ile paylaşabilir hale gelmişlerdir. Hatta üçüncü bölümde ayrıntılarıyla açıklanacağı gibi günümüzde sanal sınıf ve dersanelerle dersler ve sınavlar dahi internet ortamında icra edilebilmekte, öğrenciler evlerinden bir internet bağlantısı ile öğretmen ve diğer öğrencilerle birlikte eğitim ve öğretim faaliyetine katılabilmektedirler. İnternetin toplum yaşantısına etkileri tek tek saymakla bitirilemez. Ancak şunu söylemek pekâlâ mümkündür ki, internet bilgi toplumunun en önemli yapısal dinamiği haline gelmeye başlamıştır.

Bu denli büyük imkânlar sunan internet hiç şüphe yok ki bir o kadar da riskli bir yapılanmadır. Çünkü internet, ağların ağı olması hasebiyle küresel bir bütünlük arz ettiği için mutlak kontrolü çok zor ve hatta imkânsızdır. Bunun dışında tüm teknolojik sistemler gibi internet de düzenleme boşlukları olan ve bu boşluklar dolayısıyla büyük zarar olasılıklarını bünyesinde barındıran bir sistemdir. Bu riskler her geçen gün kendini o kadar derinden hissettirmektedir ki, artık internet sunduğu imkânlardan çok, neden olduğu riskler dolayısıyla bir tedirginlik kaynağı haline gelmiştir. Ancak burada bir modern toplum paradoksu ile karşılaşılmaktadır. Yani günümüzde internet aracılığıyla banka hesapları boşaltılabilmekte, tüm haberleşme olanakları takip edilebilir hale getirilerek mahremiyet olgusu ortadan kaldırılabilmekte, internet aracılığıyla gönderilen casus ve kötücül yazılımlarla tüm bilişim sistemlerinin devre dışı bırakılması, verilerin tahrip edilmesi, sosyal, kültürel, ahlaki değerlerin hiçe sayılması, illegal yapılanmaların yeniden canlanması veya rahatça organize olmaları

mümkün olabilmektedir. Dolayısıyla internet başlı başına bir risk odağı görünümündedir. Ancak buna rağmen internet modern toplumu öylesine sarmalayan bir ağa dönüşmüştür ki, günümüzde internet bunca risklerine karşın vazgeçilmez bir değere sahip olmuştur. Bu ilişki sadece internet için geçerli olmayıp modern toplumun diğer unsurları için de geçerli olmaktadır. Şu halde modern toplumun sistemli bir şekilde devamlılığı risk kaynaklarını ortadan kaldırmakla mümkün olamayacağına göre - örneğin tüm dünyada internet bağlantısını kesmek, nükleer santralleri kapatmak, tıbbi araştırmaları durdurmak...v.b. – yapılması gereken şey toplumu bu riskler karşında korumak için risk kaynaklarını olabildiğince kontrol altında tutmaya çalışmaktır. İşte bu nedenledir ki bilgi toplumu olarak kabul edilen modern toplum aynı zamanda bir risk toplumdur.

Modern toplumda risk kaynaklarını kontrol altında tutmak için kullanılan araçlardan biri de hukuk, bilhassa da ceza hukukudur. Çünkü ceza hukuku, *Prittwitz'in* de ifade ettiği gibi, toplumsal bir alt sistemdir ve toplum işleyişini doğrudan yönlendirir. Bunun temelinde de özgürlük alanlarına doğrudan ve en etkili müdahalenin ceza hukuku düzenlemeleriyle gerçekleşmesi yatmaktadır. İnternetin de önemli bir risk kaynağı olarak hukuksal alana taşınması süreci dikkatle incelenecek olursa özellikle ceza hukukunda gerçekleştirilen düzenlemelerin ağırlığı kendini hissettirmektedir. *Kanaatimizce* interneti modern toplumunun temel dinamiklerinden biri olarak kabul ettikten sonra ceza hukukundaki görünümünü belirlemek için modern ceza hukukunun temel eğilimlerinin göz önünde bulundurulması gerekmektedir. Keza modern ceza hukuku anlayışının, klasik ceza hukuku anlayışına özgü yapılarda bir değişim ve dönüşüm anlamına gelecek olan özellikleri ayrıntılı bir şekilde doktrinden görüşlerle birlikte ortaya konulmuştur. Bu değerlendirmede dikkati çeken husus her geçen gün artış gösteren risklere karşı kendini daha da güçlü hissettiren güvenlik ihtiyacıdır. Bu ihtiyacın karşılanması için özgürlük kullanımından fedakârlık edilmesi, güvenlik içinde özgürlüğün anlamlandırılması olağandır. Özellikle klasik ceza hukuku anlayışının liberal yönelimleri ile birlikte Belirlilik, Kanunilik, Kusur, Ultima Ratio ve Şüpheden Sanık/Özgürlük Yaralanır (*in dubio pro reo / libertate*) prensiplerinin özgürlük ve güvenlik arasında hassas bir denge oluşturduğu ifade edilebilir. Ancak modern ceza hukukunda *Arnold'un* ifadesiyle sarkaç hareketliliği güvenlikten yana gerçekleşmekte, başka bir ifade ile dengenin özgürlük aleyhine güvenlik lehine bozulduğu veya en azından bozulmaya elverişli hale geldiği gözlemlenebilmektedir²²⁰. Bunun en önemli kanıtları arasında *Ünver'in* deyimiyle kanun koyucunun, hukuksal değer korunmasının eleştirisel

²²⁰ **ARNOLD**, Düşman Ceza Hukuku, sh: 537.

fonksiyonunu suç olmaktan çıkartmak olarak değil aksine suç haline getirme şeklinde yorumlaması, *Sieber'in* deyimiyle cezalandırılabilir alanın öne çekilmesi, *Hassamer'in* deyimiyle de soyut tehlike suçlarının artışı gösterilebilir.

Günümüzde bu sürecin en bariz tespit edilebildiği iki alandan bahsedilmektedir. Bunlardan biri terörle mücadele ikinci ise internet suçluluğudur. İnternet ortamında risk barındıran her hareketin potansiyel güvenlik tehdidi olarak algılanması, her geçen gün internet ortamında işlenen hareketlerin suç haline getirilmeye çalışılması veya mevcut düzenlemelerin sınırlarının interneti de kapsayacak şekilde genişletilmesi, internet ortamındaki her türlü içeriğin kontrole tabi tutulmaya çalışılması, kontrol imkanının zorlaştığı noktada doğrudan internet erişiminin engellenmesi gibi örnekler internetin modern toplumunun ve dolayısıyla da modern ceza hukukunun öncelikli risk kaynaklarından biri olduğu tezini güçlendirmektedir. Örneğin Sınır Tanımayan Gazeteciler Örgütü'nün yaptığı araştırmaya göre; Belarus, Çin, İran, Kuzey Kore, Küba, Mısır, Myanmar, Özbekistan, Suriye, Suudi Arabistan, Tunus, Türkmenistan ve Vietnam dünya üzerinde internet kullanımını sınırlayan ve sansüre tabi tutan ülkelerdir²²¹. Bu ülkelerin sosyal, siyasal ve ekonomik alt yapıları dikkatle incelendiğinde internetin ceza hukuku anlamında bir özgürlükler problemi olarak da algılanması gerektiği sonucu ortaya çıkmaktadır. *Kanaatimizce* bu noktada modern ceza hukuku perspektifinden internete bakıldığında iki noktada oluşturulacak değerlendirmenin gerek yasa koyucu gerekse uygulama inisiyatifi açısından temel hareket noktalarını netleştireceği düşünülebilir. Birincisi güvenliğin ancak özgürlükten ödün vererek mi gerçekleşeceği sorunu ikincisi ise her hukuksal değer ihlalini veya ihlal tehlikesini ceza hukuku yaptırımlarına tabi tutmanın yerindeliği sorunudur.

Birinci sorun açısından internetin gerçekten bir takım riskleri bünyesinde barındırması hasebiyle bireysel ve toplumsal güvenliği tehdit edebilecek yönlerinin bulunduğu yukarıda da ifade edilmiştir. Bu da hiç şüphe yok ki bir güvenlik ihtiyacı hissettirmektedir. Ancak güvenliğin tesisi için özgürlüklerin feda edilmesi gerekmez. Bu konuda, tarafımızca da isabetli görülen, *Ökçesiz'in* özgürlük ve güvenlik ilişkisi dikkate değerdir²²². Şöyle ki; *Ökçesiz'e* göre tehlike, “güvenlik” kavramının içeriğinin özgürlüğü yadsıyıcı biçimde

²²¹ İnternete kullanım sınırlaması getiren ülkelerle ilgili ayrıntılı tespit ve değerlendirmeler için bkz. **WIELAND**, Kornad, Meinungsfreiheit im Internet, sh: 15 v.d. (http://www.law.tuwien.ac.at/bakk_arbeit_wieland.pdf, Erişim Tarihi: 10.01.2009, Saat:10:10)

²²² **ÖKÇESİZ**, Hayrettin, “Düşman Ceza Hukuku” Düşüncesinin Eleştirisi, in: KGCHS/8, sh: 557 v.d.

doldurulmasından doğmaktadır. Bu durumda özgürlük de güvenliğin yadsıyıcısı olarak anlaşılmaktadır. Ancak esasında güvenlik ve özgürlük birbirinin yadsıyıcısı değil de destekleyicisi olarak görülse o zaman ceza hukukunca da kullanılabilir bir konsensüse ulaşmak mümkün olabilecektir. Yazar özgürlük ve güvenlik arasındaki bu ilişkiyi şöyle bir tanımla ortaya koymayı tercih etmiştir;

“Güvenlik, sürekli kılınmış eşit ve daha çok özgürlüktür.”²²³

Gerçekten de güvenliğin, özgürlüklerin sürekli kılınmasını mümkün kılacak tedbirler olarak düşünüldüğünde, ancak bir özgürlük kullanımının sürekliliğini engelleyecek nitelikte hukuksal değer ihlallerinin cezai yaptırıma tabi tutulması gerektiği sonucuna ulaşılabilmektedir. Dolayısıyla özgürlük, güvenliğin tehdidi veya yadsıyıcısı değil bilakis kaynağıdır. Bu bağlamda internette var olan risklerin ceza hukuku anlamında bir güvenlik kaygısını ortaya koymasının temel şartı eşit ve daha çok özgürlüğü sürekli kılacak imkanların engellenmesi veya ortadan kaldırılması olmalıdır. Yani güvenliği korumak adına var olan özgürlük alanları da ihlal edilemez. Örneğin, bir paylaşım sitesinde yer alan ve kamu düzeni aleyhine olduğuna kanaat getirilen bir görüntüye erişimi engellemek için ilgili web sitesinin tümünün erişiminin engellenmesi bu anlamda korunmak istenen değerle koruma aracı arasında bir orantısızlık doğurmaktadır. Güvenliğin amacı daha çok özgürlüğe ulaşımı kolaylaştırmak ve bu özgürlükleri sürekli kılmak olmalıdır. Zaten sürekli kılınmış eşit özgürlükler ortamı da, modern ceza hukukunun korumayı hedeflediği toplumsal düzenden başka bir şey değildir.

Bu değerlendirmeye paralel olarak ikinci soruna değinilecek olursa; özellikle görüşleri ortaya konan yazarlardan *Ünver* ve *Prittwitz*'te her hukuksal değer ihlalinin ceza hukuku kapsamına alınmaması gerektiği, aksi taktirde modern dünyada risk kaynaklarının çokluğu nedeniyle her davranışın bir hukuksal değeri ihlal edeceği veya etme tehlikesini barındıracağından hareketle, toplumsal yaşamın dinamik yapısının bundan olumsuz etkileneyeceği açıkça ortaya konulmuştur. Netice itibariyle, her davranışın cezalandırılabilirliğinden bahsetmek ceza hukuku normlarının ultima ratio prensinin, *Hassamer*'in değimiyle, prima ratio'ya dönüşmesi anlamına gelecektir. Her ne kadar modern ceza hukuku eğilimi bu yönde dahi olsa, yukarıda ortaya konan güvenlik kabulü çerçevesinde ancak özgürlüklerin sürekli kılınmasını engelleyecek veya yok edecek ağırlıkta eylemlerin

²²³ ÖKÇESİZ, Eleştiri, sh: 558.

cezai yaptırıma tabi tutulması gerekmektedir. İşte *Ünver* ve *Prittwitz* bu düşüncüyü “*izin verilen risk*” yaklaşımı içerisinde değerlendirmektedirler. İnterneti riskli bir işletme olarak kabul ettiğimiz takdirde, internet ortamında gerçekleştirilecek her türlü eylemin ortaya koyduğu tehlike ve zarar ceza hukuku yaptırımına tabi tutulmaya çalışılırsa, toplumsal dinamizm engellenir ve sağlıklı bir toplumsal gelişimin var oluş imkanları elinden alınır. Netice itibariyle toplumsal yaşamın statik bir hale getirilmemesi ve sürekli gelişiminin sağlanabilmesi için bireylerin kişiliklerini geliştirebilecekleri güvenli bir hareket serbestisine ihtiyaçları vardır. Bu hareket serbestisi güvenlik kaygısıyla ölçüsüz olarak kısıtlanırsa ceza hukukunun tesis etmeyi amaçladığı toplum düzenine ulaşamaz. Burada güvenlik kaygısının ön plana çıkarılmasıyla gerçekleştirilecek özgürlük kısıtlamalarının ölçüsü de, aktüel veya potansiyel ihlal modelinin korunması amaçlanan hukuksal değeri ne ölçüde zedeleyeceği değerlendirilmesidir.

Bu noktada *Ünver* sorunu iki olay grubu içinde değerlendirmektedir²²⁴. Birincisi “*filin toplumsal uygunluğu*” olarak tanımlanan olaylardır. Bu olaylar genellikle önemsiz, az ağırlıkta olan ve suç teşkil eden eylemin neticesinin belirli bir ağırlığa adlandırılabilen önemsiz olaydır. Ancak yazar böyle bir teorik sınıflandırmanın elzem olmadığını, ilgili suç tipine ilişkin normun ratio legisine göre yapılacak bir yorumun aynı neticeyi ortaya koyacağını düşünmektedir²²⁵. İkinci grupta ise gerçek anlamda izin verilen risk teşkil eden olaylar vardır. Bu grupta söz konu eylem ile bir hukuksal değer ihlali gerçekleşmekte ise, eylemin gerçekleştirilmesindeki değer ile ihlal edilen değer karşılaştırılarak aralarında bir tartma işlemi gerçekleştirilip risk teşkil eden eylemin bir özgürlük kullanımı kapsamında değerlendirilip değerlendirilemeyeceğine karar verilecektir²²⁶. Burada önemli olan izin verilen riskin aktüel veya potansiyel olarak ihlale yöneldiği değer karşısında tolere edilebilecek düzeyde kalmasıdır. Şayet ihlal yöneldiği değer korunması anlamında tolere edilebilecek düzeyin üstünde bir netice ortaya koymaktaysa artık burada izin vermeyi meşru kılan bir sebep olmayacaktır.

İşte internet günümüzde her geçen gün daha da risk potansiyeli yüksek bir yapılanma olmaya devam ederken, yeni ihlal modellerine ve imkanlarına elverişli hale gelirken dahi bu risk potansiyelinin veya ihlal modellerinin modern toplumun dinamikleri içerisinde ne ölçüde

²²⁴ ÜNVER, İzin Verilen Risk, sh: 356.

²²⁵ ÜNVER, İzin Verilen Risk, sh: 356.

²²⁶ ÜNVER, İzin Verilen Risk, sh: 357.

tolore edilebilir olduğunun tespiti yapılmak zorundadır. Bu tespit de ceza hukuku perspektifinden temel hak ve özgürlükleri doğru anlama sorumluluğunu da beraberinde getirmektedir. Aksi takdirde her risk veya hareket cezalandırılmaya kalkılırsa ceza hukuku özgürlüklerin güvencesi olmak özelliğini yitire “riskiyle” karşı karşıya kalacaktır. Bu çerçevede *Erman*’ın şu ifadelerini oldukça anlamlı bulmaktayız.

“ *Ceza silahına sarılmanın bir bedeli vardır ve bu bedel de ceza hukuku prensiplerinin bu silahtan medet uman hukuk dalında da egemen olmasını önceden kabul etmektir; hem ceza müeyyidesinden yararlanmak istemek, hem de bu prensiplere ters düşen hükümlere yer vermek hatadır.*”²²⁷

Bu değerlendirmelere Türk Ceza Hukukunun seyri açısından bakılacak olursa, özellikle son 20 senelik sürecin genel olarak bilişim suçları özelinde de internet aracılığıyla işlenebilen suçlar bakımından sorunlu olduğu gözler önüne serilmektedir.

Her şeyden önce Avrupa Konseyi Siber Suç Sözleşmesi, kürselleşen dünyanın en önemli problemlerinden biri olan internet suçluluğu ile mücadele konusunda uluslar üstü standartları belirleme ve uygulamaya yöneltme bakımından çok büyük önemi haizdir. Türkiye bu Sözleşmeye imza koymasına rağmen henüz onaylamamış, dolayısıyla da uygulama alanına yansıtamamıştır. Sözleşmenin henüz onay safhasından geçememiş olmasında, sözleşme hükümleri ve düzeni konusundaki bir takım çekinceler önemli rol oynamaktadır. Bu çekincelerin en önemlisi bu sözleşme ve bu sözleşmeyle birlikte ya da paralelinde kabul edilen ek protokollerin gerektirdiği teknik ve bilgisel alt yapının hazırlanamamış olması ile Avrupa Birliğince belirlenen standartlarının yakalanmasında yaşanan güçlükler gösterilmektedir. Ancak bilişim teknolojilerinin her geçen gün gelişerek yenilenmeleri ve doğalarından kaynaklanan süreçsellikleri dolayısıyla tüm hazırlıkların veya koşulların tamamlanmış olmasını beklemek isabetli görülmemektedir.

Dolayısıyla *kanaatimizce* çok önemli kazanımları beraberinde getirecek bu sözleşmenin gecikmeksizin onaylanması ve aktüel ya da potansiyel eksikliklerin bu süreç içerisinde giderilmesine çalışılması gerekmektedir. Çünkü niteliği itibariyle tüm ülkeler için geçerli bilişim sorunlarını düzenleyen ve hatta yukarıda da ifade edildiği gibi öncelikle Avrupa Birliği üyesi ülkeleri kapsamına rağmen sonrasında Avrupa Birliği üyesi olmayan önemli

²²⁷ ÜNVER, TCK ve Ceza Kanunu Tasarısının Değerlendirilmesi, sh:61’den naklen.

devletlerin de taraf olmayı elzem gördükleri bu sözleşme etrafında dinamik bir de bilişim hukuku hassasiyeti oluşturmuş, ek protokollerle bu hassasiyet desteklenmiş ve hali hazırda üye devletlerin aktif katılımlarıyla yeni sorunlara kolektif bir çözüm getirme bilinci oluşmuştur. Türkiye Cumhuriyeti Devletinin de bu bilince ortak olması sadece normatif bir düzenleme olmanın ötesinde bir hassasiyet odağı oluşturan bu sözleşmenin getireceği dinamizmden faydalanmalıdır.

Bir diğer sancılı süreç ise Kişisel Verilerin Korunması Hakkında Kanun Tasarısının yıllardır kanunlaşmamış olmasıdır. İnternet teknolojisinin gelişim yönü itibariyle en çok koruma görmesi gereken alan kişisel verilere ilişkin alanlardır. Özellikle devletsel uygulamaların dahi artık internet ortamına taşınmaya başlaması, kişisel verilerin güvenliği konusunda ciddi tedbirlerin alınması gerekliliğini bir kez daha gözler önüne sermektedir²²⁸.

²²⁸ “Bir kişinin Türkiye Cumhuriyeti kimlik numarasını kullanarak, lise diploma notundan ne kadar maaş aldığına, su ve telefon borcundan ÖSS’de aldığı puana kadar pek çok bilgiye ulaşılabilir. AA muhabirinin yazılım uzmanlarından aldığı bilgilere göre, “e-devlet” uygulaması sayesinde pek çok bilgiye ulaşılması mümkün hale geldi. Vatandaşların ya da iş dünyasının devlet kurumlarıyla olan ilişki ve işlemlerinin elektronik ortamda gerçekleştirilmesi olarak tanımlanan e-devlet uygulaması, internetin yaşamımızda daha etkin rol üstlenmesiyle kamu hizmetlerini, vatandaşın daha kolay ulaşabileceği bir konuma getirdi. Devleti vatandaşına yakınlaştırmada önemli bir fırsat sunan internet, aynı zamanda kişisel ve özel bilgilere de ulaşılabilmesine olanak sağlıyor. Bir kişinin internet ortamında sadece TC kimlik numarasını kullanarak o kişiyle ilgili yüzlerce bilgiye ulaşılabilir. Örneğin bir kurumun internet sitesinin ilgili kısmına yazılacak TC Kimlik numarası ile o kişinin adı, soyadı, doğum tarihi gibi bilgilere erişilebilir. Doğum tarihi ve ad soyad bilgilerini bir başka kurumun internet sitesinde kullanarak bu kez o kişinin ikametgah adresi elde ediliyor. Adres bilgileriyle bir başka kurumun internet sitesinden nüfus cüzdanı bilgilerine, vergi numarasına, SSK veya Bağ-Kur numarası gibi bilgilere ulaşılabilir. Bunun gibi “zincirleme şeklinde” elde edilen her yeni bilgi ile bir başka kurumun internet sitesinden öteki kişisel bilgilere ulaşılabilir. Elde edilen bu bilgilerle de söz konusu kişinin telefon numarasından, aldığı maaşın miktarına, maaşına ne oranda zam yapıldığına, kaç yıldır çalıştığına, Bağ-Kur maaşını hangi bankanın şubesinden çektiğine, diploma notunun kaç olduğuna, su, elektrik ve telefon faturalarına ve ÖSS’den aldığı puana kadar pek çok bilgiye ulaşmak mümkün hale geliyor. Örneğin Sosyal Güvenlik Kurumu’nun “www.sgk.gov.tr” adresinden, kişinin sosyal güvencesinin olup olmadığı, adı, soyadı, doğum tarihi, kızsık soyadı, işe giriş tarihi, aldığı maaş ve zam oranları, kaç yıldır sigortalı olarak çalıştığı, ilgili aylar içinde kaç gün işe gittiği, ne kadar devamsızlık yaptığı, kaç değişik iş yerinde çalıştığı, prim ödeme gün sayısı, SSK sicil numarası gibi bilgilere kolayca ulaşmak mümkün. Buradan alınan bilgiler ışığında, SSK sicil numarası ya da TC kimlik numarası ile Emlak Konut Gayrimenkul Yatırım Ortaklığı A.Ş.’ye ait “www.keyodemeleri.com” adresine girilerek kişinin ne kadar Konut Edindirme Yardımı aldığı da bulunabilir. Aynı şekilde, TC kimlik numarası kullanılarak Sosyal Sigortalar Kurumunun internet sitesinden anne ve baba adı ile gün ay yıl olarak doğum tarihi bilgileri elde edilebilir. Kişinin anne ve baba adı bilgileri ile Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü’nün internet sitesindeki kimlik numarası sorgulama sayfasından nüfus cüzdanında yer alan aile sıra no, cilt no, birey sıra no, mahalle ve köy bilgilerine de erişilebilir. TC kimlik numarası ile kişinin Bağ-Kur Genel Müdürlüğü’nün web sayfasından Bağ-Kur’lu olup olmadığını da öğrenmek mümkün. Bağ-Kur’lu ise mesleğe kabul tarihi, emekli olup olmadığı, Bağ-Kur’a olan borcu, kaç gün hizmet verdiği, Bağ-Kur aylığını hangi bankanın hangi şubesinden aldığı, en son maaşını hangi tarihte aldığı, mesleğini hangi ilde icra ettiği, vergi numarası, Bağ-Kur sağlık hizmetinden yararlanıp yararlanmadığı, sağlık priminin kesilip kesilmediği de ortaya çıkıyor. Elde edilen bilgilerle Gelir İdaresi Başkanlığı’nın internet sitesinden söz konusu kişinin evinin bulunduğu cadde, sokak, kapı numarası gibi açık adresine ulaşılabilir. Buradaki adres bilgileri kullanılarak ise Türk Telekom’un internet sitesinden kişinin telefon numarası varsa mail adresi, fatura borcu ve faturanın son ödeme tarihi öğrenilebilir. İnternette edinilen bilgilerle, kişinin okul hayatında başarılı olup olmadığı da ortaya çıkıyor. Öğrenci Seçme ve Yerleştirme Merkezinin internet sitesinde TC kimlik numarası girilerek kişinin lise diploma notu, ÖSS’den aldığı puanı, LES ve KPSS öğrenim süresince burs alıp almadığı, mezun olduğu okulu ve bölümü öğrenilebilir. Bazı şehirlerin su ve kanalizasyon idarelerinin internet sitelerinde ise ilgili

Bu kadar önemli ve acil çözüm getirilmesi gereken bir konuda yıllardır bir adım atılmamış olması çok ciddi çelişkileri hissettirmektedir. Çünkü bir taraftan özellikle 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Hakkında Kanun'un yürürlüğe girmesiyle artış gösteren internet erişimlerinin engellenmesi vakalarıyla güvenlik gerekçesiyle sadece bir verinin- ki bu veri görsel ya da işitsel olabilir – erişimini engellemek için tüm bir web sitesini erişilmez kılmak gibi ölçülülüğü tartışmalı uygulamalar gidilirken, diğer taraftan daha çok yasal koruma öngören ve daha ölçülü olacağından hiç şüphe duyulmayacak uygulama ve tedbirlerin konu edildiği bir yasanın gündeme dahi alınmaması ulaşılmak istenen hedef konusunda bir takım yanlışlara sebebiyet vermektedir²²⁹.

Bu noktada 5651 sayılı Kanunda düzenlenen erişimin engellenmesi düzenlemesi üzerinde durmak faydalı olacaktır. her şeyden önce ifade etmek gerekir ki ilgili Kanun md. 8 çerçevesinde iki değişik erişimin engellenmesi uygulamasına rastlanmaktadır. Bunlardan birincisi koruma tedbiri olarak erişimin engellenmesi bir diğeri ise idari yaptırım olarak erişimin engellenmesidir. Bir koruma tedbiri olarak erişimin engellenmesinde öncelikle suç teşkil eden içeriğin md. 8/1-a ve b'de sayılan suçlardan biri olması gerekmektedir. Kanun koyucu burada sınırlı sayıda suç tipinden ibaret olan bir katalog oluşturmuştur. Buna göre erişim engellenmesi kararı verilebilmesi için 5237 sayılı TCK'de düzenlenen intihara yönlendirme, çocukların cinsel istismarı, uyuşturucu ve uyarıcı madde kullanılmasını kolaylaştırma, sağlık için tehlikeli madde temini, müstehcenlik, fuhuş, kumar oynanması için yer ve imkan sağlama suçları ile birlikte 25/7/1951 tarihli ve 5816 sayılı Atatürk Aleyhine İşlenen Suçlar Hakkında Kanunda yer alan suçlar söz konusu olmalıdır. Ancak bir içeriğe

kısımına sadece ad ve soyad yazarak su borcu olup olmadığına, kullanılan su miktarına erişilebiliyor. Yazılım Geliştirme Uzmanı Yusuf Çakır, AA muhabirine yaptığı açıklamada, e-devlet uygulamasını desteklediğini ancak, kişisel ve özel bilgilere bu kadar kolay ulaşılabilmesinin çok sakıncalı olduğunu söyledi. Vatandaşların kişisel bilgilerinin parça parça değişik kurumların internet sitelerinde bulunduğunu anlatan Çakır, bir bilgiye ulaşmaya çalışan kişi, x kurumundan bulamasa da y kurumundan o bilgiyi buluyor. Yani kişinin elimizde sadece birkaç bilgisi varken adı soyadı, yaşı gibi, o bilgilerden yola çıkıp kişinin yüzlerce bilgisine ulaşıyor" diye konuştu. Kişisel bilgilerin kötü niyetli insanlar tarafından farklı amaçlarla kullanılabilmesine işaret eden Çakır, şunları söyledi: "İnternette elde edilen bu bilgilerle sahte nüfus cüzdanı yapılabilir. Bir bankaya telefon açıp 'kredi kartımı kaybettim adresime yeni gönderin' dediğim zaman bana sorulacak sorular belli. Adı, soyadı, annenizin kızlık soyadı, adresi vs. Bu bilgilerin hepsine ulaşabiliyorsunuz. Kötü niyetli olan bir kişi, vatandaşlık numarasını öğrendiği kişilerin tüm özel bilgilerine ulaşabilir ve illegal işlerde kullanılabilir. Bu bilgilerle kredi kartı sahteciliği de dahil birçok yasa dışı iş yapılabilir." Çakır, bütün bu riskleri ortadan kaldırmak için elektronik imza uygulamasına geçilmesi gerektiğini ve kişisel bilgilerin tek bir noktada toplanması gerektiğini belirtti." Kaynak: <http://www.milliyet.com.tr/Ekonomi/SonDakika.aspx?aType=SonDakika&Kategori=ekonomi&ArticleID=1048956&Date=19.01.2009&b=e-devletin zararları&ver=13> (Erişim Tarihi: 19.01.2009, Saat: 13:00)

²²⁹ **DÜLGER**, Murat Volkan, İnternet Erişiminin Engellenmesi, in: İBD, C:2007/4, İstanbul, 2007, sh: 1507.

erişimin engellenmesi için anılan suçların işlenmiş olması gerekmemekte, bu suçların işlendiğine yönelik yeterli şüphenin varlığı aranmaktadır. Bir koruma tedbiri olarak erişimin engellenmesi açısından sadece yeterli şüphenin varlığının aranmasının isabetsiz olduğu ve CMK’de düzenlenen koruma tedbirlerinde olduğu gibi “*kuvvetli şüphe*” kriteri üzerinden hareket etmenin daha isabetli olduğu yönünde doktrinde görüşler mevcuttur²³⁰.

Bir koruma tedbiri olarak erişimin engellenmesi kararının veriliş sürecine bakılacak olursa; 5651 sayılı Kanununun 8. maddesi 2. fıkrasına göre erişimin engellenmesi kararı, soruşturma evresinde hâkim, kovuşturma evresinde ise mahkeme tarafından verilir. Soruşturma evresinde, gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısı tarafından da erişimin engellenmesine karar verilebilir. Maddenin 4. fıkrasına göre ise içeriği birinci fıkrada belirtilen suçları oluşturan yayınların içerik veya yer sağlayıcısının yurt dışında bulunması halinde veya içerik veya yer sağlayıcısı yurt içinde bulunsa bile, içeriği çocukların cinsel istismarı (TCK m. 103 f. 1) ve müstehcenlik (TCK m. 226) suçlarını oluşturan yayınlara ilişkin olarak erişimin engellenmesi kararının re’sen Başkanlık tarafından verileceği hükme bağlanmıştır. Şu hale göre Kanununun 8. maddesinde sayılan katalog suçlardan ötürü, erişimin engellenmesi kararı ya bir hakim veya savcı ya da İletişim Başkanlığı tarafından verilebilmektedir²³¹.

Genel hatlarıyla ikinci erişimi engelleme imkanı olan idari tedbir olarak erişimin engellenmesine dikkat edilecek olursa; içeriği md. 8’de belirtilen suçları oluşturan yayınlarda, içerik sağlayıcıyı veya yer sağlayıcının yurt dışında bulunması halinde veya içerik sağlayıcı veya yer sağlayıcı yurt içinde bulunsa bile, içeriği TCK md. 103/1’de düzenlenen çocukların cinsel istismarı veya md. 226 düzenlenen müstehcenlik suçlarını oluşturan yayınlara ilişkin olarak erişimin engellenmesine Telekomünikasyon İletişim Başkanlığınca re’sen karar verileceği belirtilmiştir.

Kısaca açıklanan bu iki uygulama özellikle son zamanlarda Türkiye’de internet ortamında hareket özgürlüğünü çok ciddi bir biçimde kısıtlayan özellikleriyle ön plana çıkmıştır. Örneğin bir paylaşım sitesine yüklenen ve katalog suçlardan herhangi birini içeren bir yazı veya görüntünün erişimini engellemek için sıklıkla tüm paylaşım sitesinin erişiminin

²³⁰ TAŞKIN, Bilişim Suçları, sh: 156.

²³¹ BOZEL, Savaş, 5651 Sayılı Kanuna İstinaden Bazı İnternet Sitelerine Erişimin Engellenmesi Tedbirlerine Eleştirel Bir Yaklaşım, Kaynak: <http://www.e-akademi.org/makaleler/sbozer-5.htm> (Erişim Tarihi: 22.06.2008, Saat: 13:00)

engellenmesi bir koruma tedbiri olarak erişimin engellenmesi durumunda, söz konusu koruma tedbirinin uygulanması bakımından ölçülülük ilkesinin ciddi bir biçimde ihlal edildiği tartışmalarını gündeme getirmektedir²³². Yine Ceza Muhakemesi Hukuku prensipleri doğrultusunda değerlendirildiğinde, bir koruma tedbirinin ceza gibi uygulanmaması ve bu tedbire başvurulmasındaki temel amacın ceza muhakemesi süreçlerinin sağlıklı işlemesine yardımcı olmak olmalıdır. Ancak yukarıda ayrıntılarıyla aktarıldığı üzere, internetin bir suçluluk alanı olarak konum değiştirmesi ve modern ceza hukuku eğilimlerinin de interneti ciddi bir risk algısıyla çevrelemesi sonucu, internet aracılığıyla kullanılan özgürlüğü ikinci plana atarcasına erişimin engellenmesi kararlarına sıklıkla başvurulması kanaatimizce internetin modern ceza hukuku anlayışı içindeki yerini de kolaylıkla ortaya koyması bakımından önemli bir örnek teşkil etmektedir. Esasında daha ciddi bir sorun erişimin engellenmesi uygulamasının bir koruma tedbiri olarak yargı makamları tarafından kararlaştırılması değil bir idari tedbir olarak Telekomünikasyon İletişim Başkanlığınca re'sen uygulanmasında yatmaktadır. Çünkü bu durumlarda 5651 sayılı Kanun ile yargı işlevi görmeyen bir makama “*yeterli suç şüphesi*” değerlendirmesi yapma yetkisi verilmekte ve şartları oluştuğuna kanaat getirdiği noktada re'sen erişimin engellenmesi kararı verip uygulamaya geçirmektedir. Her ne kadar müdahale alanının bir suç katalogu düzenlemek suretiyle kısıtlanması düşünülse de, internette kullanılan bir özgürlüğün idari bir makamın değerlendirmesine açık bir şekilde risk altına sokulması düşünülemez²³³.

Unutulmamalıdır ki, kanunların anayasal çizgide doldurmadıkları boşluklar hiç şüphe yok ki egemen güç tarafından güvenlik kaygısıyla veya bahanesiyle fiili uygulamalarla doldurulacaktır ki bu uygulamaları önleyecek bir mekanizmanın olmayışı, uygulamaların denetlenmesinde de büyük zorlukların yaşanmasına sebebiyet verecektir.

2.- İNTERNET SUÇLULUĞU VE ULUSLAR ARASI CEZA HUKUKU²³⁴

²³² DÜLGER, İnternet Erişiminin Engellenmesi, sh: 1514.

²³³ BOZEL, Erişimin Engellenmesi, , Kaynak: <http://www.e-akademi.org/makaleler/sbozer-5.htm> (Erişim Tarihi: 22.06.2008, Saat: 13:00)

²³⁴ Bu başlık altında internet ile uluslar arası ceza hukuku ilişkisi incelenirken sadece Uluslar arası Ceza Mahkemesi Roma Statüsü çerçevesinde getirilen düzenlemeler ışığında oluşan uluslar arası ceza hukuku bağlamı kabul edilmiştir. İnternetin uluslar arası anlamda düzenlenmesine ilişkin diğer sözleşmesel ilişkiler (Avrupa Siber Suç Sözleşmesi ve ek protokolleri gibi) ilerleyen bölümlerde ele alınacağı için burada kapsama dahil edilmemiştir.

İnternetin ceza hukuku bakımından özellikli durumlarından biri de uluslar arası hukukla ilişkisidir. Çünkü küresel bir iletişim ve veri aktarım ağı olan internetin yapısı itibariyle ulusal ölçekte getirilen hukuksal düzenlemelerle kontrol altına alınması mümkün değildir. Çünkü bu tarz düzenlemelerle ancak kaynağı söz konusu ülkenin egemenlik sınırları içerisinde bulunan suçlar için fonksiyonel neticeler alınmaktadır. Yalnız artık bu gerçek sadece devletin soruşturma ve kovuşturma organları tarafından değil aynı zamanda söz konusu suçun failleri tarafından da fark edilmiştir. Böyle bir durumun da ceza hukukunun etkinliğini ciddi ölçüde hafifleten bir etkiye sahip olduğunu dile getirmek gerekmektedir. Bu yüzden internet suçluluğu ile mücadele için etkin bir suç politikasının tesisi için mutlak suretle internet ile uluslara arası hukuk ilişkisinin kurulması gerekmektedir. Bu ilişkide de uluslar arası hukuk ayağını hiç şüphe yok ki uluslar arası ceza hukuku oluşturmaktadır. Bu bakımdan öncelikle uluslar arası ceza hukukunun yapısını kısaca ortaya koyduktan sonra bu yapı içerisinde internetin hangi noktaya eklemlendirileceği tartışılmalıdır.

Bir ülke sınırları içerisinde işlenen suçlar çoğu zaman o ülkenin iç hukuk düzenlemeleriyle yaptırım altına alınır. Çünkü ihlal edilen hukuksal değer bakımından o ülkenin egemenlik yetkilerini kullanarak söz konusu ihlalin telafisi için daha “yerel” çözümler getirilir. Ancak öyle suç tipleri vardır ki bunlar hangi ülke sınırları dahilinde işlenirse işlensin, o suç tipi ile ihlal edilen hukuksal değer niteliği itibariyle sadece “yerel” bir yaklaşım hedeflenen neticeyi beraberinde getirmez. Çünkü ihlal edilen hukuksal değer “evrensel” ve bu suçlarla mücadele için sadece ulusal sınırlar dahilinde değil aynı zamanda ulusal sınırların ötesinde de bir takım düzenlemelere gitmek gerekmektedir.²³⁵ İnsanlığa karşı suçlar, barışa karşı suçlar ve savaş suçları bu suçlara en bariz örneklerdir.²³⁶ Bu bağlamda iç hukuk kurallarının yanı sıra uluslar arası kuralları da ihlal eden suçlar söz konusu olduğunda ulusal ceza hukuku ile uluslar arası ceza hukuku bir arada düşünülmesi gerekmektedir. Bu anlamı ile uluslar arası ceza hukuku, ceza kanunlarının uygulanması nedeniyle devletler arasında çıkan ihtilafları ve uluslar arası bazı suçları tespit, bunları önleme, ortadan kaldırma ve bu husustaki yetkileri tayin eden kurallardan meydana gelir.²³⁷

²³⁵ Hukuksal değerler ile ilgili yerel – evrensel tartışması için bkz. 1.1.4.- Küreselleşme ve Ceza Hukuku, sh: 21 v.d.

²³⁶ Bu konuda ayrıntılı bilgi için bkz. http://www.ucmk.org.tr/images/belgeler/ucm_sucun_unsurlari.pdf (Erişim Tarihi: 22.09.2007).

²³⁷ AYDIN, Devrim, Uluslar arası Ceza Hukukunun Gelişimi, in: AÜHFD, C: 51, S:4, Ankara, 2002, sh: 134.

Genel anlamda uluslar arası hukuk yaklaşık 300 yıllık bir geçmişe dayanmasına rağmen uluslar arası ceza hukukuna ilişkin gelişmeler özellikle II. Dünya Savaşı'ndan sonra hareketlilik kazanmıştır. 1948 tarihli Soykırım Sözleşmesi imzalanıncaya kadar ceza hukukunun uluslar arası boyutu, suçluların iadesi ve sığınma konuların ile sınırlıyken, bugün ise uluslar arası ceza hukuku, işlenen bir suç nedeniyle birden çok ülkenin ceza kanunları arasındaki itilafları konu aldığı gibi işlenen bir suçun bütün devletlere zarar vermesini, bir suçun uluslar arası işlenen toplumunun tümü için tehlike oluşturmasını da incelemektedir. Dünyanın gelmiş olduğu konum itibarıyla yukarıda örneklenen ve uluslar arası niteliği kabul edilen suçlar nedeniyle devletlerden ayrı olarak bireylerin de uluslar arası hukukta sorumluluklarını kabul edilmektedir. Özetle 20. yüzyılda yaşanan siyasi ve hukuki gelişmeler sonucunda devletlerin, milletlerin veya bireylerin bazı suçları işlemeleri halinde bu durumu düzenleyecek bir uluslar arası ceza hukuku ortaya çıkmıştır.²³⁸

Bu noktada “uluslar arası suç” kavramının da hangi bağlamda ele alınması gerektiği de açıklığa kavuşturulmalıdır. 17. yüzyıl başlarında devletler hukukunun yaratıcısı olan *Hugo Grotius*, doğal hukuka aykırı hareket eden devlet karşı girişilecek “haklı bir savaş”ın cezalandırma işlevini göreceği fikrini ileri sürerek uluslar arası düzenin ihlalinin müeyyidesini de ortaya koyuyordu. Uluslar arası ceza hukukunun gelişimini sağlayan temel neden, bazı fiillerin işlenmesi durumlarda uluslar arası kamu düzeni, egemen devletlerin kendi aralarında oluşturdukları ve bir arada yaşamalarını sağlayan emredici kurallar bölümüdür. Bu nedenle uluslar arası kamu düzenine aykırı eylemler “uluslar arası suç” niteliğindedir.²³⁹ Uluslar arası hukuk tarafından “suç” olarak kabul edilen fiiller sadece aleyhine işlendikleri devletlerin menfaatlerini değil, bütün uluslararası toplumun menfaatlerini zedeler niteliktedir ve suçtan doğrudan zarar görmemiş olsa bile diğer bütün devletlerin de güvenliklerine yönelik bir tehdittir. Uluslar arası suçlar sadece yönelttikleri ve zarar verdikleri devletin değil, tüm uluslar arası toplumun ve tüm devletlerin güvenliklerini tehlike atan hareketlerdir. Ceza hukuku kavramları kullanılarak bir açıklama yapılacak olursa; uluslar arası nitelikteki suçların ihlal ettiği hukuki değer, uluslar arası toplumunun genel menfaatleri ve uluslar arası düzeni ile ilgili değerlerdir.²⁴⁰

²³⁸ AYDIN, Uluslar arası Ceza Hukuku, sh: 134.

²³⁹ AYDIN, Uluslar arası Ceza Hukuku, sh: 137.

²⁴⁰ “Uluslararası suçlar” kavramı ile uluslararası hukuka aykırı olan ve uluslararası sözleşmelerle kovuşturulması kabul edilen suçlar anlaşılmaktadır. Ancak uluslararası suçlar da kendi içinde iki kategoriye ayrılmaktadır. Birinci kategoriye “uluslararası hukuk suçları”, ikinci kategoriye ise “diğer uluslararası suçlar” oluşturmaktadır. “Uluslararası hukuk suçları” ya da “uluslararası hukuka karşı suçlar” kavramı ile doğrudan

Uluslar arası ceza hukuku bakımından en önemli hukuksal metin olan 18 Temmuz 1998 tarihli Uluslar arası Ceza Mahkemesi Roma Statüsü'nün 5. maddesi Uluslar arası Ceza Mahkemesinin yetkisine giren suçları düzenlemiştir.²⁴¹

Buraya kadar yapılan açıklamalarla uluslar arası ceza hukukunun genel bir görünümü çıkartılmış oldu. Bu görünümü esas alarak interneti ve internetin ceza hukuku yansımalarının uluslara arası ceza hukuku bakımından nasıl yorumlanması gerektiği hususunda her şeyden önce sorunun doğru tespit edilmesi gerekmektedir. Çünkü özellikle son yıllarda internetin iletişim sistemlerinin en esaslı bir parçası durumuna gelmesiyle, uluslar arası suçlar yeni bir boyut kazanmıştır.²⁴² Böylece, internet çerçevesinde işlenen suçlar bağlamında ceza hukukunun devletler hukuku ile yeni bir ilişki ortaya çıkmaktadır. Özellikle internet ortamında işlenen suçların nerede işlendiğinin saptanması yönünden yeni düzenlemelere gereksinim duyulmaktadır.²⁴³ Burada iki boyutlu bir değerlendirme kriteri esas kabul edilmelidir. Birincisi Uluslar arası Ceza Mahkemesi Roma Statüsü'nün 5. maddesinde sayma usulü ile belirlenen suç tiplerinin internet aracılığıyla işlenmesi, ikinci ise

uluslararası hukuka göre cezai sorumluluğu gerektiren fiiller kastedilmektedir. Literatürde uluslararası hukuk suçları olarak soykırım suçu, insanlığa karşı suçlar, savaş suçları ve saldırı savaşı (saldırganlık) suçu olarak dört grup suç kabul edilmektedir. Çekirdek suçlar olarak da adlandırılan bu suçlar, uluslararası toplumun tamamını ilgilendiren en ağır suçlardır. "Diğer uluslararası suçlar" için ise doğrudan uluslararası hukuka göre cezai sorumluluk öngörülmemekte, uluslararası sözleşmelerle devletlere bu fiillerin cezalandırılabilirliğini sağlama yükümlülüğü getirilmektedir. Uluslararası suçları işleyen fail, doğrudan uluslararası hukukun bir ceza normunu ihlal etmekte ve doğrudan uluslararası hukukun ceza normlarına dayanarak cezalandırılması mümkün olmaktadır. Buna karşın diğer uluslararası suçların kovuşturulması ve cezalandırılmasının temelini uluslararası hukuk değil, iç hukuka dahil edilen uluslararası sözleşmeler oluşturmaktadır. Diğer uluslararası suçlara örnek olarak hava ulaşımına karşı suçlar, deniz ulaşımına karşı suçlar, uyuşturucu madde suçlarının belli bazı şekilleri, terör suçları, paralarda sahtecilik, insan ticareti, göçmen kaçakçılığı, işkence, fuhuş amaçlı insan ticareti gibi suçlar gösterilebilir." , TURHAN, Faruk, Yeni Türk Ceza Kanununda Uluslar arası Suçlar, <http://www.ceza-bb.adalet.gov.tr/makale/101.doc> (Erişim Tarihi: 22.09.2007)'den naklen.

²⁴¹ **YILMAZ/ERKEN**, Uluslar arası Ceza Mahkemesi Hakkında, http://www.ucmk.org.tr/index.php?option=com_content&task=view&id=32&Itemid=49 (Erişim Tarihi: 22.09.2007); **ALİBABA**, Arzu, Uluslar arası Ceza Mahkemesinin Kuruluşu, in: AÜHFD, C: 49, S: 1-4, Ankara, 2000, sh: 199 vd.

²⁴² Konuyla ilgili bir örnek vermek gerekirse 2000 yılında bir Fransız derneğinin Fransız Mahkemelerine başvurarak Yahoo'nun Fransa'da filtre edilmesini istemesiyle açılan dava dikkate alınabilir. Davanın sebebi Yahoo'nun açık arttırma sayfalarında bazı kullanıcılar Nazi Savaş hatıra eşyaları satılmasını (savaş madalyaları vs.). Fransız yasalarına böyle bir açık arttırma suç teşkil etmekteydi. Davanın tarafı olan dernek, Yahoo'ya başvurarak bu sayfaların Fransa'ya filtre edilerek sunulmasını istediğinde, Yahoo tarafından kendilerinin Amerikan şirketi olduğunu ve Amerika'dan yayın yaptıklarını, bu bakımdan Fransız yasal düzenlemelerin bu konuya uygulanamayacağını ifade edilmiştir. Bunun üzerine dernek Fransız Mahkemelerinde dava açtı ve Yahoo'nun toptan Fransa'da filtre edilmesini istedi. Mahkeme davayı kabul etmiştir. Bunun üzerine Yahoo geri adım attı ve bu sayfaları Fransız kullanıcılarına sunmamayı kabul etti ve Fransa'da toptan filitri edilmekten kurtuldu. Dava ile ilgili detaylı bilgi için bkz. **NIGGLI**, Irk Ayrımcılığı ve İnternet, sh: 280 vd.

²⁴³ **İÇEL/DONAY**, Ceza Hukuku , sh: 19.

söz konusu suç katalogunda yer almasa dahi internet aracılığıyla işlenen suçların mevcut uluslar arası ceza hukuku sistematigi içinde değerlendirilip değerlendirilemeyeceğidir.

Roma Statüsü'nün 5. maddesinde sayma yoluyla belirtilmiş ve devamı maddelerinde detaylandırılmış suç tiplerinin (Savaş, saldırı, insanlığa karşı ve soykırım suçları) niteliğine bakılacak olursa üç temel kriteri esas aldığı görülmektedir. Bunlar özgürlük, vücut bütünlüğü, insan onurudur. Söz konusu suç katalogunda sıralanmış suçlardan insan onurunun korunmasına yönelik bazı suç tipleri dışında²⁴⁴ diğer suçlar doğrudan internetin araç olarak kullanılması suretiyle işlenmeye elverişli suçlar olarak görünmemektedir. Fakat Roma Statüsü 25. maddenin 3. fıkrasında getirmiş olduğu düzenleme ile internetin uluslar arası suçların işlenmesinde bir araç olarak kullanılmasına ve bu kullanımın cezai yaptırıma tabi tutulmasına zemin hazırlamıştır. Şöyle ki; uluslar arası suçlardan kişisel sorumluluğu düzenleyen 25. maddenin 3 fıkrası anılan Statü gereğince Uluslar arası Ceza Mahkemesinin yargı yetkisine giren bir suçtan dolayı hangi hallerde kişisel ceza sorumluluğuna gidileceğini belirlemiştir.

Bu kriterler nazarı dikkate alındığı zaman Mahkemenin yargı yetkisi dahilindeki suçların teşviki, emri, kışkırtılması, ikna edilmesi gibi unsurlar bakımından günümüzün etkili aracı hiç şüphesiz ki kitle haberleşme araçları ve bilhassa internettir. Çünkü internet, yapısı itibariyle kontrol edilmesi güç bir iletişim imkanı ve yazı, resim ses ve görüntü transferinin mümkün olmasıyla elverişli bir araç olduğu için, bu tarz illegal örgütlenmeler tarafından giriştikleri hukuka aykırı eylemleri yaygınlaştırmak, kişileri bunlara teşvik etmek, kışkırtmak, ikna etmek amacıyla sıklıkla kullanılmaktadır. Bu anlamda internetin bir araç olarak Statü tarafından Mahkemenin yargı yetkisi dahilinde kabul edilen suçların işlenişinde ağırlıklı olarak dolaylı bir etkiye sahip olduğu kabul edilebilir. Burada internet dolaylı bir etkiye sahip olduğu, istisnai durumlar hariç söz konusu suçların doğrudan işlenişinde değil bu suçların işlenişine zemin hazırlanmasında kullanılmasından kaynaklanmaktadır.

Bu açıdan internetin uluslar arası ceza hukukunda nasıl bir görünüme sahip olduğu konusunda durum açık görülmektedir. *Kanaatimizce* esas tartışmalı konu söz konusu suç katalogunda yer almasa dahi internet aracılığıyla işlenen suçların mevcut uluslar arası ceza hukuku sistematigi içinde değerlendirilip değerlendirilmemesi ile ilgilidir. Bu konuda *Hilgendorf*'un yorumu dikkat çekicidir ve kanımca isabetlidir.

²⁴⁴ md. 7/2 – e (İşkence), h (Apartheid), md. 8/2-b/xii (Merhamet gösterilmeyeceğini ilan etme), xiv (Düşman taraf uyruklu kişilerin, mahkemelerdeki hak ve eylemlerinin ortadan kaldırıldığı, askıya alındığı veya kabul edilemez olduğunun ilanı), xxi (İnsan onuruna hakaret eder nitelikte, özellikle aşağılayıcı ve küçük düşürücü hareketler) gibi.

Yazara göre uluslar arası ceza hukukunun gelişmesi internetin uluslar arası ceza hukukunda düzenlenebileceği düşüncesinin imkansız görünmediğini dile getirirken bu tür bir ceza hukukunun nasıl bir içeriğe sahip olabileceği henüz tamamıyla netleştirilememiştir.

“Ceza hukuku, hukuk toplumu tarafından önem atfedilen hukuksal değerlerin korunmasına hizmet etmektedir. Bu tespit, uluslar arası alanda geçerli olması hedeflenen bir ceza hukuku düşüncesine uyarlandığında, hukuksal değerler açısından sadece evrensel olarak tanınmış bulunan değerler gözlenebilmektedir. Bu grup altında ancak insan doğasıyla temellendirilen hukuksal değerler sayılabilir - yaşam hakkı gibi, ki buna vücut bütünlüğü, özgürlük ve şerefın korunması kavramları da bağlanmaktadır -. Bu bağlamda; dünya çapında geçerli olması beklenen internet ceza hukuku, anılan hukuksal değerlerin ihlalini cezalandırmayı amaçlayan birkaç suç tipi belirleyecektir. Bu noktada dikkate şayandır ki; anılan hukuksal değerler, istisnalar hariç (mesela şeref), internet yayıncılığı üzerinden ihlal edilememektedir. Bu sebepten dolayı, internet alanındaki ceza hukuku koruması, gelecekte de ulusal hukuk düzenlerinde büyük oranda yer ayıracaktır. Yeni bir uluslar arası kurumun ihdasına veya bazı internet suç tiplerinin uluslar arası ceza divanının yetki alanına dahil edilmesine bugün için bir gereklilik yoktur. Dünya çapında cezalandırılmasını istediğimiz internet yayınlarını evrensel takip ilkesine dahil etmek yeterli olacaktır.”²⁴⁵

3.- İNTERNET ORTAMINDA İŞLENEN SUÇLARIN SINIFLANDIRMA SORUNU

3.1.- Genel Açıklamalar

İnternet ortamında işlenen suçlar bakımından ilk önemli sorun bu suç tiplerinin sınıflandırılması sorunudur. Her şeyden önce ceza hukukunda suç tiplerinin sınıflandırılması, sağladığı yorum ve kavrama kolaylığının yanından sistemi oluşturan unsurların sistematik bir hiyerarşi veya benzerlik – farklılık ilişkisi içinde gruplandırılıp düzenlenmesi gereğini ifade etmektedir. Böyle bir anlayış karşısında suçların sınıflandırılması gerek bilimsel gerek kanun koyma faaliyetleri tekniği açısından bir zorunluluktur olarak kabul edilebilir. Öyle ki *Ünver* suçların gruplandırılmadan kanunlarda yığın halinde bırakılmaları veya uygun bir

²⁴⁵ HILGENDORF, Yeni Medya Araçları , sh: 287 – 288.

sınıflandırma olmadan ve rasgele düzenlenmelerinin suç teorisinin gereklerine de aykırı düşeceğini savunarak suçların gruplandırmasının önemini şöyle dile getirmiştir²⁴⁶:

“Suçların gruplandırılması sorunu yalnızca elverişsizlik ve yasama tekniği yönünden değil aynı zamanda bilimsel açıdan da önem taşır. Gruplandırma yorum yönünden, yasama tekniği yönünden normun bilimsel açıdan incelenmesi bakımından da gereklidir. Çünkü ceza kanunlarının özel bölümündeki hükümlerin gruplandırılması hükümler arasındaki ilişkiyi benzerlik ve farklılığı saptayıp bilimsel bir çalışmanın yapılabilmesi açısından olduğu kadar çok çeşitli teorik ve pratik yararlar açısından da önemlidir.”

Genel anlamda ceza hukukunda suçların sınıflandırması yapılırken farklı ölçütlerden hareket edilebilmektedir. Örneğin subjektif unsurların esas alındığı bir değerlendirmede suçun kusurluluk unsuru, faili suça iten saik, failin karakteri ya da failin tehlikelilik durumu göz önünde bulundurulabileceği gibi, objektif unsurlara itibar edilerek hareket, netice, tipe uygunluk, hukuksal değer de bir gruplandırma ölçütü olarak tercih edilebilir. Suçların gruplandırılmasında hukuksal değer dışında suçu işleyen kişinin niteliği suçta kullanılan araçlar da dikkate alınan hususlardır. Keza bu ölçütler yanında suçun pasif süjesinin veya suçlar karşılığı kanunlarda öngörülen cezaların suçların işlendikleri zaman da birer gruplandırma ölçütü olarak tavsiye edilmiştir.²⁴⁷

İnternet ortamında işlenen suçların sınıflandırılması ile ilgili değerlendirmeye geçmeden önce bilişim suçları ile ilgili yapılan bazı sınıflandırma örneklerini ortaya koymakta fayda vardır. Çünkü daha önce de dile getirildiği üzere internet bir bilişim sistemi olarak kabul edildiği için bu alanla ilgili ceza hukuku sorunları aynı zamanda bilişim suçları içinde telakki edilmektedir. Başka bir açıdan bakıldığında da bir bilişim sistemi olması ve yapısal olarak bilgisayarlar arası iletişim ağından ibaret olması dolayısıyla “bilişim suçu” ve “bilgisayar suçu” ifadeleriyle anlatılmak istenen suç tipleri bir ölçüde internet ortamında işlenen suçları ilgilendirmektedir. Dolayısıyla bilgisayar suçlarını kapsar nitelikte bilişim suçları için yapılan sınıflandırma girişimlerinde hangi esasların göz önünde bulundurulduğu, internet ortamında işlenebilen suçlara yönelik gerçekleştirilecek sınıflandırma girişimlerinde önem arz etmektedir. Bu değerlendirmeyi yaparken de belirtilen amaca uygun olarak tarihsel gelişim sürecine paralel olarak örneklendirme yapılmaya gayret edilmiştir.

²⁴⁶ ÜNVER, Hukuksal Değer, sh: 798.

²⁴⁷ ÜNVER, Hukuksal Değer, sh: 799.

3.2. - Avrupa Konseyi Siber Suç Sözleşmesine Kadar Yapılan Bilişim Suçlarına İlişkin Sınıflandırma Örnekleri

Bilgisayar ve sistemlerinin ceza hukukunun düzenleme kapsamına girmeye başladığı 80'li yıllarda öncelikle “bilgisayar suçu” kavramının kullanıldığı dikkati çekmektedir. Bu yönde bir tercihin de henüz yeni bir teknoloji olan bilgisayar teknolojisinin sınırlı bir kullanım alanına hitap etmesinden kaynaklandığı söylenebilir. Nitekim bugün bakıldığında, o dönemde yapılan suç tasnifleri de dikkate alınacak olursa teknik alt yapının henüz yeterince çözülememesinden dolayı detaylı ve ceza hukuku tekniği açısından yeterli bir sınıflandırmaya gidilemediği görülmektedir. Örneğin *Sieber* bilgisayar suçu kavramı altında bilgisayar verilerinin değiştirilmesi, veri casusluğu ve program korsanlığını ve bu sahadaki sabotajları, sistemlere yetki dışı girilmesini gibi suç tiplerini belirlemiştir.²⁴⁸

Yine aynı dönemlerde *Pradel – Feuillard*, bilgisayar suçlarını geleneksel suçlar uyarınca veri ve programları suç teşkil edecek şekilde değiştirmek veya üzerinde oynamak, veri ve programları bozmak ve kullanımlarına engel olmak, veri ve bilgisayar sistemlerine izinsiz giriş, bilgisayar sistemlerini izinsiz olarak kullanmak fiilleri olarak belirlemiştir.²⁴⁹

Bequal, yukarıdaki yazarlara oranla farklı bir yaklaşımı yakalamaya çalışmış ve bilgisayar suçlarını hırsızlık, mal edinme, mülkiyete karşı fiiller ve hizmet hırsızlığı olarak dört üst başlık altında incelemekte ve bilgisayar aracılığıyla gerçekleştirilen değişik eylemlerin bu dört ana gruptan bir tanesi içinde değerlendirilebileceğini ifade etmiştir.²⁵⁰

Sarzana da ise bilgisayar suçlarını üç alt kategori içinde ele almıştır. Yazar birinci kategoride bilgisayar aracılığıyla suç failinin bir yarar sağlaması geniş anlamda bile olsa mağdurun bir zarar görmesi amacıyla işlenen fiilleri ele almaktadır. Bunlar içinde bilgisayar, veri, program ve unsurlarına yönelik hırsızlıklar, hizmet hırsızlıkları, maddi yararlaraya yönelik hırsızlıklar, mali suçları değerlendirmektedir. Yazar ikinci kategoride bilgisayarın veya ürünlerinin tamamen veya kısmen tahrip edilmesi, yok edilmesi amacıyla bilgisayarın fiziki varlığına yönelik fiilleri ele almaktadır. Bunlar endüstriyel sabotajlar, siyasi sabotajlar,

²⁴⁸ YAZICIOĞLU, Bilgisayar Suçları, sh: 144'den naklen.

²⁴⁹ YAZICIOĞLU, Bilgisayar Suçları, sh: 144'den naklen.

²⁵⁰ YAZICIOĞLU, Bilgisayar Suçları, sh: 144'den naklen.

vandalizim hareketleridir. Üçüncü kategorideyse, bilgisayar marifetiyle kişilerin veya toplulukların fiziki varlıklarına yönelik fiiller yer almaktadır. Bunlar da yok etme ve tahrip, katliam ve tehditlere ilişkin fiillerdir.²⁵¹

Özellikle 90 yılların başından itibaren Türk hukukçuları da bu yeni alanla ilgilenmeye başlamışlar ve bir takım sınıflandırma girişimlerinde bulunmuşlardır. Örneğin *Dönmezer* bilgisayar suçlarını ya bilgisayar sistemi içinde işlenen suçlar ve bilgisayara karşı işlenen suçlar olarak iki gruba ayırmakta ya da bilgisayar sisteminin bilgi bankalarının, programlarının güvenliğini koruyacak suçlar ve teknik aracın kendisini korumak amacını güden suçlar olarak sınıflandırmaktaydı.²⁵²

Ersoy, 765 sayılı TCK'da 1991 yılında gerçekleşen yenileştirme hareketlerinin bir ürünü olan "bilişim" kavramını esas alarak bu alanda işlenen suçları bilişim sistemleri ile işlenen suçlar, bilişim sistemine karşı suçlar ve bilişim araçlarına karşı işlenen suçlar olmak üzere üç kategori içinde değerlendirmiştir.²⁵³

İnanıcı ise, bilişim suçlarını iki temel ayırım içinde tasarlamıştır. Bunlardan birincisi bilişim sistemine karşı işlenen suçlardır. Buna göre bilişim sisteminin kendisine karşı işlenen suçlar, bilişim sistemindeki program ve verilere karşı işlenen suçlar ve bilgisayar kullanıcılarına karşı işlenen suçlar bu kategori içinde değerlendirilebilmektedir. İkinci grupta ise bilişim sistemi aracılığıyla işlenen suçlar yer almaktadır. Bu grupta da bilgisayar aracılığıyla işlenen ekonomik suçlar, bilgisayar aracılığıyla işlenen sahtecilik suçları, bilgisayar aracılığıyla işlenen ahlaki suçlar ve bilgisayar aracılığıyla işlenen şahsi haklara tecavüz suçları yer almaktadır.²⁵⁴

90'lı yılların ortalarından itibaren bilişim teknolojisinde gerçekleşen hızlı gelişime paralel olarak ceza hukukunda bilişim sistemi ve araçları aracılığıyla işlenen suçlara yönelik daha isabetli ve detaylı değerlendirmeler yapıldığı dikkati çekmektedir. Örneğin *Karagülmez'*

²⁵¹ **YAZICIOĞLU**, *Bilgisayar Suçları*, sh: 145'den naklen.

²⁵² **DÖNMEZER**, *Sulhi, Kişiler ve Mala Karşı Cürümler*, 16. Baskı, İstanbul, 2001, sh: 616.

²⁵³ **ERSOY**, *Bilişim Suçları*, sh: 160.

²⁵⁴ **İNANICI**, Haluk, *Bilişim ve Yazılım Hukuku Uygulama İçinden Görünüşü*, in: *İBD*, C: 70/7-8-9, İstanbul, 1996, sh:514.

in aktardığı ve bilgisayarın suçtaki rolünü esas alan bir görüş bilişim suçlarını üç kategori içinde değerlendirmeyi uygun görmüştür. Buna göre birinci kategoride bilgisayara suçun hedefidir. Bu kategorideki suçlara, bilgisayar donanımı veya yazılımlarının çalınması örnek olarak verilmektedir. İkinci kategoride, bilgisayar suçun konusudur. Burada ise, klasik suçlardaki yol kesme, gasp gibi, bilişim sitesine saldırmak, ona zarar vermek belirtilebilir. Bu kategori son 20-30 yılda teknoloji patlamasının sonucu olarak meydana gelen, virüs saldırıları, “worm”lar, trojen atları, yazılım bombaları, ağ yoklayıcıları, erişimi engelleme veya işletimi bozma gibi bütün suç türlerini kapsar. Bu kategorideki pek çok suçlu mali bir kazanç elde etmekten öte, kötüniyetle veya zarar verme saiki içerisinde hareket ederler. Üçüncü kategoride ise, bilgisayarlar, klasik suçları daha karışık tarzda işlemek için suçta araç olarak kullanılabilirler. Bu klasik suçlar arasında, kimlik hırsızlığı, çocuk pornografisi, telif hakları ihlali, mail veya kablolu bağlantı sahtekarlığı belirtilebilir.²⁵⁵

3.3. - Avrupa Siber Suç Sözleşmesinin Getirdiği Sınıflandırma

Özellikle 2000 yılından itibaren bilişim suçları kategorisinde internet ortamında işlenen suçlar ön plana çıkmaya başlamış ve gerek ulusal gerekse uluslar arası normatif düzenlemelerle internet kullanımı dolayısıyla işlenen suçlarla mücadeleye ağırlık verilmiştir. Daha önce de ifade edildiği üzere bilişim – iletişim teknolojisindeki gelişim süreçsel olarak ele alındığında en basit anlamda bilgisayar kullanımı ve buna bağlı gelişen suç tiplerinin küresel ağ bağlantılarının hayata geçirilmesi ve internetin herkes tarafından kullanılabilir hale getirilmesiyle ortaya çıkan suç tiplerinin sınıflandırılmasının farklılık arz etmesi doğaldır. Keza internete yönelik bu gelişimi ilk somut örneklerini 8 Kasım 2001 tarihinde kabul edilmiş ve 23 Kasım 2001 tarihinde Macaristan’ın Budapeşte kentinde imzaya açılmış olan Avrupa Konseyi Siber Suç Sözleşmesinde görülmektedir.²⁵⁶

²⁵⁵ **KARAGÜLMEZ**, Bilişim Suçları, sh: 53.

²⁵⁶ Avrupa Konseyi Siber Suç Sözleşmesi’nin yapısı, tarihsel arka planı ve kapsamı ile ilgili ayrıntılı bilgi için bkz. **BREYER**, Patrick, Die Cyber- Crime- Konvention des Europarats, in: DuD (Datenschutz und Datensicherheit) 25 (2001) 10, sh: 592 vd. ; **SCHWARZENEGGER**, Christian, Die internationale harmonisierung des Computer- und Internetstrafrecht durch Convention on Cybercrime vom 23 November 2001, in: Strafrech, Strafprozessrecht und Menschenrechte. Festschrift für Stefan Trechsel zum 65. geburstag (Der:Andreas DONATSCH/ Marc FORSTER/ Christian SCHWARZENEGGER), Zürich, sh: 305 vd.; **HILGENDORF**, Eric, Tendenzen und Probleme einer Harmonisierung des Internetstrafrechts auf Europaeischer Ebene, in: Internet- Recht und Strafrecht (Der:Christian SCHWARZENEGGER/ Oliver ARTER /Florian S. JÖRG), Bern, 2005, 257 vd.

Söz konusu Sözleşmede düzenlenen ve cezai yaptırıma tabi tutulan suç tipleri dört ana başlık altında sınıflandırılmıştır. Bunlardan birincisi “Bilgisayar Veri ve Sistemlerinin Gizliliğine, Bütünlüğüne ve Kullanıma Açık Bulundurulmasına Yönelik Suçlar” dır. En genel anlamda bilişim suçları olarak kabul gören bu gruptaki suç teşkil eden eylemler haksız erişim, yasadışı müdahale, verilere müdahale, sistemlere müdahale, cihazları kötüye kullanma yer almaktadır. İkinci grupta ise “Bilgisayarlarla İlişkili Suçlar” düzenlenmektedir. Bu grupta bilgisayar sistemlerini kullanarak gerçekleştirilen klasik suçlar ele alınmaktadır. Bilgisayar aracılığıyla gerçekleştirilen sahtecilik ve dolandırıcılık eylemleri bu grup içinde yer almaktadır. Üçüncü grupta ise “İçerikle İlgili Suçlar” yer almaktadır ki bu grupta çocuk pornografisine ilişkin suçlar düzenlenmektedir. Nihayet dördüncü grupta “Telif Haklarının ve Benzer Hakların İhlaline İlişkin Suçlar” düzenlenmektedir.²⁵⁷ Dikkat edilecek olursa yapılan bu sınıflandırmada, internet kullanımının artışıyla birlikte en çok işlenen filler müeyyide altına alınmıştır. Bankaların internet üzerinden verdikleri hizmetlerin sabote edilmesi ve haksız kazan elde edilmesi, internet aracılığıyla gizli bilgilere haksız erişim, yasa dışı müdahaleler, sahtecilik, internette film, müzik ve benzeri telif hakkını haiz eserlerin bu hakları zedeleyici tarzda indirilmesi (download), çocuk pornografisinin internet aracılığıyla yaygınlık kazanması, hukuk düzenine aykırı içerikte yayınların yapılması ve insanların suça sevk edilmeleri gibi durumlarla ulusal ölçekte mücadelenin yetersiz kaldığı düşüncesiyle hazırlanan bu Sözleşme artık internetin bilişim suçları bakımından temel unsur olarak görülmesinde önemli bir rol oynamıştır.²⁵⁸

3.4.- *İnternet Özelinde Yapılan Sınıflandırma Örnekleri*

Avrupa Konseyi Siber Suç Sözleşmesinden sonra bilişim ve iletişim teknolojilerindeki gelişim yönü artık internet merkezli bir seyir izlediğinden dolayı bu noktadan itibaren de internetin ön plana çıkarıldığı ve ceza hukukunun bir yan alanı olarak “İnternet Ceza Hukuku (*Internetstrafrecht*) ” tartışmalarının başlatıldığı bir dönemde internetin esas alındığı suç tasniflerine rastlanmaktadır²⁵⁹. Bu sınıflandırmalara birkaç örnek vermek gerekirse;

²⁵⁷ Avrupa Konseyi Siber Suç Sözleşmesindeki maddi ceza hukukuna ilişkin düzenlemenin ayrıntıları için bkz. **HELVACIOĞLU**, Avrupa Konseyi Siber Suç Sözleşmesi, sh: 277 v.d.

²⁵⁸ **HILGENDORF/VALERIUS/FRANK**, Computer- und Internetstrafrecht, sh:29.

²⁵⁹ “İnternet Ceza Hukuku”nun, ceza hukukunun bir alt disiplini olup olmadığına ilişkin için bkz. **HEINRICH**, Bernd, Aktuelle Probleme des Internetstrafrechts, Kaynak: <http://www.humboldt-forum-recht.de/deutsch/11-2006/seite1.html> (Erişim Tarihi: 18.02.2008, Saat: 09:40).

Malek, ceza hukuku uygulamasında yeni bir fenomen olarak kabul ettiği İnternet Ceza Hukukunu kapsamlı bir biçimde genel ve özel hükümler bakımından önemli tartışmalarla ortaya koyarken suç tipleri bakımından Alman Ceza Hukukunun normatif düzenlemelerini esas alarak dörtlü bir ayrımı kabul etmiştir.²⁶⁰ Birinci kategoride ekonomik bağlamda gerçekleştirilen suç tiplerini almıştır. Bunlara örnek olarak veri casusluğu (§ 202a), verilerin değiştirilmesi (§ 303a), bilgisayar sabotajı (§303b), delil değerini haiz verilerin üzerinde sahtecilik (§ 269), bilgisayar dolandırıcılığı (§ 263a), dolandırıcılık (§ 263), şantaj (§ 253), bir bahis oyununun izinsiz düzenlenmesi (§ 284) olarak belirtilmiştir. İkinci kategoride ise fikri haklara ilişkin suç tipleri yer almaktadır. Bunlara da örnek olarak Fikri Haklar Kanununun (*UrhG*) telif hakları bakımından korumaya alınmış değerlere karşı suçları kapsayan § 106, 107,108 ve 108a hükümlerini göstermiştir. Üçüncü kategoride kişi haklarına ve mahremiyetine karşı işlenen suçları ele alan *Malek* bu kategori içinde kişisel ve ticari açıdan giz alanı oluşturan verilere karşı işlenen suçları düzenleyen § 203 ve § 204 ile yine özellikle kişisel mahremiyet alanının resim alınmak ve bunları yaymak suretiyle ihlal edilmesine yönelik § 201a hükmünü esas kabul etmiştir. Nihayet dördüncü kategoride açıklama ve yayma suçları olarak belirlediği pornografik yayınların yayılması ve muhafazası (§ 184), şerefe karşı işlenen suçlar (§ 185 vd.), demokratik hukuk devleti ve kamu düzeni aleyhine işlenen suçlar olarak belirlemiştir.²⁶¹

Rüther ise internet ortamında işlenen suçları “Dar Anlamda İnternet Suçları” ve “Geniş Anlamda İnternet Suçları” olmak üzere iki başlık altında toplamaktadır. *Rüther*’e göre dar anlamda internet suçları, internetin ve dolayısıyla bilgisayarın bir “eylem hedefi” kabul edildiği suçlardır. Bu suçlara örnek olarak bir sisteme yetkisiz erişim, sistemi engellemeye, bozmaya, veri değiştirme veya yok etme vb. amaçlarla gerçekleştirilen Hacking, Cracking, Domain – Hijacking gibi eylemlerin vücut verdiği suç tipleri gösterilebilir. Geniş anlamda internet suçlarının sınıflandırılmasında da yine internetin ve dolayısıyla bilgisayarın hangi tarzda ele alındığı önem arz etmektedir. Bu sınıflandırmada ise internet ve bilgisayar dar anlamda internet suçlarının aksine bir eylem hedefi değil bir eylem aracı olarak kabul edilmektedir. İnternetin bir araç olarak kullanıldığı suç tiplerine örnek olarak da klasik mal varlığı suçlarını – örneğin dolandırıcılık – gösterilmektedir.²⁶²

²⁶⁰ MALEK, Klaus, Strafsachen im Internet, Heidelberg, 2005, sh: 42 vd.

²⁶¹ Özel olarak belirtilmeyen durumlarda tüm paragraflar Alman Ceza Kanuna aittir.

²⁶² RÜTHER, Werner, Phänomene der Internetdelinquenz, Kaynak: www.cyber-crime.info/medien-material/internetdelinquenz/ (Erişim Tarihi: 08.11.2007, Saat: 11:16).

Rüther'in sınıflandırma çabalarına benzer bir yaklaşım da *Schreiber*'de görülmektedir. *Schreiber* de internette işlenen suçları iki kategori altında toplamaktadır. Birinci kategoriye "dar anlamda internet suçları" olarak kabul eden yazar bu suç tipleri için Hacking, Cracking, Denial of Service Attacken (DOS), bilgisayar virüsleri vb. şekillerde işlenen ve İsviçre Ceza Kanunu § 143, 143 (bis), 144 (bis) de düzenlenen suç tiplerini örnek olarak göstermiştir. Yazar bu kategoriye belirlerken temel hareket noktasını bir ağ bağlantısının varlığının şart olup olmamasına göre tespit etmiştir. Buna göre dar anlamda internet suçları için bir ağ bağlantısının varlığı bir ön kabul olarak kendini göstermektedir. İkinci sınıf internet suçlarında ise *Schreiber* işlenmeleri için mutlak suretle bir ağ bağlantısına ihtiyaç duyulmayan suç tiplerini kastetmektedir. Bu suç tiplerinde internetin daha çok salt bir araç olarak kullanılması durumu söz konusudur. Bir başka deyişle bu suçların işlenmeleri için internet olmazsa olmaz bir koşul değildir. Bu kategorideki suç tiplerine örnek olarak da dolandırıcılık, fikri hakların ihlali, ırk ayrımcılığı ve çocuk pornografisi gösterilebilir.²⁶³

Bunun dışında *Kronig/ Bollmann* da, internet servis sağlayıcısının konumu ve bu konumlarından kaynaklanan ceza sorumlulukları esastan hareket ederek internetin salt veri transferine mi hizmet ettiği yoksa cezalandırılabilir içeriklerin belli bir süre dahilinde edinilebilmesine olanak tanıyan bir medya aracı mı olduğu kriterleri temelinden bir sınıflandırma yapmışlardır. Buna göre birinci gruptaki suç tipleri internetin veri kayıtları veya transferleri esnasında veya bunlar üzerinde kısa süreli müdahalelerle işlenmektedir. Bunlara örnek olarak²⁶⁴ bir edimin hile ile temini (§ 150/3), fikri hak ihlalleri, Talih Oyunları Kanununun ihlali, üretim ve işletme sırlarının aleyhine işlenen suçlar (§ 162), para sahteciliği (§ 305 bis) verilebilir. İkinci grup suç tipinde ise belli bir sürekliliğin ve erişilebilirliğin gerektiği kabul edilmektedir. Bu anlamda şiddet görüntüleri (§ 135), bir internet sitesindeki yanıltıcı içerik ile dolandırıcılık (§ 148), pornografi (§ 197) ve ırk ayrımcılığı (§ 261 bis) bu kategoride gösterilebilecek suç tiplerinden sayılmaktadır.

Boese, internette içerik suçları olarak nitelendirilebilecek suç tiplerini esas alarak bu tarz suçları iletişim suçları (*Kommunikationsdelikte*) olarak değerlendirmiş ve iki temel

²⁶³ **SCHREIBER**, Wolfgang, *Phänomenologie und Lagebilder der Internetkriminalität*, Vortragmanuskript, Europäische Polizeiakademie, **CEPOL**- Seminar, Rechtsprobleme im Zusammenhang mit der Internet, Münster, 2001, sh:

²⁶⁴ Bu grupta örnek olarak verilen tüm suç tipleri İsviçre Ceza Kanunu hükümlerinde düzenlenen suç tipleridir.

ayırma tabi tutmuştur. Bunlardan birincisi yayma suçlarıdır²⁶⁵. Bu suç tipleri açısından yazar, hukuka aykırı içeriğe sahip olan verilerin internette ulaşılabilir kılınması, transferinin mümkün hale getirilmesi, yayılması gibi fiilleri esas kabul etmektedir. Buna göre Alman Ceza Kanununun §§ 86, 86a./1-1, 109d, 130/ 2- 1, 130a/ 1 ve 2, 131/ 1, 184/ 1 ve 3, 186/ 2, 187/ 2 düzenlenen suç tiplerini yayma suçlarına örnek olarak göstermektedir. İkinci kategori ise açıklama suçlarıdır.²⁶⁶ Açıklama suçlarında ise hukuka aykırı bir içeriğin diğer kişiler tarafından da öğrenilebilecek, edinilebilecek tarzda aktarılması, açıklanması temel hareket noktasını teşkil etmektedir. Buna göre de Alman Ceza Kanunu §§ 90, 90a, 103, 111, 126, 130/1 ve 2, 140/1- 2, 185, 186/ 1, 187/1 örnek olarak gösterilmektedir.

Vassilaki de internetin hangi fillerle kötüye kullanıldığı konusunda bir sınıflandırmaya gitmiş ve ikili bir ayırım esasını kabul etmiştir. Bunlardan birincisi hukuka aykırı içeriklerin yayılmasıyla bağlantılı suçlardır. Bunları da cinsel bütünlüğe karşı işlenen suçlar - ki bu kategori içinde çocuk pornografisi, kişilerin cinsel mahremiyetlerini yazı, resim, görüntü ve sair veri kaynaklarıyla ifşa etmeye yönelik eylemler bulunmaktadır -, kamu düzeni aleyhine işlenen suçlar ve bilgilerin birbirlerine göstergelerle erişilecek birimler şeklinde sunulduğu metinlerin manipüle edilmesi olarak üç alt başlık altında toplamıştır. İkinci kategoride ise üçüncü kişilerin enformasyon üzerindeki haklarının ihlal edildiği suçları ele almaktadır. Yazar yine bu suçları da fikri haklara ve veri muhafazası hukukuna ilişkin mevzuatın ihlali olmak üzere iki alt başlık altında incelemiştir.²⁶⁷

Nihayet özellikle internet ortamında işlenen suçlara ilişkin olarak Türkiye’de yapılan sınıflandırmalara örnek olarak 5237 sayılı TCK’yi esas alarak bir ayırımına giden *Yazıcıoğlu*, internet özelinde bir ayırım yapmaktan ziyade internet ortamında işlenen suçları genel anlamda bilişim suçlarını içerisinde eritmiştir. *Yazıcıoğlu*’na göre Bilişim suçlarını iki temel ayırım içinde düşünmek mümkündür. Bu suçlar bilişim alanının doğurduğu yeni hukukî yararlar karşı gerçekleştirilen «dar anlamda bilişim suçları» ve klâsik suçların bilişim

²⁶⁵ **BOESE**, Oliver, Strafrechtliche Verantwortlichkeit für Verweisungen durch Links im Internet, sh: 111 v.d , Kaynak: <http://deposit.ddb.de/cgi-bin/dokserv?idn=963762524> (Erişim Tarihi: 08.11.2007, Saat: 14:10)

²⁶⁶ **BOESE**, Oliver, Strafrechtliche Verantwortlichkeit, sh: 118 vd.

²⁶⁷ **VASSILAKI**, E. Irini, Materielles Strafrecht, Strafprozessrecht, Rechtsinformatik und Informationsgesellschaft, Freundesgabe Büllersbach, 2002, sh: 348 vd. (Kaynak: http://www.alfred-buellesbach.de/PDF/33_Vassilaki_Materielles.pdf, Erişim Tarihi: 14.10.2007, Saat: 18:50)

olanakları marifetiyle gerçekleştirilmesi olarak karşımıza çıkan «geniş anlamda bilişim suçları»dır.²⁶⁸

Gerçek bilişim suçları olarak adlandırılan birinci suç grubu da, “bilişim sistemlerine izinsiz girilmesi” (md. 243), “bilişim sistemlerindeki verilere müdahalelerde bulunulması” (md. 244), “bilişim sistemleri marifetiyle haksız menfaat temini” (md. 244/4) gibi bilişim sistemlerinin özelliğinden kaynaklanan ve yeni hukuksal değerle bağlamında gerçekleştirilen doğrudan bilişim suçları ya da dar anlamda bilişim suçları şeklinde adlandırılan gerçek bilişim suçları ve bilişim teknolojilerinin getirdiği imkânlar dolayısıyla ortaya çıkan “haberleşmenin gizliliğini ihlâl” (md. 132), “haberleşmenin engellenmesi” (md. 124), “eğitim ve öğretimin engellenmesi” (md.112), “kamu kurumu veya kamu kurumu niteliğindeki meslek kuruluşlarının faaliyetlerinin engellenmesi” (md. 113), gibi dolayısıyla bilişim suçları diye de ikiye ayrılmaktadır. Bununla birlikte “hakaret ve sövme” (md. 125), “müstehcenlik” (md. 226), “kumar oynanması için yer ve imkân sağlanması” (md. 228) “suç işlemeye tahrik” (md. 214) gibi klâsik nitelikli suçların bilişim teknolojileri marifetiyle işleyebilmesi de mümkündür. Hırsızlık ve Dolandırıcılık suç tipleri bakımından da, bu suçların bilişim sistemleri kullanmak suretiyle işlenmesi de ağırlaştırıcı neden olarak düzenlenmiştir.

Başka bir sınıflandırma örneği bağlamında *Sınar* ele alındığında ise, internet ortamında ortaya çıkabilecek eylemlerine ilişkin olarak ikili bir ayrımı esas aldığı görmek mümkündür. Bunlar internet aracılığıyla işlenen eylemler ve internete özgü eylemlerdir.²⁶⁹ Yazara göre internetin ortaya çıkışı ve yaygınlaşması, geleneksel olarak ifade edilen toplum hayatında geçmişten beri var olan ve hukuk düzeni tarafından da suç olarak tanımlanarak yaptırım altına alınan eylemlerin hayata geçirilebileceği yeni bir fırsat alanının doğmasına neden olmuştur. Nitekim evrensel ölçekte hemen her hukuk düzeni tarafından tanımlanmış bulunan klasik suç tipleri yani hırsızlık, sahtecilik, çocukların müstehcen yayımlarda kullanılması, hakaret, suçlunun övülmesi, suç işlemeye tahrik, devlet güçlerine karşı tahkir iftira gibi eylemler internet ortamında işlendiği takdirde internet aracılığıyla işlenen suçlar kategorisi oluşmuş olacaktır. İnternete özgü eylemler başlığı altında yer alan eylemler ise, internet aracılığıyla gerçekleştirilen eylemlerden farklı olarak doğrudan internetin işleyişi ve internet yayıncılığı ile ilgilidir. Bu kapsamda internetteki bir web sitesini kırmak veya tahrif etmek, interneti

²⁶⁸ **YAZICIOĞLU**, Yeni Türk Ceza Kanununun Bilişim Suçları, sh: 396 vd.; Aynı sınıflandırma örneğinin 765 sayılı TCK’ye uyarlanmış hali için bkz. **YAZICIOĞLU**, Bilgisayar Ağları Marifetiyle , sh: 36 vd.

²⁶⁹ **SINAR**, İnternet, sh: 78.

kullanarak bir başkasına ait sisteme yetkisiz olarak girmek, elektronik posta sistemlerini çeşitli amaçlar için kullanarak kişileri rahatsız etmek ve zarar uğratmak gibi eylemler internete özgü eylemler olarak gösterilebilirler.²⁷⁰

3.5.- Değerlendirme

Bir suçluluk alanında birden fazla suçun yer aldığı durumlarda, bu suçların belli kıstaslar esas alınmak suretiyle sınıflandırmaya tabi tutulması özellikle suç tipinin tespitinde sistematik düşünmeyi elverişli kılmaktadır. Özellikle internet ortamında işlenen suçlarda söz konusu olduğu gibi, karmaşık yapıları eylemlerin kategorize edilmesi noktasında bu tür sınıflandırmaların büyük önemi vardır. Çünkü bir suçluluk alanında sınıflandırılan suç tipleri arasında sistematik bir ilişki kurulurken her bir sınıflandırma içinde konumlandırılan suç tipleri arasında da sistematik bir bağ kurulmaktadır. Başka bir anlatımla, örneğin internet ortamında işlenen suçlar, müdahale suçları ve içerik suçları olarak sınıflandırıldıktan sonra her bir sınıflandırma içinde yer alan tek tek suçlar da belli noktalarda ortak bir takım özellikleri barındırmaktadırlar ve bu özellikler o bağlamda değerlendirilecek suçlar için sistematik yorumu mümkün hale getirmektedir. Bu bağlamda internet ortamında işlenen suçları sınıflandırmaya tabi tutmanın gerektiği kanaatindeyiz.

Yukarıda üç dönem itibariyle ortaya konulan sınıflandırma çabaları dikkatle incelenecek olursa, özellikle sınıflandırma ölçütleri anlamında tek bir tercihin yapılmadığı dolayısıyla karma bir bakış açısının yansıtılmaya çalışıldığı gözlemlenmektedir. Yani ölçüt olarak sadece korunması amaçlanan hukuksal değere, suç teşkil eden harekete, neticeye, suçun konusuna göre bir sınıflandırma yapılmamıştır. Bunun da internetin kendine özgü yapısından kaynaklandığı düşüncesindeyiz. Çünkü internet her geçen gün gelişen ve çeşitlenen bir yapıya sahiptir. Dolayısıyla getirilecek sınıflandırma ölçütlerinin bu gelişimle aynı paralelde olması gerekmektedir. Aksi takdirde bir çatışmadan bahsetmek kaçınılmazdır. Bu noktada önemli bir hususun altını çizmek gerekmektedir. İnternet ortamında işlenen suçları “internet aracılığıyla işlenen suçlar – internete özgü suçlar” olarak bir ayrıma tutmanın yukarıda vurgulanan bakış açısıyla isabetli bir tercih olmadığı görülmektedir. Çünkü internetin tarihsel gelişim süreci dikkate alındığında, çok kısa süreler içinde internete özgü kabul edilen bir hareket özgünlüğünü yitirebilmekte ve diğer bilişim sistemleri ile de gerçekleştirilebilmektedir. Gözden ırak tutulmaması gereken nokta, internetin bir bilişim

²⁷⁰ SINAR, İnternet, sh: 81.

sistemi olmasıdır. Genelde bilişim sistemleri için kullanılan “Bilişim Sistemine Özgü Suçlar – Bilişim Sistemi Aracılığıyla İşlenen Suçlar” ayrımını doğrudan internete uygulamak bilişim sistemi – internet ilişkisinin yanlış yorumlandığı izlenimi vermektedir. Bilişim sistemi ifadesiyle, interneti de kapsar nitelikte üst bir yapı kastedilmektedir. Bu anlamda bir hareketin bilişim sistemine özgü olup olmadığı söylenebilir. Çünkü bilişim sisteminin, bu kapsam dahilinde yer alan bütün alt sistemlere teşmil eden temel bir takım özellikleri vardır. Ancak interneti bu genişlikte algılamamak gerektiği düşüncesindeyiz. Bu nedenle bundan sonraki açıklamalarda da interneti suçta bir araç olarak kabul ederek “internet aracılığıyla işlenen suçlar” üst başlığı kapsamında ortaya konulacaktır.

Yapılan sınıflandırma örnekleri göz önünde bulundurulduğunda internet ortamında işlenebilen suçlar bakımından en fonksiyonel sınıflandırma sisteminin internet ortamında işlenen içerik ve müdahale suçları ayrımına dayanan sistem olabileceği kanaatindeyiz. Zira teknik olarak internetin yaşadığı gelişim süreci bakımından interneti sınırlayan ve gelecekteki olası gelişmeleri göz önünde bulundurmadan dar anlamda bilişim suçları ve geniş anlamda bilişim suçları şeklindeki bir ayırım genel geçer olma özelliğinden uzak olacaktır. Ayrıca internetin toplumsal yaşamda kullanılma alanının genişlemesi ve çeşitlenmesiyle bugün internet aracılığıyla işlenemeyecek bir suçun ileride bu kategoriye aktarılması durumunda karışıklıkların doğması muhtemeldir. Bundan dolayı internet ortamında işlenebilen suçların içerik suçları ve müdahale suçları olarak belirlemek, bu yönde yaşanacak karışıklığı da önleyebilir bir nitelik kazanmaktadır.

İçerik suçu tanımlamasıyla, internet ortamında herhangi bir içeriğin açıklanması veya yayılması suretiyle oluşabilecek suçlar ifade edilmeye çalışılırken, müdahale suçu tanımlamasıyla internet ortamında herhangi bir içerikle bağlantısı olmaksızın, teknik imkanlar kullanılmak suretiyle, bir sisteme girme, sisteme zarar verme, manipüle etme, bu ve buna benzer eylemlerle kendine menfaat sağlama gibi hareketleri içeren suç tipleri işaret edilmektedir. Burada “müdahale” dar olarak değil geniş anlamıyla ele almak gerekir. Dikkat edilirse burada tercih edilen ayırım kriterleri internetin genel fonksiyonlarına kapsamlı bir bakış niteliğindedir. Dolayısıyla internet ortamında işlenebilen bir suç incelendiğinde, onun dar yada geniş anlamda bir bilişim suçu olup olmadığına bakılmaksızın yapı itibarıyla bir içerikle mi yoksa bir müdahaleyle mi ilgili olup olmadığına bakmak yeterli olacaktır.

İKİNCİ BÖLÜM

SUÇ GENEL TEORİSİ ÇERÇEVESİNDE İNTERNET ORTAMINDA İŞLENEN SUÇLARA İLİŞKİN YAPISAL DEĞERLENDİRİLMELER

1. – 5237 SAYILI TCK MD. 6/1-G HÜKMÜNCE BİR KİTLE İLETİŞİM ARACI OLARAK İNTERNET

1.1.- Genel Açıklamalar

5237 sayılı TCK md. 6’da, kanunda yer alan düzenlemelerde önem arz eden belli başlı kavramlar tanımlanmıştır. Söz konusu maddenin g bendinde kanunda geçen *basın- yayın yoluyla* ifadesinin *her türlü yazılı, görsel, işitsel ve elektronik kitle iletişim aracıyla yapılan yayınlar* anlamına geldiği açık bir şekilde ortaya konulmuştur. Bu tanımla birlikte modern zamanların en çok kullanılan ve en etkili iletişim aracı olan internetin, 5237 sayılı TCK sistematüğinde bir basın – yayın aracı olarak değerlendirilip değerlendirilemeyeceği gündeme gelmektedir. Bu bağlamda internet özelinde bir değerlendirmeye girmeden önce kanun koyucunun tercihi doğrultusunda basın- yayın aracı olmanın temel ölçütünü teşkil eden “*kitle iletişimini mümkün kılma*” üzerinde durmak isabetli olacaktır. Çünkü internetin milyonlarca bilgisayarı birbirine bağlan bir ağ olarak kabul edilmesi, milyonlarca bilgisayar kullanıcısının birbirleriyle “*kitlesel iletişim*” halinde olmalarını zorunlu kılmaz. Pekâlâ, internet ortamında kişiler birbirleriyle özel iletişim kanallarını, örneğin e- posta veya MSN gibi eş zamanlı mesajlaşma programlarını tercih etmek suretiyle “*bireysel iletişim*” kurmayı da tercih edebilirler.²⁷¹ Fakat gün geçtikçe gelişen internet teknolojisinin bugün gelmiş olduğu nokta itibariyle kurulan iletişimin bireysel mi yoksa kitlesel mi olduğu bu kadar net bir biçimde ayrıt edilemeyebilmektedir. Dolayısıyla teorik anlamda “*kitle iletişimin*” veya başka bir kullanımla “*kitle haberleşmenin*” temel yapısı ortaya konularak, internetin hangi durumlarda 5237 sayılı TCK md. 6/1-g çerçevesinde bir basın – yayın aracı olduğunun tespiti daha sağlıklı olacaktır.

Her şeyden önce haberleşmenin/iletişimin ne olduğu ve nasıl kurulduğu üzerinde kısaca durmak gerekmektedir. Haberleşme, *İçel/ Ünver’in* de isabetle vurguladığı üzere, bilgi,

²⁷¹ DÜLGER, İnternet Erişiminin Engellenmesi, sh: 1496 – 1497.

düşünce veya tutumların ortak semboller sistemi aracılığıyla kişiler veya gruplar arasında değiş tokuş edildiği bir süreçtir²⁷². Bu tanımdan hareketle haberleşmenin unsurları ortaya konulacak olursa; haberleşmenin öncelikle bir değiş tokuş süreci olduğu noktasından başlanmalıdır. Çünkü böyle bir sürecin varlığı bir noktasiyla taraflar arsında bir ilişkinin varlığını ön kabul olarak belirler ki, netice itibariyle ulaşılmak istenen amaç da taraflar arasında sağlıklı bir ilişkidir. Bu bağlamda söz konusu değiş tokuşun süjesi olarak taraflara ihtiyaç duyulmaktadır. Haberleşmenin tarafları kaynak ve hedef olarak iki kategori içinde değerlendirilmektedir. Kaynak, bir değiş tokuş süreci olarak haberleşmenin içeriğini karşı tarafa yönlendiren, hedef ise bu objenin yönlendirildiği kişidir²⁷³. Haberleşmede kaynak ve hedef sayısal anlamda tekliği veya çokluğu konusunda belli bir sınırlandırılmaya gidilmemiştir. Ancak kaynak ve hedefin sayısal pozisyonuna göre kurulan haberleşme sürecinin niteliği (bireysel – kitlesel) değişiklik arz etmektedir. Son olarak da, kaynak ile hedef arasında kurulan süreçte değiş tokuşu kabil bir içeriğin bulunması gerekmektedir. Tanıma geri dönülecek olursa bu içerik bir bilgi, bir düşünce, bir duygu, bir tutum olabilir. Önemli olan bu içeriğin hedef tarafından algılanabilir formatta iletilmesidir. Aksi takdirde kurulan ilişki amaca uygunluk bakımından bir haberleşme sürecine vücut vermez, basit bir iletim olmakla kalır²⁷⁴.

Bu temel yapı üzerinde *Schurmann*, teknik olarak haberleşmeyi sırasıyla “Kaynak → Kodlayıcı → İşaret → Kod Açıcı → Hedef (=Kitle)” sürecinin neticesinden ibaret görmektedir. Kaynak, hedef ve işaret unsurları üzerinde yukarıda durulmuştur. Bunlara ek olarak bu süreçsel dizgede kodlayıcı ve kod açıcıyla karşılaşmaktadır. Bunlar da bir haberleşmenin sağlıklı ve amaca uygun kurulabilmesi için kaynak ve hedef arasındaki ortak alanın oluştuğu araçlardır. Bu ortak alanlara örnek olarak konuşma dilini vücut dilini göstermek mümkündür²⁷⁵. Netice itibariyle *Schurmann*'ın betimlediği bu süreçsel dizge sağlıklı bir şekilde kurulduğu takdirde gerçek anlamda bir haberleşme kurulmuş olacaktır. Zaten haberleşme (*Communication*) kelimesinin Latince kaynağı olan “*communis*” de “ortak” anlamına geldiğine göre bir noktada birleşmek şarttır. Bu birleşim aynı alanı paylaşım

²⁷² İÇEL/ ÜNVER, Kitle Haberleşme Hukuku, sh: 4; GEDİK, Kitle İletişim Özgürlüğü, sh: 26.

²⁷³ GEDİK, Kitle İletişim Özgürlüğü, sh: 26 v.d.

²⁷⁴ İÇEL/ ÜNVER, Kitle Haberleşme Hukuku, sh: 4.

²⁷⁵ OSKAY, Ünsal, XIX. Yüzyıldan Günümüze Kitle İletişimin Kültürel İşlevleri – Kuramsal Bir Yaklaşım , Ankara, 1992, sh: 310.

anlamına gelir. Haberleşme teorisi anlamında bir ortak paylaşım da, kaynağın kodlayıcısıyla hedefin kod açıcısının örtüştüğü noktada doğmaktadır²⁷⁶.

Yukarıda kaynak – hedef sayısına bağlı olarak kurulan haberleşmenin niteliğinde değişiklik oluşacağı ifade edilmişti. Buna göre kaynak ile hedefin birer taraftan olduğu haberleşme süreci “*bireysel haberleşme*”, kaynak ile hedefin birden çok taraftan oluşması durumunda kurulan haberleşme sürecine ise “*kitlesel haberleşme*” adı verilmektedir²⁷⁷. Bireysel iletişim husus pek sorunlu bir nokta olarak görülmemektedir. Dolayısıyla bu noktadan sonra haberleşmenin kitlesel gerçekleştiği “*kitle haberleşme*” üzerinde konsantre olunmalıdır. Haberleşmenin ne olduğu ortaya konulduğuna göre “*kitle*” kavramının da bu bağlamda ne anlam ifade ettiğine kısaca bakmak gerekir.

Haberleşme tarzının belirleyicisi olarak “*kitle*” kavramı üzerinde hemfikir olunan bir kavram değildir. *İçel/ Ünver* kitle kavramını açıklarken ikili bir ayrıma gitmeyi uygun görmekte dirler. Yazarlara göre kitle haberleşme kapsamında kitle kavramı sosyolojik çerçevede dar boyutta değil geniş boyutta yorumlanması gerekir²⁷⁸. Daha açık bir ifade ile belirli bir mekanda buldukları varsayılan büyük sayıdaki insanların meydana getirdiği her çeşit insan topluluğu geniş anlamda kitle kapsamına girer ve kitlesel haberleşmenin yöneldiği “*kitle*” kavramını ortaya koyar. Yine *Gedik*, bir amaç birliği olmayan sürekliliği bulunmayan temel güdülerle bir araya gelmiş toplulukları “*kitle*” olarak tanımlamaktadır²⁷⁹. Son bir örnek olarak *Zillioğlu* da, kitle iletişimi tanımlarken hedef olarak kitlenin büyük ve dağınık olması gerektiğini ortaya koymuştur²⁸⁰.

Tüm bu örnekler bir arada düşünüldüğünde “*kitle*” kavramı ile ilgili belirlenen temel kriterin büyük sayıda insandan oluşan bir topluluk veya topluluklar kümesi olduğu görülmektedir. Buna ek olarak üzerinde bir uzlaşım olmamakla beraber dağınıklık ve geçicilik unsurları da “*kitle*” kavramının somutlaştırılmasında göz önünde bulundurulabilir. Buna göre doktrinde üzerinde uzlaşım sağlanan unsurlar esas alınmak üzere kitle haberleşmeyi bilgi,

²⁷⁶ **OSKAY**, Kitle İletişimin Kültürel İşlevleri, sh: 310 – 311.

²⁷⁷ **DÜLGER**, İnternet Erişiminin Engellenmesi, sh: 1497; **GEDİK**, Kitle İletişim Özgürlüğü, sh: 25 – 26.

²⁷⁸ **İÇEL/ ÜNVER**, Kitle Haberleşme Hukuku, sh: 10.

²⁷⁹ **GEDİK**, Kitle İletişim Özgürlüğü, sh: 24.

²⁸⁰ **ZILLIOĞLU**, Merih, İletişim Nedir?, 2. Baskı, İstanbul, 2003, sh: 25.

düşünce, duygu ve tutumların uygun araçlarla çok sayıda insandan oluşan bir topluluğa ulaştırılması süreci olarak tanımlanabilmektedir. İşte kitlesel haberleşmeyi mümkün kılan araçlar da kitle haberleşme araçlarını teşkil etmektedir. Kitap, dergi, gazete, radyo, televizyon, sinema gibi görsel işitsel iletişim araçları yöneldikleri hedefler esas alındığında birer kitle haberleşme aracı olarak kabul edilmekte ve 5237 sayılı TCK md. 6/1-g hükmünce birer basın – yayın aracı sayılmaktadırlar.

1.2.- Değerlendirmeler

Kanaatimizce bu teorik alt yapıya göre internetin, kanun koyucunun tercihi doğrultusunda, bir kitle haberleşme aracı olmak suretiyle basın- yayın aracı olup olmadığı tartışması maddeler halinde şu şekilde ortaya konulabilir:

i.- Öncelikle internetin birinci bölümde detaylarıyla ortaya konulan yapısı gereği, yukarıda yapılan çözümlenmeler referans alındığında bir haberleşme aracı olduğundan hiç şüphe yoktur. Bu yüzden bu konuda başkaca açıklama yapmayı gereksiz görmekteyiz. Ancak yapı itibariyle genel eğilim çerçevesinde internetin bireysel haberleşme aracı mı yoksa kitle haberleşme aracı mı olduğu sorunu önem arz etmektedir. Doktrinde yukarıda çözümlenen ayırımı paralel olarak bireysel ve kitlesel haberleşme arasındaki farkları belirlemeye yönelik girişimlere rastlanmaktadır. Bunlara en yeni örnek *Gedik'in* gruplandırma çabasıdır. Buna göre bir kitle haberleşme kaynağının bir kişi değil gazete televizyon gibi örgütlenmiş bir topluluk olması, geri beslemenin (feed back) çok zor ve hatta imkansız olması, alıcı yani hedefin dikkatinin zayıf ve dağınık olması ve son olarak hızlı gerçekleştiği için inandırıcılığının az olması dolayısıyla bireysel haberleşmeden ayrılır²⁸¹.

Bu kriterleri bireysel ve kitlesel haberleşme arasındaki farklılığı ortaya koymak bakımından yeterli kabul etmek imkansızdır. Nitekim bu kriterler internete uygulandığı zaman internet ne bir bireysel haberleşme aracı ne de bir kitle haberleşme aracı olarak kabul edilebilir. Çünkü kitle haberleşme aracı olmak için aranan kaynağın örgütlenmiş bir topluluk olması kriteri günümüz internet teknolojisinde söz konusu değildir. Örneğin, bugün herkes kamusal erişilebilirliği haiz bir web sitesi oluşturabilir, bu web sitesinden, bir gazete, dergi v.s. gibi, haber, düşünce kanaat yayınlatabilir. Böyle bir durumda söz konusu web sitesini, bir kişiye ait olması, örgütlenmiş bir yapısının olmaması nedeniyle bir kitle haberleşme aracı

²⁸¹ **GEDİK**, Kitle İletişim Özgürlüğü, sh: 28.

kabul etmemek mümkün değildir. Yine kitle haberleşme araçlarında geri bildirim çok zor ve hatta imkansız olduğu görüşü de modern haberleşme teknolojileri ile kesinlikle örtüşmemektedir. Bugün bir web sitesinde yayınlanan haber, görüş veya eleştiriler anında yorumlanabilmekte, eleştirilebilmekte ve kaynak ile hedef arasında bir dinamik bir ilişki oluşmaktadır. Buradan da ortaya çıkmaktadır ki, internet klasik kitle haberleşme formlarını günümüz teknolojisinde yeniden şekillendirmekte ve kitle haberleşmeye yeni bir eksen kazandırmaktadır. Bu haliyle internet pekala bir kitle haberleşme aracı olarak kabul edilebilecektir²⁸².

ii.- Ancak internet sadece bir kitle haberleşme aracı değildir. Çünkü sunduğu hizmetler gereği kullanıcılar, kitlesel bir haberleşme sürecine girmeden sadece belli kişiler arasında haberleşme ağı kurabilmektedirler. E-posta veya MSN gibi eş zamanlı mesajlaşma veya sohbet programları bunun en önemli örnekleridir. Şu halde internet bireyler arası bağlantının kurulduğu bir süreci olarak bir bireysel haberleşme aracı olarak da kullanılabilir. Dolayısıyla internet klasik haberleşme ayrımı içinde *sui generis* bir konuma ulaşmaktadır. Yani kullanım tarzına bağlı olarak hem bireysel hem de kitle haberleşme aracı kabul edilebilmektedir. O halde internet için karma haberleşme aracı ifadesini kullanmak yerinde olabilecektir. Netice itibariyle 5237 sayılı TCK md. 6/1-g hükmü karşısında internet için *ad hoc* kitle haberleşme aracı demek imkansızdır. İnternetin araç olarak kullanıldığı suçlarda, kullanım tarzına paralel olarak her somut olayda bir değerlendirme yapmak şarttır. Bunun önemi, 5237 sayılı TCK'nin özel hükümler bölümünde yer alan kimi suçlarda, işlenişinde basın yayın araçlarının kullanılması suçu nitelikli hale getirebilmektedir. Dolayısıyla internet sadece bir kitle iletişim aracı olmak anlamında basın yayın aracı olarak kabul edilecek olursa, bireysel bir iletişim aracı olması özelliği göz önünde bulundurulmadan yanlış değerlendirmelere sebebiyet verilebilir.

iii.- Yukarıda kitle haberleşme araçları ile ilgili yapılan açıklamalarda “*kitle*” kavramının çok sayıda insan tarafından oluşturulan topluluk olarak tanımlandığı görülmüştür. Klasik kitle haberleşme araçları bakımından “*kitle*”nin bu şekilde anlaşılacağı söylenebilir. Çünkü kitle haberleşmenin karşıtı olan bireysel haberleşme araçları genellikle bir veya az sayıda kişiyle aynı anda kurulan haberleşme olarak kabul edilmektedir. Ancak internet teknolojisinin gelmiş olduğu aşama nazarı dikkate alınacak olursa, bireysel haberleşme aracı olarak görülen e-posta alış verişinde kaynak kullanıcı aynı anda onlarca ve

²⁸² SALİHPAŞAOĞLU, Basın Özgürlüğü, sh: 24; DÜLGER, İnternet Erişiminin Engellenmesi, sh: 1497.

hatta yüzlerce kişiye aynı e-postayı gönderebilmektedir. Bu anlamda klasik anlamda kaynak – hedef sayısından hareketle bir “*kitle*” tanımına ulaşmak, kitlenin karşılığı olan “çok sayıda insan” nitelemesinin muğlaklığı karşısında problemler ortaya koyabilecektir. *Kanaatimizce* böyle durumlarda internetin kendine özgü yapısı içinde önemli bir tespitin yapılması gerekmektedir. Her ne kadar bir seferde onlarca, yüzlerce ve hatta binlerce kişiye gönderilen bir mail kitlesel bir iletişim izlenimi verse de, özünde burada söz konusu olan kümülatif (yığılan) bireysel iletişimlerdir. Çünkü bir seferde binlerce kişi muhatap alınmakta ve fakat kaynak kullanıcı hedef kullanıcıların adreslerine/ hesaplarına özel olarak yani bireysel olarak bir veri iletmektedir. Bu nedenledir ki, kurulan binlerce bireysel iletişimin kümülatif bir değerlendirmesi, hedef sayısına bakılarak bir kitle iletişimin varlığını mümkün kılmaz. Bu anlamda özellikle internet ile birlikte kitle haberleşme anlayışının bir değişime uğradığı, artık haberleşme taraflarının sayısı esas alınarak bireysel veya kitle haberleşmeden bahsedilebilmesinin hatalı sonuçlara sebebiyet verebileceği görülmektedir. *Kanaatimizce* interneti 5237 sayılı TCK md. 6/1-g hükmüne bir kitle haberleşme aracı olması anlamında basın – yayın aracı olarak kabul edebilmek için, içeriğin sayısal anlamda belli bir çoğunluğa ulaşmış olmadığına bakmadan, söz konusu içeriğe kamusal erişilebilirliğinin söz konusu olup olmadığına bakmak gerekecektir²⁸³.

iv.- İnternetin hangi ölçülerde bir kitle haberleşme aracı olduğu irdelendikten sonra internetin basın ile ilişkisi üzerinde durmak gerekmektedir²⁸⁴. Çünkü internet yukarıda özetlendiği üzere kitle haberleşme aracı kimliği ile bir basın – yayın aracı olarak kabul edilmektedir. Peki interneti bir basın aracı olarak kabul etmek mümkün müdür? Bu sorunun önemi şuradan kaynaklanmaktadır; şayet internet bir basın aracı olarak kabul edilebilirse otomatik olarak 5187 sayılı Basın Kanunu’nun düzenleme kapsamı altına girmektedir²⁸⁵. 5187 sayılı Basın Kanunu ile yürürlükten kaldırılan 5680 sayılı Basın Kanunu 15. 05.2002 tarih ve 4756 sayılı Kanununun 26. maddesiyle eklenen Ek Madde 9 ile “ *Bu Kanununun yalan haber, hakaret ve benzeri fiillerden doğacak maddi ve manevi zararlarla ilgili hükümleri, 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 benzeri hakkında da uygulanır*” şeklinde bir ifade kullanılmaktaydı. Ancak bu hüküm doktrinde yoğun eleştirilere uğramış ve 5187 sayılı yeni Basın Kanununda benzer bir hükme

²⁸³ Kamusal erişilebilirlik konusunda bkz. **NIGGLI**, İrt Ayrımcılığı ve İnternet, sh: 275.

²⁸⁴ Basın kavramının tarihsel gelişim süreci ve internet ile olan ilişkisi ile ilgili değerlendirmeler için bkz. **SALİHPAŞALIOĞLU**, Basın Özgürlüğü, sh: 22 v.d.

²⁸⁵ **İLKİZ**, Fikret, İnternet Ortamında Yayınlar, in: İnternet ve Hukuk, sh: 452 v.d.

yer verilmemiştir. Eleştirilerin çokluğu ve haklılığı ile söz konusu hükümlerin yeni Basın Kanununa alınmamış olması Basın Kanununda yer alan düzenlemelerle interneti düzenlenmesinin mümkün olmadığını açık bir biçimde göstermektedir. Çünkü arada bir doku uyumsuzluğu vardır. İnternet yayıncılığı; televizyon yayıncılığının ve gazete yayıncılığının kendi aralarında farklılar göstermesi gibi, bu her ikisinden de farklı bir yapı göstermekte internetin kendine özgü olanaklarından yararlanmaktadır²⁸⁶. Zaten bu yaklaşım tarzından hareketle internet yayıncılığının düzenlenmesi ve internette yayınlanan içeriklerin sebebiyet verdiği suçlarla mücadele konusunda 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun yürürlüğe girmiştir.

2.- İNTERNET ARACILIĞIYLA İŞLENEN İÇERİK SUÇLARDA İHMALİ VE İCRAİ HAREKETLER

2.1. Genel Olarak İcrai – İhmali Suç Ayırımı

İnternet ortamında işlenebilen içerik ve müdahale suçları bakımından dikkat edilmesi gereken bir husus da, suç teşkil eden eylemlerin hareket unsuru bakımından icrai mi yoksa ihmali mi gerçekleştirildiğidir. Daha önce detaylarıyla üzerinde durulduğu üzere, internet teknolojisi hizmet kolaylığı bakımından toplumun hemen hemen tüm kesiminde kullanılan bir teknoloji olmasına rağmen, teknik açıdan çok karmaşık bir yapıdır ve özellikle internet sükjelerinin sergiledikleri tutumlar tipik neticenin tespitinde hatalı sonuçlara ulaşılmasına neden olabilirler²⁸⁷. Bu bakımdan internet sükjelerinin yukarıda aktarılan sorumluluk çerçeveleri dahilinde, içerik ve müdahale suçlarına ilişkin icrai ve ihmali davranışlar üzerinde durulmalıdır.

Bilindiği gibi hareketin şekline göre suç temel olarak iki kategoride ele alınmaktadır²⁸⁸. Bunlardan birinde fail dış dünyada bir değişiklik neticesi doğuran aktif bir davranış sergilemektedir. Diğerinde ise fail kendi yeteneğine ve mevcut araçlara göre somut

²⁸⁶ DÜLGER, İnternete Erişimin Engellenmesi, sh: 1498 – 1499.

²⁸⁷ BAŞPINAR/ KOCABEY, İnternette Fikri Hakların Korunması, sh: 34.

²⁸⁸ Öztürk/ Erdem Hareketin şekli bakımından suçları, bağlı hareketli suçlar, serbest hareketli suçlar, icrai suçlar ve ihmali suçlar olmak üzere dört başlık altında toplamışlardır. ÖZTÜRK/ ERDEM, Uygulamalı Ceza Hukuku, sh: 132.

ve bireysel olarak mümkün olan belli bir iradi davranışı yapmamaktadır. İşte birinci alternatifte failin davranışı bir suç teşkil ediyorsa bu icrai suç, ikinci alternatifte failin davranışı suç teşkil ediyorsa da ihmali suç söz konusu olur²⁸⁹. Türk hukukunda ihmal ve icrayı kapsayan üst kavram olarak hareket kavramı kullanılmaktadır. İhmali ifade etmek üzere, olumsuz menfi, negatif hareket; icrayı ifade etmek üzere ise olumlu, müspet, pozitif hareket terimlerinin kullanıldığına rastlanmaktadır²⁹⁰. *Hakeri*'nin de ifade ettiği üzere, Türk Ceza Hukuku terminolojisinde de ihmal ve icrayı kapsamak üzere davranış teriminin kullanıldığı görülmektedir²⁹¹.

TCK'nin özel hükümlerinde yer alan suçlara bakıldığında genel olarak icrai nitelikli yani aktif bir davranış gerektiren suçların ağırlıklı olarak düzenlendiği görülmektedir. Buna karşılık çok az sayıda suç tipinde, bir davranışın ihmal edilmesi suretiyle gerçekleştiği açıkça yazmaktadır. Bu nedenle, bir davranışın ihmali dolayısıyla suçun gerçekleştiğinin açıkça belirtildiği suç tiplerinin dışında kalan suçlar suçların ancak icrai hareketle işlenebileceği yönünde bir kanı oluşmaktadır. Ancak bu doğru bir değerlendirme değildir. Çünkü Kanunda yer alan bir suç tipinde ayrıca ve açıkça ihmal kavramının kullanılmamış olması o suçun ihmali bir hareketle işlenmesine engel teşkil etmemektedir. Zira suç tipinde neticenin pozitif veya negatif hareketle meydana gelmesi arasında ilke olarak ayırım yapılmamaktadır²⁹².

Doktrinde ihmal kavramından ne anlaşılması gerektiği konusunda birbirine yakın görüşler ortaya konulmaktadır. Örneğin *İçel'e* göre ihmal, yapılması gereken bir hareketin yapılmamasıdır²⁹³. Yine *Öztürk/ Erdem* göre ihmal icradan farklı olarak deneysel bir gerçeklik olmayıp, hukuksal açıdan kişiden beklenen bir hareketin gerçekleştirilmemesidir²⁹⁴. *Özgenç* ise ihmal, davranış normlarıyla kişiye belli bir icrai davranışta bulunma yükümlülüğünün tahmil edildiği hallerde kişinin bu yükümlülüğü yerine getirmemesi olarak

²⁸⁹ **YILDIZ**, Türk Ceza Hukuku, sh: 179; **HAKERİ**, Hakan, Ceza Hukuku Genel Hükümler, 7. Baskı, Ankara, 2008, sh: 113.

²⁹⁰ **HAKERİ**, Ceza Hukuku, sh: 114.

²⁹¹ **HAKERİ**, Ceza Hukuku, sh: 111; **HAKERİ**, Hakan, İhmali Suçlar, in: CHD (Ed: Veli Özer ÖZBEK), Y:2, S: 4, Ankara, 2007, sh: 138- 139.

²⁹² **HAKERİ**, Ceza Hukuku, sh: 112.

²⁹³ **İÇEL**, Ceza Hukuku, sh: 58.

²⁹⁴ **ÖZTÜRK/ ERDEM**, Uygulamalı Ceza Hukuku, sh: 132.

kabul ederken²⁹⁵ *Hakeri*'ye göre ihmal kavramından anlaşılması gereken, bir kimsenin kendi yeteneğine ve mevcut araçlara göre somut ve bireysel olarak mümkün olan belli bir iradi davranışı yapmamasıdır²⁹⁶. Yazar ihmali suçlar denildiğinde akla gelen hususun, bir kimsenin ya özel bir yükümlülüğe aykırı olarak ya da genel bir hareket yükümlülüğüne aykırı olarak belli bir hareketi yapmayı ihmal etmek suretiyle işlediği suçlar olduğunu ifade etmiştir²⁹⁷. Bu noktada ihmal suçların çeşitlerine de göz atmak yerinde olur.

Doktrinde ihmali suçlar bakımından farklı başlıklar kullanıldığı görülmektedir. *Öztürk/Erдем* gerçek ihmali suçlar ve görünüşte ihmali suçlar (İhmal Suretiyle İcra Suçları) olmak üzere ikili bir ayırım kabul etmiştir. Buna göre gerçek ihmali suçlarda belirli bir davranışta bulunma zorunluluğu suç tipinde öngörülmektedir²⁹⁸. Suç tipinde öngörülen bu davranışta bulunma zorunluluğuna itaat edilememesi suretiyle ihmali davranış gerçekleşme ve bu davranış bir suç olma vasfıyla cezalandırılmaktadır. Yazarlar buna örnek olarak TCK md. 257/2'de düzenlenen görevi ihmal ve md. 98'de düzenlenen yardım ve bildirim yükümlülüğünün yerine getirilmemesi suçunu göstermişlerdir²⁹⁹. Görünüşte ihmali ya da başka bir deyişle ihmal suretiyle icra suçları ise, gerçek ihmali suçlardan farklı olarak kanunda tanımlanmaz. Burada aslında aktif olarak işlenebilen bir suçun hareketsiz kalınarak işlenmesi durumu söz konusudur. Bu bağlamda ihmal suretiyle bir neticenin doğmasını

²⁹⁵ ÖZGENÇ, Ceza Hukuku, sh: 212.

²⁹⁶ HAKERİ, İhmali Suçlar, sh: 140.

²⁹⁷ HAKERİ, Ceza Hukuku, sh: 112.

²⁹⁸ ÖZTÜRK/ERDEM, Uygulamalı Ceza Hukuku, sh: 133.

²⁹⁹ **Madde 257 - (1)** Kanunda ayrıca suç olarak tanımlanan hâller dışında, görevinin gereklerine aykırı hareket etmek suretiyle, kişilerin mağduriyetine veya kamunun zararına neden olan ya da kişilere haksız bir kazanç sağlayan kamu görevlisi, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır.

(2) Kanunda ayrıca suç olarak tanımlanan hâller dışında, görevinin gereklerini yapmakta ihmal veya gecikme göstererek, kişilerin mağduriyetine veya kamunun zararına neden olan ya da kişilere haksız bir kazanç sağlayan kamu görevlisi, altı aydan iki yıla kadar hapis cezası ile cezalandırılır.

(3) İrtikâp suçunu oluşturmadığı takdirde, görevinin gereklerine uygun davranması için veya bu nedenle kişilerden kendisine veya bir başkasına çıkar sağlayan kamu görevlisi, birinci fıkra hükmüne göre cezalandırılır.

Madde 98 - (1) Yaşı, hastalığı veya yaralanması dolayısıyla ya da başka herhangi bir nedenle kendini idare edemeyecek durumda olan kimseye hâl ve koşulların elverdiği ölçüde yardım etmeyen ya da durumu derhâl ilgili makamlara bildirmeyen kişi, bir yıla kadar hapis veya adli para cezası ile cezalandırılır.

(2) Yardım veya bildirim yükümlülüğünün yerine getirilmemesi dolayısıyla kişinin ölmesi durumunda, bir yıldan üç yıla kadar hapis cezasına hükmolunur.

engellemeyen kişi ancak belli şartlar söz konusu olursa, o davranışı aktif olarak icra eden kişi gibi cezai müeyyideye tabi tutulur³⁰⁰. Öncelikle bu suçlarda fail neticeyi önleme bakımından hukuki bir yükümlülük altında olması gerekmektedir. Bu bakımdan yazarlar bu tür suçların aynı zamanda mahsus suç olma niteliğinde olduğunu kabul etmektedirler. Bu yükümlülüğün kaynağı kanun, sözleşme ya da failin daha önceki yükümlülüğe aykırı davranışından ileri gelmektedir. İkinci ve buna bağlı olarak hukuki yükümlülüğün gerçekleşen bir neticeden dolayı sorumluluk ortaya çıkarabilmesi için failin hareketsiz kalacağı yerde harekete geçmiş olsaydı, neticeyi de önleyebilmesinin mümkün olması gerekmektedir. Aksi bir durum söz konusu olursa burada görünüşte ihmali suçtan bahsedilememektedir³⁰¹.

Hakeri ise, ihmali suçları yine iki başlık altında incelerken, ihmali suçları saf ihmali suçlar ve garantörsel ihmali suçlar olarak isimlendirmiştir. Yazar saf ihmali suçları, kanunun kişiden icrai bir davranış beklediği yerde, bu davranışı yapmamak suretiyle işlenen ve sırf bu davranışın yapılmamasının suçun oluşması bakımından yeterli olduğu, ayrıca garantörlük şartının öngörülmediği suçlar olarak tanımlamaktadır³⁰². Bu tür suçlarda fail kanunda belirtilen bir ihmali hareketi yapmakla suç işlemekteyken ayrıca bunun için garantör olması gerekmemektedir. Bu suç tipine örnek olarak TCK md. 116 gösterilmektedir³⁰³. *Hakeri*'ye göre esas itibarıyla garantörsel ihmali suç düzenlemesine ilişkin hükümler içeren ve ihmal suretiyle kasten adam öldürmeyi düzenleyen md. düzenleniş şekli ve yeri itibarıyla saf ihmali suç niteliğindedir.

³⁰⁰ **ÖZTÜRK/ERDEM**, Uygulamalı Ceza Hukuku, sh: 133. Benzer bir değerlendirme için **YILDIZ**, Türk Ceza Hukuku, sh: 180 v.d.

³⁰¹ Aynı yönde değerlendirmeler için bkz. **ÖZGENÇ**, Ceza Hukuku, sh: 217 v.d.

³⁰² **HAKERİ**, Ceza Hukuku, sh: 112

³⁰³ **Madde 116 - (1)** Bir kimsenin konutuna, konutunun eklentilerine rızasına aykırı olarak giren veya rıza ile girdikten sonra buradan çıkmayan kişi, mağdurun şikâyeti üzerine, altı aydan iki yıla kadar hapis cezası ile cezalandırılır.

(2) (**Değişik fıkra: 31/03/2005 - 5328 S.K./8.mad**) Birinci fıkra kapsamına giren fiillerin, açık bir rızaya gerek duyulmaksızın girilmesi mutad olan yerler dışında kalan işyerleri ve eklentileri hakkında işlenmesi halinde, mağdurun şikâyeti üzerine altı aydan bir yıla kadar hapis veya adli para cezasına hükmolunur.

(3) (**Değişik fıkra: 31/03/2005 - 5328 S.K./8.mad**) Evlilik birliğinde aile bireylerinden ya da konutun veya işyerinin birden fazla kişi tarafından ortak kullanılması durumunda bu kişilerden birinin rızası varsa, yukarıdaki fıkralar hükümleri uygulanmaz. Ancak bunun için rıza açıklamasının meşru bir amaca yönelik olması gerekir.

(4) Fiilin, cebir veya tehdit kullanılmak suretiyle ya da gece vakti işlenmesi hâlinde, bir yıldan üç yıla kadar hapis cezasına hükmolunur.

Garantörsel ihmali suçlar da ise ceza kanununda yer alan ve kural olarak bir icrai davranışla gerçekleştirilen bir suç tipinin ihmali bir davranışla işlenmesi halinde ortaya çıkar. Bu tip suçlarda failin neticeye neden olan pozitif bir hareketinden söz etmek mümkün değilse de, fail bu neticenin ortaya çıkmasını arzu ettiğinden tepkisiz kalmakta ve kanunda öngörülmüş netice de fail sayesinde meydana gelmektedir. Bu bağlamda *Hakeri*, garantörsel ihmali suçlarda hem icra hem de ihmal kusurunun mevcut olduğunu ifade ederken, garantörsel ihmali suçlara ilişkin olarak TCK’da müstakil bir hükmün bulunmadığını dile getirmiştir³⁰⁴.

Garantörlük kavramının kaynağına da değinen yazar, Anayasamızdaki “*temel hak ve hürriyetler, kişinin topluma, ailesine ve diğer kişilere karşı ödev ve sorumluluklarını da ihtiva eder.*” hükmünden (md. 12) veya ceza kanununun özel kısmındaki müstakil suç tiplerinin dayandığı, insanlara zarar vermemeye yönelik “genel emir”den, yine ceza kanunu tarafından garanti altına alınmış ve herkese yönelik bir “*ceza kanununun özel kısmındaki müstakil suç tiplerinde açıklanmış bulunan neticeyi önleme yükümlülüğü*” çıkarılmasa da kanun koyucunun bazı özel hallerde, böyle bir yükümlülüğü öngörmeyi uygun bulduğunu ve fakat bunun için ek bir takım koşulların gerçekleşmesini aradığını belirtmiştir³⁰⁵. Bu bağlamda yazar bir garantörlüğün varlığından bahsetme noktasında yukarıda aktarılan *Öztürk/Erdem*’in görünüşte ihmali suçlar için aradıkları koşullarla paralel koşullar aramaktadır. Yine *Hakeri* de garantörlüğün kaynağı olarak kanun, sözleşme veya ön gelen tehlikeli eylemi kabul etmiştir³⁰⁶.

Nihayet *Hakeri*, ihmali suçlarda nedensellik ilişkisi üzerinde dururken, ihmali suçlarda ihmal edilen hareket yapılıyorsa, netice kesinlik sınırında yakın bir olasılıkla engellenebilecekti denilebiliyorsa, ihmalin nedensel olduğunun kabul edilmesi gerektiğini vurgulamaktadır³⁰⁷.

³⁰⁴ **HAKERİ**, Ceza Hukuku, sh: 114; **HAKERİ**, İhmali Suçlar, sh: 143.

³⁰⁵ **HAKERİ**, Ceza Hukuku, sh: 115.

³⁰⁶ **HAKERİ**, Ceza Hukuku, sh: 115 - 116.

³⁰⁷ “*Ateşli silah mermi çekirdeği ile yaralanıp kaldırıldığı Ankara hastanesinde çene ve boyun solundaki yaralarına dikiş atılıp evine gönderilen ve yakınmalarının artması üzerine ertesi gün tekrar aynı hastaneye başvurulduğunda sol göğüs omuru dış kısmında yumuşak dokuları arasında mermi çekirdeği bulunduğu fark edilip Hacettepe Hastanesine sevk edilen ve aynı gün orada ölen C.T.nin otopsi raporuna göre ölümünün ateşli silah mermi çekirdeği yaralanmasına bağlı birinci göğüs omur kırığı işe birlikte omurilik zedelenmesi sonucu meydana geldiği ve kişiye bir adet mermi çekirdeği isabet ettiği ve müstakilen öldürücü nitelikte olduğu belirtilmesi karşısında, yaralandığı gün kaldırıldığı Ankara Hastanesinde ateşli silah yarası tespit edilerek*

2.2.- İnternet Ortamında İşlenen Suçlarda İhmali ve İcrai Hareketler

Bu açıklamalar ışığında internet ortamında işlenebilecek içerik ve müdahale suçları bakımından internet sùjelerinin hareketin şekline göre icrai mi ihmali davranacakları hususuna göz atılacak olursa şu tespitleri yapmak mümkündür:

İçerik sağlayıcı, tanımı gereği bir içeriği internet ortamına aktaran ve o içerik üzerinde doğrudan tasarrufta bulunan bir internet sùjesi olarak içerik suçları anlamında hiç şüphe yok ki icrai davranışta bulunmaları gerekecektir. Çünkü burada bir içerik aktif bir davranışla teknik imkanlar kullanılmak suretiyle internet ortamına aktarılmaktadır. Bu davranış tam olarak icrai suçlarda gözlemlenen bir davranıştır. Yine link vermek suretiyle suç içerikli bir veriye erişimi sağlaması durumunda da yine içerik sağlayıcının aktif bir davranışıyla karşılaşılmaktadır. Ancak bir içerik sağlayıcı, internet ortamına aktardığı içeriğin suç teşkil ettiğine ve söz konusu içeriğin kaldırılması veya değiştirilmesi talebine ilişkin bir bildirim almasına rağmen, bildirim gereğini yerine getirmezse ihmali davranış sergilediği söylenebilir. Keza aynı durum erişim ve yer sağlayıcı için geçerli olmaktadır.

İnternet sùjelerinin ihmali davranışlarda bulunabilecekleri kabulüyle birlikte, içerik suçları bakımından internet sùjelerinin sergiledikleri ihmali davranışların *Hakeri*'nin ayırımıyla saf ihmali suçlara mı yoksa garantörsel ihmali suçlara mı vücut vereceği sorusu akla gelmektedir. 5651 sayılı Kanunda internet sùjelerinin yükümlülük ve sorumluluklarının belirlendiği düşünülecek olursa; ilgili Kanun gerek içerik sağlayıcıya gerek yer sağlayıcıya gerekse erişim sağlayıcıya suç teşkil eden içeriklerin internet ortamından uzak tutulması konusunda bir garantörlük tesis etmiştir. Bu garantörlük teknik imkanlar çerçevesi dahilinde içerik sağlayıcı için suç teşkil içeriklerin kaldırılması veya değiştirilmesi, yer sağlayıcı için ilgili içeriği barındırmama ve nihayet erişim sağlayıcı için de ilgili içere erişimin engellenmesi sağlamaktır. Şayet bu internet sùjeleri, Kanun tarafından düzenlenen bu sorumlulukları yerine getirmemek suretiyle bir içerik suçun işlenmesine sebebiyet verdikleri takdirde³⁰⁸, ihmal davranışı ile somut netice arasında bir nedensellik bağının da söz konusu

gereken şekilde müdahale ve tedaviye devam edilmesi halinde yaralının kurtarılmasının tıbben mümkün olup olmadığının Ölene ait rapor ve otopsi zabıtları Adli Tıp Kurumu ilgili ihdisas dairesine gönderilerek sorulmak suretiyle araştırma yapılıp durumunun tayin ve tepsini gerektiği gözetilmeksizin noksan araştırmayla karar verilmesi yasaya aykırıdır.” HAKERİ, Ceza Hukuku, sh: 137’ den naklen.

³⁰⁸ Bkz. § 7. Suça İştirak Hükümleri Bağlamında İnternet Sùjelerinin Konumları Ve Cezai Sorumlulukları.

olduğu bir durumda, ortada yükümlülüğünü yerine getirmeyen internet süjesi bakımından garantörsel bir ihmali suçun varlığı kabul edilmelidir.

İnternet ortamında işlenen müdahale suçları olarak nitelendirdiğimiz suç tiplerinin büyük bir çoğunluğunda ise tipe uygun eylem unsuru icrai hareketlerle gerçekleştirilmektedir. Örneğin bir kimsenin bilgisayarına virüs bulaştırmak suretiyle verileri tahribine sebebiyet vermek, bir kişinin mail şifresinin kırılması veya değiştirilmesi suretiyle haberleşmenin engellenmesi, yine bir kişiye ait olan interaktif bankacılık şifresinin çalınması ve bu şifreyle kişinin hesabının boşaltılması gibi eylemler özellikleri gereğince aktif bir hareketin gerçekleştirilmesi gereken eylemlerdir. Dolayısıyla bu eylemlerin gerçekleştirilmesi suretiyle işlenen suçların icrai suçlar olarak kabul edilmesi mümkündür.

Bunun yanında müdahale suçları bakımından ihmali hareketle tipe uygun eylemin gerçekleştirilip gerçekleştirilemeyeceği hususunda da öncelikle şunu ifade etmek mümkündür ki, içerik suçlarına nazaran müdahale suçlarının ihmali hareketle işlenmesi daha dar bir alanda söz konusu olmaktadır. Örneğin içerik sağlayıcısı olduğu ve ücretsiz antivirüs yazılımlarının indirilebildiği bir sitede hiçbir uyarı bulundurmuyarak, erişildiği takdirde kullanıcının bilgisayarındaki verileri kullanılamaz hale getiren kötücül yazılımı kayıtlı halde tutan failin, aktif olarak programı indiren kullanıcının bilgisayarına bir kötücül yazılım yüklememesine rağmen, kullanıcı tarafından fark edilmesi güç olan ve bir antivirüs yazılımı zannıyla indirilebilen bu kötücül yazılımı muhafaza ettiği, kullanıma sunduğu için ihmal suretiyle verilere zarar verme suçundan sorumlu tutulabileceği *kanaatindeyiz*. Ancak söz konusu fail kötücül yazılımı bizzat diğer kullanıcıların bilgisayarlarındaki verilere zarar verme kastıyla ilgili siteye yüklediyse, her ne kadar o yazılımın başka bilgisayarlara yüklenmesi komutunu vermek suretiyle icrai bir harekette bulunmamış olsa da, şart teorisinin nedensellik kabulü çerçevesinde doğan netice bakımından salt o yazılımı muhafaza etmek ve kullanıma sunmaktan dolayı icrai hareket ettiğinin kabulü gerekmektedir.

3.- İNTERNET ORTAMINDA İŞLENEN SUÇLARDA MANEVİ UNSUR SORUNU

İnternet ortamında işlenen suçların yapısal özelliği bakımdan üzerinde önemle durulması gereken hususlardan biri de manevi unsur problemidir. Çünkü internet kullanımının her geçen gün gösterdiği artış herkesin bu teknolojiye faydalanmasına olanak tanımaktadır. Bu anlamda yaşam koşullarını iyileştirme bakımından çok önemli kolaylıklar sağlayan

internet teknolojisi aynı zamanda önemli riskleri de bünyesinde barındırmaktadır. Bunların başında insanların bilinçsiz ve bilgisiz kullanımları dolayısıyla yaşadıkları sorunlar yer almaktadır. Öyle internet ki eli mause tutan herkesin kullanabileceği bir hale gelmiştir.³⁰⁹ Dolayısıyla girilen eylemlerin de neticesinin dikkatlice göz önünde bulundurulması gerekmektedir. İşte bu sebeple internet ortamında işlenen suçlar bakımından manevi unsur önemli bir yer tutmaktadır.

Suçun manevi unsuru en genel tabiriyle failin fiille olan sübjektif ilişkisidir.³¹⁰ Bir başka anlatımla, suçun maddi unsurunu gerçekleştirmiş olan irade ile hukuk düzenin koymuş olduğu bir kural arasındaki aykırılıktır³¹¹. Bilindiği üzere bir eylemin suç olarak nitelendirilebilmesi için tipe uygun hukuka aykırı ve kusurlu bir davranış olması gerekmektedir. Bu anlamda kusurluluk kapsamı içinde değerlendirilen manevi unsur suçun temel yapısal özelliklerinden birini teşkil etmektedir. Kişinin gerçekleştirdiği bir fiilden dolayısıyla ceza hukuku anlamında sorumlu tutulabilmesi için salt eylediği hareketi ile netice arasında bir nedensellik bağı yeterli olmamakta, bunun yanında faille gerçekleştirdiği fiille arasında sübjektif nitelikte bir ilişkinin de bulunması esastır. Söz konusu bu ilişkinin kurulması ön şart olarak failin isnad kabiliyetine sahip olmasına ve daha sonra da kusurlu bir hareketinin olmasına bağlıdır. Dolayısıyla isnad kabiliyetinin mevcut olması bir kimsenin işlediği fiilden dolayı cezalandırılabilmesi için yeterli değildir. Bunun dışında failin somut olayda da iradesinin kusurlu olduğunun ortaya konulması gerekmektedir.

Hakeri'nin tanımlanmasıyla kusur suç teşkil eden bir fiilin isnad kabiliyetine sahip olan bir kimse tarafından bilerek ve isteyerek (kast) veya en azından bilerek (taksir) yapılmasıdır.³¹² Kusurluluk kapsamında manevi unsur, suçun bir unsuru olarak sadece işlenen bir fiile mahsus olarak ele alınır. Bu açıdan bakıldığında kusurluluk aynı zamanda ceza sorumluluğunun da bireyselleşmesi ve eylemin karşılığı olan ceza sorumluluğunun sınırlarının belirlenmesin bakımından önemli bir yere sahiptir.³¹³

³⁰⁹ **YALÇIN**, Sosyolojik, sh: 87.

³¹⁰ **ÖNDER**, Ayhan, Ceza Hukuku Genel Hükümler C: II, İstanbul, 1989, sh: 287.

³¹¹ **HAKERİ**, Ceza Hukuku, sh: 137.

³¹² **HAKERİ**, Ceza Hukuku, sh: 138 v.d.

³¹³ **ÖZTÜRK**, Bahri /**ERDEM**, Mustafa Ruhan/ **ÖZBEK**, Veli Özer, Uygulamalı Ceza hukuku ve Güvenlik Tedbirleri Hukuku, 5. Bası, Ankara, 2001, sh: 200.

Konunun önem derecesindeki temel etken Avrupa Konseyi Siber Suç Sözleşmesi'nin konuya yaklaşım tarzı ile ilgilidir. Sözleşmesinin gerekçesinde, sözleşme kapsamında ele alınan tüm siber suçların ancak kasten işlenebilir olduğu vurgulanmıştır. Bunun sonucu olarak, suç sayılan fiillerin taksirle işlenmesi halinde ceza sorumluluğunun varlığından bahsedilemeyeceği ortaya konulmuştur. Bu yaklaşım yukarıda dile getirilen bakış açısını destekler niteliktedir. Çünkü özellikle internet aracılığıyla girişilen eylemler daima hukuka uygun olmamaktadır. Bazen bu teknik alanda, bilgisizlik, dikkatsizlik sonucu suç teşkil edebilecek eylemler ortaya çıkmaktadır. Dolayısıyla istemeden hem ciddi zararlara sebebiyet verilmekte hem de ceza sorumluluğu doğuracak durumlar ortaya çıkmaktadır.

Bu anlayışın normatif düzenlemelere yansıyan bir örneğini Türk Ceza Kanunundan vermek de mümkündür. 5237 sayılı TCK md. 243'e göre bir bilişim sisteminin bütününe veya bir kısmına hukuka aykırı olarak giren ve orada kalan kimse cezalandırılmaktadır. İşte anılan düzenlemede bilerek ve isteyerek bir bilişim sistemine girmeyen kimselerin eylemini cezai yaptırıma tabi tutmamak için taksiri ortadan kaldırırcasına isteme unsurunu vurgular şekilde "girdikten sonra orada kalmaya devam etmeyi" aramaktadır³¹⁴. 243. maddeye ilişkin TBMM Genel Kurulunda yapılan görüşmelerde suçun unsurlarına ilişkin bir değişiklik teklif edilmiş ve bu teklif kabul edilerek madde son şeklini almıştır. Suçun unsurlarında yapılması istenen değişikliğe ilişkin

"Biliyorsunuz, bir de bilgisayar sistemini bozan hackerler var, onlar size bir şey gönderdi üzerine tıkladınız ve bir sisteme girdiniz. Hemen bunu suç haline getirirsek, çok geniş bir kapsama almış oluruz, suç kapsamını genişletmiş oluruz. Burada da - hazırladığımız taslakta- girme ve orada kalma şerhini koyduk; çünkü, bu bir kasttır. Kazara girersiniz çıkarsınız, bu başka bir şey; ama girdiniz kaldınız, değiştirdiniz, bozdunuz, bu farklı bir şey. İşte biz tasarıda, buraya açıklık getirdik . Bağlantılı olarak 244'te de bir açıklık getiriyoruz³¹⁵." gerekçesi ileri sürülmüştür.

³¹⁴ **Madde 243** - (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 hâlinde, 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.

³¹⁵ **KETİZMEN**, Bilişim Suçları sh:92'den naklen.

Bu da Avrupa Konseyi Siber Suç Sözleşmesi'ne paralel olarak, bu tarz suçların ancak kasten işlenebileceğinin bir örneği olarak göz önünde bulundurulmalıdır. Ancak unutmamak gerekir ki; Sözleşme sadece bu alandaki suçların ancak kasten işlenebileceğine işaret etmiş ve fakat gerekçede geçen “kasıtlı” ibaresinin kesin anlamının her devletin kendi iç hukuk yorumuna bırakıldığı belirtilmiştir.³¹⁶ Bu bakımdan mutlak suretle iç hukuk düzenlemelerinin dikkate alınması gerekmektedir.

Bir eylemin kasten işlenebilmesi için mutlak suretle iki unsurunun da gerçekleşmesi gerekmektedir. Bunlar bilme ve isteme unsurlarıdır. Kastın bilme unsuru “ fiilin işlendiği sırada” mevcut olmalıdır. Failin kasten hareket etmiş sayılabilmesi için kastın bilme unsurunun tipiklikte ön görülen bütün unsurları kapsamına alması gerekir. Kastın bilme unsuru hareketi ve hareketle netice arasında bulunması gereken nedensellik bağımlı da içermelidir³¹⁷. Kastın bulunması için suç tipinde yer alan objektif nitelikteki tüm unsurların fail tarafından bilinmesi yetmez; bunların istenmiş olması da gerekir. Kastın isteme unsuru her şeyden önce kasıtlı bir hareketle taksirli bir hareketi birbirinden ayırmaya yarar. Gerçekten taksirden farklı olarak kastta fail neticeyi istemektedir. Dolayısıyla kasıtlı bir eylemden bahsedebilmek için mutlak suretle bilmek ve istemek unsurlarının bir arada olmasını aramak gerekmektedir.³¹⁸

Avrupa Siber Suç Sözleşmesinin atfıyla 5237 sayılı TCK'de kastın nasıl düzenlendiğine kısaca bakılacak olursa, md. 21'in değerlendirilmesi gerekmektedir. Buna göre, suçun oluşması için kastın varlığı zorunludur. Bu ifadenin başka bir anlamı da şudur ki; kanunda özel olarak belirtilmediği sürece taksirle işlenen eylemden dolayı sorumluluk söz konusu değildir. Kanun koyucu aynı madde içinde kast ile neyi vurgulamaya çalıştığını da belirtmiştir. 21. maddenin birinci fıkrasında kast, suçun kanuni tanımındaki unsurların bilerek ve istenerek gerçekleştirilmesi olarak tanımlanmıştır. Dolayısıyla burada yukarıda ifade edildiği gibi kastın her iki unsuru da yani bilmek ve istemek unsuru da açıkça vurgulanmaktadır. Ancak kanun sistematığı içerisinde tehlikeli ikilemlere neden olması muhtemel bir eksiklik yer almaktadır. Şöyle ki; her ne kadar 21. maddede kastın varlığı için

³¹⁶ İÇEL, Avrupa Konseyi Siber Suç Sözleşmesi, sh: 8-9.

³¹⁷ ÖZTÜRK/ ERDEM, Uygulamalı Ceza Hukuku, sh: 196.

³¹⁸ ÖZTÜRK/ ERDEM, Uygulamalı Ceza Hukuku, sh: 197.

bilmek ve istemek unsurlarının her ikisi de aranırken hata müessesesinin düzenlendiği 30. maddenin birinci fıkrasında farklı bir düzenleme yer almaktadır.

TCK md. 30/1.'de “ *fiilin icrası sırasında suçun kanuni tanımındaki maddi unsurları bilmeyen kimse, kasten hareket etmiş olmaz*” diyerek kastın yokluğu açıklanırken, sadece bilme unsuru üzerinde durulmuş fakat isteme unsuruna değinilmemiştir. Doktrinde, hata kurumuna ilişkin hükümde bilmeyen bir kimsenin istemeyeceği düşünülerek 30/1. maddede sadece bilme unsurundan bahsetmek fakat isteme unsurundan bahsetmemek büyük bir eksik olarak yorumlanmıştır³¹⁹. Doktrinde aksi yönde düşünen yazarlar da mevcuttur. Örneğin, *Özgenç*'e göre, istemek kastın bir unsurunu oluşturmamaktadır. Kişi işlediği fiilin sonucunu öngörmüş ise, bunların gerçekleşmesini istemese bile, kasten hareket etmiş sayılır. Örneğin bir kişi bir fiili gerçekleştirmeye zorlanıyorsa, bunu neden olacağı neticelerin de farkında olacaktır. Her ne kadar bu fiili işlemeyi ve gerçekleşen neticeyi istemese de fail kasten hareket etmektedir. Bu nedenle, kast açısından isteme unsurundan söz edilmesi doğru değildir. Yazara göre, bu ayırım kastın bir kusurluluk şekli olarak kabulünün bir sonucudur³²⁰. Kastı hareketin bir parçası olarak gören *Koca/ Üzülmöz*'e göre ise, hareket ancak belli bir amaca yönelik olarak icra edilen iradi hareketler olduğu için hareketin bir vasfı olarak irade kastı oluşturur. Bunun dışında ayrıca kasta ait bir isteme unsurundan bahsedilmesi gerekmez.³²¹

Yine 30. maddenin dördüncü fıkrasında hukuki hata düzenlenmiştir. Buna göre 30. maddenin 4. fıkrasına göre “ *işlediği fiilin haksızlık oluşturduğu konusunda kaçınılmaz bir hataya düşen kişi cezalandırılmaz*”. Kişi işlediği fiilin hukukun kabul görmez bir davranış olduğunun bilincinde olmalıdır. İşlenen fiilin hukuken kabul görmez bir davranış oluşturduğu hususundaki hatanın kaçınılmaz olması durumunda kişi kusurlu sayılamaz. Hatanın kaçınılmaz olduğunun belirlenmesinde ise kişinin bilgi düzeyi, gördüğü eğitim, içinde bulunduğu sosyal ve kültürel çevre koşulları göz önünde bulundurulur³²². Bu düzenleme de eleştirilere tabi olmuştur. *Ünver* bu düzenleme ile hata ve hukuka aykırılık bilincinin

³¹⁹ Konu ile ilgili detaylı eleştiriler için bkz. **ÜNVER**, Yener, Yeni Türk Ceza Hukukunda Kusurluluk, in : CHD (Ed: Veli Özer ÖZBEK) Y:1, Sayı: 1, Ankara, 2006, sh: 37 vd.; benzer yönde görüşler ve “isteme” unsurunun gerekliliğine ilişkin teorik çözümler için ayrıca bkz **OZANSÜ**, Mehmet Cemil, Ceza Hukukunda Kasttan Doğan Sübjektif Sorumluluk, Ankara, 2007, sh: 126 v.d.

³²⁰ **ÖZGENÇ**, İzzet, Türk Ceza Hukuku – Genel Hükümler, 2. Baskı, Ankara, 2007, sh: 223 v.d.

³²¹ **KOCA**, Mahmut/ **ÜZÜLMEZ**, İlhan, Türk Ceza Hukuku Genel Hükümler, Ankara, 2008, sh: 168.

³²² TCK md. 30/4 kapsamında failin kişisel özelliklerinin esas alınmasının yaratacağı problemlere ilişkin görüş için bkz. **ÜNVER**, Yeni TCK'da Kusurluluk, sh: 54.

birbirleriyle karıştırıldığını, eksik olarak hatanın suça ilişkin olması değil haksızlığa ilişkin olarak düzenlenmesinin bu karışıklığa neden olduğunu dile getirmektedir³²³.

Nihayet Türk Ceza Kanununda kasta ilişkin düzenlemeler ile ilgili olası kasttan da bahsetmek gerecektir. Olası kast failin neticeyi öngörmüş olmasına rağmen aldırılmaması ,neticeyi göze almasıdır. *Özgenç* doğrudan kast ile olası kast arasındaki farkı ortaya koyarken bilme unsuru üzerinden hareket etmiştir. Buna göre kasten işlenebilen bir suç hem doğrudan kastla hem de olası kastla işlenebilir. Ancak maddi unsurda “bilerek”, “bildiği halde” veya “bilmesine rağmen” ifadeleri açıkça vurgulanmış ise burada artık sadece doğrudan kasttan bahsedilebilir. Bu durumlarda olası kast söz konusu olamaz³²⁴. Bu yaklaşım tarzı yukarıda da ifade edildiği gibi kastın sadece bilme unsurundan ibaret sayıldığı bir anlayış çerçevesinde bir takım çelişkileri de beraberinde getirebileceği kanaatindeyiz. Çünkü zaten kastın varlığı sadece bilme unsurunun söz konusu durumlarda geçerli ise, suçun bilerek işlenmesi açıkça ifade edilse de edilmese de doğrudan kastın temel unsuru konumundadır. O halde anılan ifadeler kullanılmadığında doğrudan kast ile olası kast hangi ölçüt esas alınmak suretiyle birbirinden ayrılacak, net bir biçimde ortaya konulmamıştır.

Fail olası kastta, “*olursa olsun, netice gerçekleşirse gerçekleşsin*” demektedir³²⁵. Bu onu bilinçli taksirden ayırır. *İçel*, olası kast ile bilinçli taksir ayrımını ortaya koyarken, failin kayıtsızlığı üzerinden hareket etmiştir. Yazara göre, bilinçli taksirde de fail sonuçları öngörmekte, fakat bunları istemediği gibi, bu sonuçların meydana gelmemesi için elinden

³²³ **ÖZGENÇ**, Ceza Hukuku, sh: 340.

³²⁴ **ÖZGENÇ**, Ceza Hukuku, sh: 238.

³²⁵ “*Sanığın olay günü akşamı tabanca ile etkili mesafeden cami çıkışı mağdura yönelik ateş etmesi sırasında mağdurun yanında bulunan üçüncü kişilerin de isabet alarak ölebileceklerini veya yaralanabileceklerini öngörmesi karşısında diz altından isabetle yaralanan diğer mağdura yönelik eylemin kastı neticenin belirleyeceği kuralı gereğince, olası kasıt ile silahla yaralama suçunu oluşturduğu anlaşıldığı halde suç vasfında hataya düşülerek yazılı şekilde öldürmeye teşebbüsten hüküm kurulması, isabetsizdir.*” (Yargıtay 1.CD, 05.07.2006, E: 2006/902 – K: 2006/2922, Kaynak: Kazancı İçtihat Programı – Online, Erişim Tarihi: 22.03.2009, Saat: 12:10)

“*Sanığın asıl hedef aldığı kişiye ateş ettiği sırada aynı otomobil içinde bulunan mağdurun da isabet alarak ölebileceğini ya da yaralanabileceğini öngörmesine rağmen, ateşlerine devam ederek mağduru yüz, sağ omuz ve sağ kalça bölgesinden yaraladığı anlaşıldığına göre, olası kastla yaralama suçundan cezalandırılması gerekir.*” (Yargıtay 1. CD, 31.03.2008, E: 2007/ 4914 – K: 2007/ 2475, Kaynak: Kazancı İçtihat Programı – Online, Erişim Tarihi: 22.03.2009, Saat: 12:15)

geleni yapmaktadır³²⁶. Başka bir anlatımla olası kasttaki kayıtsızlık ve önemsemezlik durumu bilinçli taksirde yoktur. Tam aksine bilinçli taksirde fail sonuçları önlemek için elinden geleni yapmaktadır. Doktrinde bu yaklaşım ortaya konulurken, kanun koyucunun getirdiği olası kast tanımını ise olası kastın bilinçli taksir kavramı ile karşımasına neden olmaktadır³²⁷. Gerçekten kanun bilinçli taksiri kişinin öngördüğü neticeyi istememesine karşın neticenin meydana gelmesi olarak tanımlamıştır. Halbuki olası kastta da fail neticeyi istememektedir. Ancak göze almaktadır. Bilinçli taksirde ise fail yine neticeyi öngörmekte, istememekte ve meydana gelmemesi için çaba göstermektedir. Ancak taksirden daha yoğun bir kusur çeşidi olduğu için failin cezası arttırılır. *Ünver* de olası kastın hatalı ve amacına aykırı olarak düzenlendiğini, bilinçli taksirle arasında hiçbir fark yaratılmadığını vurgulamıştır.³²⁸

Özellikle internet ortamında işlenebilen suçlarda karıştırılmaması gereken önemli bir husus da olası kast ile ikinci derece doğrudan kasttır. Bilindiği üzere failin hedefinin dışında kalan ikinci derece sonuçlar, asıl sonucun gerçekleşmesi bakımından zorunlu nitelikte ise, failin bu ikinci derece sonuçları da istediğinden hareketle ikinci derece doğrudan kastın varlığı kabul edilir. Özellikle Yargıtay'ın son yıllarda verdiği bazı kararlarda olası kastı, ikinci derece doğrudan kastın tanımı ile çerçevlendirdiği görülmektedir. Bu yönde hataların özellikle internet gibi teknolojik alt yapı sistemlerin kullanıcılarının, yeterli bilgi birikimi ve tecrübeye sahip olmadan giriştikleri eylemler bakımından etkili olabileceği düşünülebilir.

³²⁶ “Yaralama kastıyla hareket eden sanığın, ölüm sonucunu istememekle birlikte kalp rahatsızlığı olan maktulenin ölebileceğini öngördüğünün ve böylece bilinçli taksirle hareket ettiğinin anlaşılması karşısında, 5237 sayılı TCK.nun 22/3. maddesi delaletiyle 85. maddesi gereğince cezalandırılması yerine yazılı şekilde olayda uygulama yeri bulunmayan 87/4. madde ile uygulama yapılması usul ve yasaya aykırıdır.” (Yargıtay 1.CD, 22.05.2007, E: 2006/5796 – K: 2007/3947, Kaynak: Kazancı İçtihat Programı – Online, Erişim Tarihi: 22.03.2009, Saat: 12:15)

“Olay öncesi aldığı alkol nedeniyle araç kullanmamasına ilişkin uyarıları dinlemeyerek, gece vakti seyir halinde kaplamadan çıkarak banket üzerinde yürüyen yayalara çarpıp bir kişinin yaralanmasına iki kişinin de ölümüne sebebiyet veren ve olayda tam kusurlu olduğu anlaşılan sanık hakkında TCK.nun 45/3. maddesinde öngörülen bilinçli taksirin olduğu gözetilmeden, yazılı şekilde uygulama yapılmak suretiyle eksik ceza tayini, kanuna aykırıdır.” (Yargıtay 1.CD, 12.05.2005, E: 2005/1150 – K: 2007/2012, Kaynak: Kazancı İçtihat Programı – Online, Erişim Tarihi: 22.03.2009, Saat: 12:20)

“Kavga ortamında sanığın yumruk atması sonucu yere düşen maktulün, kendisinde bulunan kalp damar hastalığının olayın tesiri ve eforu ile aktif hale geçmesi sonucu gelişen solunum ve dolaşım yetmezliğinden öldüğü olayda, küçük bir yerleşim yeri olan köy ortamında sanığın, maktulün kalp hastası olduğunu bilip bilmediği detaylı bir şekilde araştırılarak sonucuna göre karar verilmelidir. Bilinmesi halinde 5237 sayılı TCK'nun 22, 23 ve 85. maddeleri kapsamında bilinçli taksir sonucu adam öldürme, aksi halde 5237 sayılı TCK'nun 86/2. maddesi aracılığıyla 85. maddeleri kapsamında sanığın hukuki durumunun değerlendirilmesi gerekir.” (Yargıtay 1.CD, 25.05.2006, E: 2006/894 – K: 2006/2130, Kaynak: Kazancı İçtihat Programı – Online, Erişim Tarihi: 22.03.2009, Saat: 12:25)

³²⁷ İÇEL, Ceza Hukuku, 190 v.d.

³²⁸ ÜNVER, Yeni TCK'de Kusurluluk, sh: 50.

Başka bir anlatımla her komutun neticesinin önceden kestirilmesi önemli bir bilgi birikimi ve tecrübeyi gerektirirken, toplumda her kesimin kullanabildiği bir teknoloji olarak internet teknolojisi, girilen eylemde manevi unsur olarak taksirden kasta uzanan yelpazede her türlü kusur çeşidinin kolaylıkla gerçekleştirilmesi ihtimalini mümkün kılmaktadır. Ancak sorun internet üzerinde gerçekleştirilen eylemlerde kusur çeşidinin tespitinin güç olmasında yatmaktadır. Örneğin bilgisayarda kayıtlı verilere zarar verici virüsleri barındırdığı kuvvetle muhtemel olan bir web sitesinden çocuk pornografisi içerikli veriyi başkasının bilgisayarına indiren bir kişinin eyleminde, kişinin çocuk pornografisi içerikli bir veriyi buldurması veya depo etmesi bakımından 5237 sayılı TCK md. 226 çerçevesinde mütehcenlik suçunu kasten işlediği noktasında bir sorun yoktur. Ancak kaynak web sitesinden çocuk pornografisi içerikli veri indirme sürecinde, söz konusu verinin depolandığı ve başkasına ait olan bilgisayardaki diğer verilere zarar verecek bir virüs veya kötücül yazılımın da bilgisayara yüklenmesi ve kayıtlı verileri kullanılamaz hale getirmesi durumunda manevi unsur bakımından nasıl bir tercih yapmak gerekecektir? Bu soruya verilecek yanıt kanaatimizce, kastın bilme unsuru ile isteme unsurunun da birlikte değerlendirilmesinde isabet olacağı neticesini ortaya koyacaktır.

Burada sadece internet aracılığıyla suç işleyen gerçek kişi fail bakımından manevi unsur üzerinde durulmuştur. Diğer internet sùjelerinin ceza sorumlulukları kapsamındaki deęerlendirmeleri daha sonra ilgili bölümde yapılacaktır. Geline bu noktada dikkatlerin toplanması gereken iki husus vardır. Birincisi Avrupa Siber Suç Sözleşmesinin atfıyla internet ortamında işlenebilen suçlarda kast seviyesinde kusurluluğun aranması dolayısıyla özellikle kastın bilme ve isteme unsurlarının aynı anda aranmasına özen gösterilmelidir Bu anlamda yukarıda da işaret edildiği üzere 21. maddenin birinci fıkrası ile 30. birinci fıkrası arasındaki unsurlara yönelik çelişki bir an önce giderilmelidir. Çünkü internet ortamında işlenebilen suçlarda bilmek kadar istemek de büyük öneme sahiptir ve hatta bu alanda olası kast ve bilinçli taksir kurumlarının dikkate alınması gerekliliği karşısında hatanın tespiti bakımından isteme unsuru daha da önem kazanmaktadır.

İkinci husus da olası kast kavramının netliğe kavuşturulması zorunluluğudur. Çünkü internette gerek içerik (açıklama ve yayma suçları) suçlarında, gerek müdahale (bilgisayar sabotajı, verilerin değiştirilmesi, ... v.b.) suçlarında gerekse de diğer suç alanlarında internetin sanal ortamda gizlilik ve anonimlik ilkesinin verdiği güvenle netice ön görülmesine rağmen eyleme devam etme iradesinin hâkim olması, olası kastın ortaya çıkma ihtimalini daha da güçlendirmektedir. Ancak hali hazırdaki durum ikinci derece doğrudan kast, olası

kast ve bilinçli taksir³²⁹ arasındaki çizginin muğlâklığı nedeniyle eylemin suç olmaktan çıkmasına dahi neden olabilecek tehlikeyi bünyesinde barındırmaktadır. Çünkü hatırlanacağı üzere Avrupa Konseyi Siber Suç Sözleşmesi bünyesindeki suçların ancak kasten işlenebileceğini ifade etmekte ve ulusal mevzuatlar da buna uyum sağlamaya çalışmaktadır. Fakat bir kast türü olan olası kast ile bir taksir türü olan bilinçli taksir birbirlerinden net bir biçimde ayrıldığı için bilinçli taksirin varlığının kabul edileceği bir durumda, taksirin özel olarak aranmadığı suç tipleri bakımından unsurları tamamlanmış bir suçtan bahsedilemeyecektir. Çünkü bilindiği üzere suç tipe uygun, kusurlu ve hukuka aykırı eylemdir. Böyle bir durumda kusurluluk unsuru oluşmadığı için ortada bir suç olmayacaktır.

4- İNTERNET ORTAMINDA İŞLENEN İÇERİK SUÇLARI BAKIMINDAN TCK MD. 26 ANLAMINDA HAKKIN KULLANILMASI HUKUKA UYGUNLUK NEDENİNİN ANLAMI

4.1.- Genel Açıklamalar

İnternet modern teknolojiler içerisinde toplum hayatını en yakından ve derinden etkilen teknoloji alanı olarak dikkat çekmektedir. Özellikle alt yapı itibariyle karmaşık bir mühendislik bilgisini barındıran bu teknoloji kullanıcıya sunulduğu haliyle herkes tarafından az ya da çok kullanılabilir. Bu kullanım her zaman doğrudan yasal amaçlara riayet neticesini doğurmamakta, yasal olmayan yollara da sapılmaktadır. Böyle bir sapma hiç şüphe yok ki hukuku devreye sokacaktır ve bu anlamda hukukun etkili silahı da ceza olacaktır. Bu nedenle ceza hukuku normlarının, diğer hukuk normlarının yeterli olmadığı noktada devreye girmesi prensip olarak kabul edilmektedir. Çünkü ceza hukuku kişi temel hak ve özgürlüklerine doğrudan müdahalenin en etkin bir biçimde gerçekleştiği alandır. Bu

³²⁹ Bu yelpaze içerisinde daha rahat ayırt edilebilme ihtimali olan kusur şeklinin bilinçli taksir olduğunu da ifade etmekte hiçbir akınca yoktur. Çünkü bir olayda bilinçli taksir belirlemesine gidilebilmesi için suçun taksirle işlenebilen bir suç olması gerekmektedir. Keza bu husus Yargıtay'ın şu kararında da açıkça ifade edilmektedir.

“1- 5237 Sayılı TCK.nun 22/3. maddesinde belirtilen bilinçli taksirin sadece taksirle işlenen suçlarda uygulanabileceği gözetilmeden, aynı kanununun 179/3. maddesinde düzenlenen kasten işlenen alkollün etkisiyle emniyetli bir şekilde araç sevk ve idare edemeyecek halde olmasına rağmen araç kullanarak trafik güvenliğini tehlikeye sokma suçunda uygulanarak sanık hakkında fazla ceza tayini,

2- 5237 sayılı TCK.nun 50 ve 51. maddesinde öngörülen nesnel ve öznel koşulları içermeyen "saniğin kusur oranı" gerekçesine dayanılarak sanık hakkında tayin edilen cezanın paraya çevrilmesine ve ertelenmesine yer olmadığına karar verilmesi, bozmayı gerektirmiştir.” (Yargıtay 2. CD, 22.2.2007, E: 2006/9904 – K: 2007/2721, Kaynak: Kazancı İçtihat Programı – Online, Erişim Tarihi: 22.03.2009, Saat: 12:40)

müdahalenin özgürlüğün esas alındığı bir sistemde son araç kullanılması bu çerçevede oldukça önemlidir.

Suç teşkil eden bir eylemin kanuni tipe uygun, kusurlu ve hukuka aykırı olması gerektiği düşünüldüğünde, bu üç ilkedden birinin gerçekleşmediği durumlarda hareket zarar neticesi bile doğurmuş olsa teknik anlamda suç kabul edilemeyecektir. Kişinin eylemi şayet bir özgürlük kullanımı çerçevesinde değerlendirilmekteyse, kişi meşru alanda kalmış sayılır ki, meşru olmayan alan da zaten suç alanıdır ve cezaya tabi tutulmaktadır. Bu değerlendirme sadece eyleyen veya eyleme maruz kalanlar için değil, kişilerin özgürlük kullanımlarının sınırların belirleyen yasa koyucu için de önem arz etmektedir. Çünkü getirilecek bir ceza düzenlemesi ile kişinin hareket özgürlüğü sınırlandırılmakta, sınırın aşıldığı noktada da cezai yaptırım öngörülmektedir. Ancak sınır içinde kaldığı takdirde eylem neticesi önem arz etmeksizin ceza hukuku anlamında meşru kabul edilmektedir. Bu tespiti biraz daha açmak ve internet ile ilişkilendirmek isabetli olacaktır.

Anatomik yapısı dikkate alındığında teknik anlamda suç, tipe uygunluk, hukuka aykırılık ve kusurluluk niteliklerine sahip bir eylemle ceza normunun ihlalidir³³⁰. Bir başka ifade ile, bir eylemin suç olarak değerlendirilebilmesi için mutlak suretle tipe uygun, kusurlu ve hukuka aykırı olması gerekmektedir. Bu unsurlardan sadece birinin olmaması dahi eylemin suç olma vasfını yitirmesi için yeterlidir. Çalışma konusu bakımından bu tespitin önemi, yukarıda verilen suç tanımı çerçevesinde hukuka aykırılığın tartışılması boyutunda kendini göstermektedir. Ancak öncelikle ceza hukukunun yapısal unsuru olarak hukuka aykırılığın kapsamı konusunda genel bir netliğin ortaya konulması gerekmektedir.

Doktrinde hukuka aykırılığın kapsamı bakımından iki farklı görüş mevcuttur. Bu görüşlerden birincisi suçun yapısal bir unsuru olan hukuka aykırılığı dar anlamda değerlendiren görüştür. Bu görüş taraftarlarına göre hukuka aykırılığı sadece ceza hukukuna aykırılık olarak anlamak gerekmektedir. Bu çerçevede hukuka aykırı eylemleri üç kategori altında değerlendirmektedirler. Birinci kategori ceza hukukuna uygun eylemlerdir. Bu kategoride yer alan eylemler ceza kanunlarınca yasaklanmamış ve uygulanmasında herhangi bir engel olmayan eylemlerdir. İkinci kategoride ise ceza hukukuna aykırı eylemler vardır. Bu eylemler ceza kanunlarınca gerçekleştirilmesi yasaklanmış eylemlerdir. Üçüncü grupta ise

³³⁰ İÇEL, Kayhan, Ceza Hukuku Genel Hükümler, 2. Kitap, Yenilenmiş 4. Baskı, İstanbul, 2007, sh: 15.

ceza hukuku bakımından önemsiz eylemler bulunmaktadır ki, bu eylemler ceza hukukunun düzenleme kapsamı dışında bulunan ve ceza hukukunu ilgilendirmeyen eylemlerdir.³³¹

Bizim de iştirak ettiğimiz ikinci görüş ise suçun yapısal unsuru olan hukuka aykırılığı sadece ceza hukukuna aykırılık şeklinde dar bir yoruma tabi tutmadan, sistematik bütünlük içerisinde tüm hukuk sistemine aykırılığı kapsayacak şekilde geniş yorumlayan görüştür.³³² Bu görüşü savunanlara göre hukuka aykırılık ya vardır ya da yoktur. Hukukun alt disiplinleri arasında her disipline münhasır bir hukuka aykırılık benimsemek sistemin bir bütün olarak işlemesine açık bir şekilde engel olacaktır. *İçel*, kanaatimizce de isabetli olarak, hukuka aykırılığı tüm hukuk düzeni nazarında birlik – bütünlük gösteren ve parçalanması olanaksız bir kavram olarak belirlerken bir eylemin belirlerken bir eylemin belirli bir hukuk dalı alanında hukuka uygun, başka bir hukuk dalı alanında hukuka aykırı sayılmasını bu hukuksal yapıya ve mantığa aykırı olarak kabul etmiştir.³³³ Yine *Özbek* de hukuka aykırılığı tipe uygun fiilin bütün hukuk düzeni ile çatışma içinde bulunması olarak kabul etmektedir.³³⁴

Öztürk/Erdem, *Lackner/Kühl*'e atıfta bulunmak suretiyle hukuka aykırılığı bütün hukuk sistemine aykırılık olarak kabul ettiklerini ortaya koyarken ayrıca hukuka aykırılık ile haksızlık kavramlarının farklı içeriklere sahip oldukları üzerinde durmaktadırlar.³³⁵ Yazarlara göre hukuka aykırılık davranış ile norma arasındaki bir çelişkiyi ifade eder ve bu nedenle derecelendirilemez, ancak haksızlık davranış ile gerçekleştirilen ve hukukun maddi değerler düzenin onaylamadığı gerek nicelik gerekse nitelik olarak derecelendirilebilir bir değersizliği ifade etmektedir.³³⁶ Hukuka aykırılığın kapsamı itibariyle aynı görüşte olan *Koca* da hukuka aykırılık ile haksızlık kavramlarının iki ayrı kavram olduğu üzerinde durmuştur. Alman doktrinine atıfta bulunan yazar, hukuka aykırılığı tipe uygun hareketin bir özelliği, yani ceza hukukunun emir ve yasaklarına karşı gelmek olarak tanımlarken haksızlığın ise, tipe uygun ve

³³¹ **İÇEL**, Ceza Hukuku, sh: 89.

³³² **KOCA**, Mahmut, YTCK'da Hukuka Uygunluk Nedenleri, CHD (Ed: Veli Özer ÖZBEK), Y:1, S: 1, Ankara, 2006, sh: 116.

³³³ **İÇEL**, Ceza Hukuku, sh: 90- 91.

³³⁴ **ÖZBEK**, Veli Özer, TCK İzmir Şerhi, 3. Baskı, Ankara, 2006, sh: 151.

³³⁵ **ÖZTÜRK/ ERDEM**, Uygulamalı Ceza Hukuku, sh: 146. Benzer yönde düşünceler için bkz. **DEMİRBAŞ**, Timur, Ceza Hukuku Genel Hükümler, 5. Baskı, Ankara, 2007, sh: 243.

³³⁶ **ÖZTÜRK/ ERDEM**, Uygulamalı Ceza Hukuku, sh: 146- 147.

hukuka aykırı fiilin bizatihi kendisini, hukuka aykırılık değerlendirmesinin konusunu onun değer yüküyle birlikte ifade ettiğini dile getirmiştir.³³⁷

Hukuka aykırılık unsurunun kapsamı konusunda yukarıda yapılan açıklamalar göz önünde bulundurulduğunda, kanuni tipe uygun ve kusurlu bir hareket, normlar hiyerarşisi bağlamında tüm hukuk sistemi için geçerli olan anayasal bir temel hak ve özgürlük kullanımı olarak değerlendirilebiliyorsa veya anayasa hukuku tekniği ile ifade edilecek olursa bir temel hak ve özgürlüğün koruma alanı (*Schutzbereich der Grundrechte*) kapsamında düşünülüyorsa bu hareket hukuka aykırı sayılmayacağından mütevellit teknik anlamda bir “suç”a da vücut vermeyecektir. O halde bir hareketin hukuka aykırılığının tespiti bakımından öncelikli olarak ele alınması gereken değerlendirme kriterini, o hareketin anayasal bir temel hak ve özgürlük kullanımı kapsamında herhangi temel hakkın koruma alanı içinde yer alıp almadığının ortaya konulması oluşturmaktadır.

Bu değerlendirmeler ışığında TCK md. 26/1’de düzenlenen “*Hakkın Kullanılması Hukuka Uygunluk Nedeni*” ele alınacak olursa, bir kişinin anayasal güvence altına alınmış bir temel hak ve özgürlüğünü kullanmasıyla ortaya çıkacak kanuni tipe uygun ve kusurlu eylem, hukuka aykırılık unsuru gerçekleşmediği için suç olarak değer kazanmayacaktır. Bu konuda doktrinde bir temel hak ve özgürlük kullanımının hangi şartlar altında TCK md. 26/1 hükmüne göre değerlendirilebileceği üzerinde durulmuştur. *Özgenç*’e göre, hak kullanımının bir hukuka uygunluk nedeni bağlamında kabul edilebilmesi için öncelikle, kişiye o hukuk düzenince tanınmış bir subjektif hakkın varlığı gerekmektedir. Bunun dışında ikinci olarak, - birinci koşulun zorunlu bir sonucu denilebilecek – hukuk düzenince kişiye tanınmış olan subjektif hakkın sınırları dahilinde kullanılması gerekmektedir. Yine kullanılan hakkın karakteristik özelliği olarak, bu hakkın kişi tarafından hiçbir merciinin aracılığına gerek kalmaksızın doğrudan doğruya kullanılabilir bir hak olması gerekmektedir.³³⁸ *İçel* de *Özgenç*’le aynı koşulları kabul etmiştir.³³⁹ *Özbek* ise, *Özgenç*’in ortaya koyduğu koşullara ek olarak hakkın kullanılması (icrası) ve yöneldiği suç arasında bir nedensellik bağının varlığını ararken *Özgenç*’te “hakkın sınırları dâhilinde kullanılması” koşuluna paralel olarak “hakkın kötüye kullanılmaması” koşulunu kabul etmiştir.³⁴⁰

³³⁷ KOCA, Hukuka Uygunluk Nedenleri, sh: 116.

³³⁸ ÖZGENÇ, İzzet, Türk Ceza Hukuku Genel Hükümler, 2. Baskı, Ankara, 2007, sh: 281.

³³⁹ İÇEL, Ceza Hukuku, sh: 140- 141.

Görüldüğü üzere TCK md. 26/1’de düzenlenen hakkın kullanılması hukuka uygunluk nedeninin hangi koşullar altında işletilebileceğine yönelik olarak doktrinde herhangi bir fikir ayrılığına rastlanmamaktadır. Genel itibariyle, kişi tarafından kullanılacak hakkın anayasal güvence altına alınmış olması, hakkın belirlenen sınırlar içinde kullanılması veya başka bir ifade ile kötüye kullanılmaması, söz konusu hakkın kişi tarafından hiçbir merciin müdahalesi olmaksızın kullanılabilir olması aranmaktadır. *Kanaatimizce*, doktrinde üzerinde hem fikir olunan bu koşulların en azından kanunun gerekçesinde de yer alması isabetli olurdu. Çünkü uygulamada bir eylemin herhangi bir hak kullanımı dahilinde kalıp kalmadığına ilişkin değerlendirme problemleriyle karşılaşılabilme ihtimali mevcuttur. Son olarak doktrinde kimi yazarlar tarafından hakkın kullanılması durumları başlığı altında bir takım hak kategorilerine yer verilmiştir.³⁴¹ Kanunun düzenlemesi ve yukarıdaki açıklamalar referans alındığında, bu tarz belirlemelere sınırlayıcı bir nitelik taşımaması nedeniyle ayrıca yer verilmeyip genel değerlendirmelerin bu kategorilere de yansıtılması gerektiği söylenmekle yetinilecektir.

Günümüzde internet ortamında işlenen suçlar bakımından da her ne kadar modern ceza hukukunun temel eğilimleri çerçevesinde güvenlik lehine bir yaklaşımla suç haline getirme iradesi söz konusu olsa da, internet kullanımı ile ilişkili olan temel hak ve özgürlüklerin sınırları ve kapsamı isabetli bir şekilde ortaya konulursa hem kanun koyucu inisiyatifi olması gereken çizgiye yönlendirilir hem de kişilerin hareket serbestisine olması gereken sınırlandırmalar ölçülü bir biçime gerçekleştirilir. Bu anlamda internet aracılığıyla işlenen suçların, temelinde bir özgürlük problemi kaynağında internette hareket serbestisine getirilen optimum sınırlandırmalar ile birlikte düşünülmesi gerektiği kanaatindeyiz. Hiç şüphe yok ki internet kullanımı düşünce özgürlüğünden sanat özgürlüğüne, özel yaşamın gizliliği hakkından fikri mülkiyet hakkına kadar birçok temel hak ve özgürlük kategorisini ilgilendirmektedir. Bu temel hak ve özgürlüklerin tek tek internet açısından ele alınması gerekmektedir. Ancak bu bölümde ceza hukuku perspektifinden internet kullanımını doğrudan ilgilendiren ve 5237 sayılı TCK md. 26’de düzenlenen bir hakkın kullanılması

³⁴⁰ **ÖZBEK**, İzmir Şerhi, sh: 365. Yazar bu tespitine örnek olarak Yargıtay’ın şu kararını göstermektedir.

“ Öğretmenlerin öğrenciler üzerinde eğitim içi disiplinin sağlanması yönünde terbiye ve itaat ettirme hakları bulunmaktadır. Ancak, bu hak disiplin cezası vermek ile bedensel zarara yol açmayacak şekilde örneğin kulak tutmak, tek ayak üzerinde durdurmak gibi davranış biçimleriyle sınırlı olup hiçbir zaman etkili eylemde bulunmayı kapsamaz. O halde öğretmenlerin terbiye hakkını kullanmaları onlara öğrenciyi dövme hakkı veremeyeceğinden, somut olayda mağdureye cetvelle vuran sanığın etkili eylem kastının olmadığından söz etmek olanaksızdır.” (Yargıtay CGK., 22.02.2000, 2000/-11, 2000/30, Kaynak: www.kazanci.com.tr)

³⁴¹ Örnek olarak bkz. **ÖZTÜRK/ ERDEM**, Uygulamalı Ceza Hukuku., 167 v.d.: **DEMİRBAŞ**, Ceza Hukuku, sh: 284 v.d.

bağlamında ele alınabilecek üç temel hak ve özgürlük çerçevesinden bakılacaktır. Bunlar düşünce özgürlüğü, ifade özgürlüğü ve haberleşme özgürlüğüdür.

Son olarak kanaatimizce bir noktanın daha altını çizmekte fayda vardır. Bir eylemin herhangi bir temel hak ve özgürlüğün koruma alanında yer alıp almadığının tartışılabilmesi için mutlak suretle Anayasanın 90. maddesinin daima göz önünde bulundurulması gerekmektedir. Çünkü md. 90 hükmünce usulüne uygun olarak kabul edilmiş ve bir temel hak ve özgürlüğü düzenleyen uluslar arası antlaşma hükümleri, iç hukukta aynı konuyu düzenleyen bir başka hükümle çatışmaları durumunda öncelikli olarak uygulanma imtiyazı sahiptir. Dolayısıyla bir hakkın usulüne göre kullanılıp kullanılmadığının tespitinde yukarıda verilen iki şarttan ikincisi yani verilen hakkın sınırlar içinde kullanılması durumu bu anayasa hükmü dikkate alınarak hareket edilmek durumundadır. Bu nedenle aşağıda sadece ilgili temel hak ve özgürlüklerin ulusal düzenlerle belirlenmiş sınırları değil aynı zamanda uluslar arası sözleşmelerle belirlenmiş çerçevesi de konuyla ilintisi ölçüsünde aktarılacaktır.

4.2.- Ceza Hukuku Bağlamında İnternetin Bazı Temel Hak Ve Özgürlüklerle İlişkisi

4.2.1.- Düşünce ve İfade Özgürlüğü

İnternet kullanımı bakımından en temel özgürlük alanlarının düşünce ve ifade özgürlüğü olduğu kanaatini taşımaktayız. Çünkü düşünce ifade özgürlüğü yaygın bir kitle ve iletişim aracı olan internet için diğer tüm özgürlük alanlarının başlangıcı niteliğindedir. Hatta *Ökçesiz, Kant*'tan alıntıladığı bir deyimle³⁴² düşünce özgürlüğünü bütün özgürlüklerin kalkamı olduğunu savunurken kamusal alanın örgütlenmesinde ve korunmasında karşılanması gereken çok ivedi bir gereksinim olarak bu üstünlüğünü sürekli duyumsattığını dile getirir.

“ *Toplumsal trafiğin işlerlik ve meşruluk düzeni olarak “temel insan hakları ve özgürlükleri pozitif hukuk yapısı”nın temel postulası olan “insan onuru”nun burada*

³⁴² “*Die Freiheit der Feder ist das einzige Palladium der Volksrechte (Kalemin özgürlüğü kamusal hakların yegane kalkandır)*”, **KANT**, Immanuel, Gemeinpruch, AA VIII, sh: 352; b.y.: Heiner Bielefeldt, Philosophie der Menschenrechte. Grundlagen eines weltweiten Freiheitsethos, Darmstadt, 1998, sh: 162 **ÖKÇESİZ**, Hayrettin, Düşüncenin Özgürlüğü Üzerine Düşünceler, in: HFSA- 6 (Der:Hayrettin ÖKÇESİZ), İstanbul, 2003, sh:30'dan naklen

*benimsediğim “ düşünmek” ile olan ilişkisinden düşünce özgürlüğünün kamusal alanın kurulmasında ve korunmasında taşıdığı kaynaksallık değeri çok açık bir biçimde belirir.”*³⁴³

İfade özgürlüğünün de genel anlamda düşünceyi açıklama özgürlüğü olarak kabulü³⁴⁴ bu anlamda bu iki özgürlük alanı arasındaki sıkı ilişkiyi ortaya koymaktadır. Öyle ki, *Lampe* ifade özgürlüğü ve düşünce özgürlüğü arasındaki ilişkiyi açıklarken her iki özgürlük alanının da insanın özüne ait olduğu belirtmiş ve bu iki özgürlük alanından hangi birine bir müdahale gerçekleşirse diğerinin zedeleneceğini ifade etmiştir.³⁴⁵ Burada öncelikle her iki özgürlük alanının temel yapılarını anayasal düzenlemeleri referans olarak ortaya koyulacak ardından bu özgürlük alanlarının hangi noktalarıyla interneti ilgilendirdiği üzerinde durulacaktır.

4.2.1.1.- Düşünce Özgürlüğü

Tüm özgürlüklerin hamisi ve kamusal alanın kurucu ögesi olan düşünce özgürlüğü inansın serbestçe düşünme ve bilgilere ulaşabilmesi, edindiği düşünce kanaatlerden dolayı kınanmaması ve bunları tek başına veya başkaları ile birlikte çeşitli yollarla serbestçe açılabilmesi, savunabilmesi, başkalarına aktarılabilmesi ve yayılabilmesi anlamına gelmektedir.³⁴⁶ *Lampe*'ye göre düşünmek insanın iç dünyasında meydana gelen, kimseye zarar vermeyen, dolayısıyla da toplumsal kurallarla sınırlandırılmayan bir süreçtir.³⁴⁷ *Kuçuradi* ise “*düşünce özgürlüğü*”nü kavramsallaştırmak için “*düşünce*” terimini de açıklığa kavuşturmak gerektiğini savunmaktadır. “*Düşünce*” terimi düşünme etkinliğinin çok çeşitli ürünlerini- fikirleri, anlayışları, kanaatleri, inançları, gereklilik önermelerini... - kapsar³⁴⁸.

³⁴³ ÖKÇESİZ, *Düşüncenin Özgürlüğü*, sh: 30.

³⁴⁴ Genel anlamda ifade özgürlüğü düşünceyi açıklama özgürlüğü olarak kabul görse dahi bizim de iştirak ettiğimiz üzere ifade özgürlüğünü düşünceyi açıklama özgürlüğü ile özdeş kabul etmemek gerekir. Çünkü ifade özgürlüğü düşünceyi açıklama özgürlüğünü ve düşünce olmayan duygu açıklamalarının da kapsar. Bu görüşün detayları için bkz. CAN, Osman, *Anayasa Değişiklikleri ve Düşünceleri Açıklama Özgürlüğü*, www.anayasa.gov.tr/eskisite/anyarg19/can.pdf (Erişim Tarihi: 18.09.2007).

³⁴⁵ *Lampe* bu yaklaşımını şöyle ifade etmiştir. “ *Bir insanı, kanaatini ifade etmekten alı koyan her kimse, o insanın düşüncesini öldürür! Dolayısıyla ifade özgürlüğü düşünce özgürlüğü gibi insan haklarından biridir. Alman Anayasası, herkese kanaatini sözlü, yazılı ve imgelerle ifade etme, yaygınlaştırma ve herkese açık olan kaynaklardan engellenmeden bilgi edinme hakkını vermiştir.*”. Değerlendirmenin ayrıntıları için bkz. LAMPE, Ernst- Joachim, *Düşünce Özgürlüğü, İfade Özgürlüğü, Demokrasi* (Çev: Nihat ÜLNER), in: *Düşünce Özgürlüğü* (Der: Hayrettin ÖKÇESİZ), İstanbul, 1998, sh: 128.

³⁴⁶ KABOĞLU, İbrahim, *Özgürlükler Hukuku*, 4. Baskı, 1998 sh: 191

³⁴⁷ LAMPE, *İfade Özgürlüğü*, sh: 128

Düşünce özgürlüğü sadece devletin müdahalelerine karşı korunan bireysel bir hak alanını güvence altına almakla kalmaz; aynı zamanda demokratik bir devlet düzenin de ön şartını oluşturur. Düşünce özgürlüğü, hem demokratik yönetimin hem de kişiliğin bütün değişik açılarının dile getirilmesinin de şartıdır. Başka bir deyişle bu özgürlük insan kişiliğinin toplumu içindeki en dolaysız ifadesi olup demokratik düzen bakımından da kurucu nitelik taşır.³⁴⁹ Nitekim devlet gibi düşünmeme özgürlüğünü, kurulu düzeni sorgulamayı, gerektiğinde kınamayı, mahkum etmeyi de içeren bir özgürlük olarak düşünce özgürlüğünün demokratik bir sistemin kurucu unsuru ve zorunlu bir sonucu olduğu yönünde bir şüphe yoktur. *Selçuk* bu düşünceyi bir adım daha öteye götürerek düşünce özgürlüğü ile insan onuru arasındaki ilişkiyi şöyle kurmaktadır.

*“ İnsan onuru bütün çağlar için geçerli bir değerdir. İnsan hakkının çiğnenmesi ise, insanın maddi ve manevi varlığını geliştirme koşulu olan düşünce özgürlüğünün çiğnenmesi, son çözümlenmede, insanı insan kılan onurun örülenmesi demektir. Zira düşünmek, düşünce üretmek insanı insan kılan etkinliktir. Onur amaç, düşünce özgürlüğü araçtır.”*³⁵⁰

Ökçesiz de düşünce özgürlüğünün kapsamı açısından “düşünce” kavramının önemi üzerinde durmaktadır. Yazara göre, bir düşüncenin kendi özgürlüğünde gerektiği gibi korunması , ancak onun düşünce olmayan şeylerden ayrılmasına bağlıdır. Bu açıdan düşünce her şeyden önce yanlıştır özelliğe sahip olmak durumundadır³⁵¹. Dilsel bir ifade olarak düşünceyi açıklama ile düşünce olmayanları açıklama arasında da bir ilişki kuran *Ökçesiz*, düşünceyi bildirim kipindeki ifadeler olarak görürken, düşünce dışındaki tüm ifadelerin ise dilek kipinde dile getirildiğini ortaya koymaktadır. Bu noktada düşünceyi açıklama özgürlüğü ile ifade özgürlüğü ilişkisine değinen yazar sonuç olarak su görüşü ortaya koymuştur.

“... Literatürde sözü edilen sınırlama ölçütleri düşünce dışı öğelerin açıklanmasında, arzu edilen sayıda ve arzu edilen kombinasyonlarla ulusal hukuka alınabilir. Ancak insan

³⁴⁸ *Kuçuradi*'ye göre “düşünce” teriminin tek kapsamadığı ürün bilgilerdir. Çünkü bilgi önermelerinin, onları ortaya koyandan bağımsız bir nesnesi vardır – bu nesnenin varlıksal özelliği ne olursa olsun. Dolayısıyla bilgi önermeleri, çeşitli yollardan doğrulanabilir – yanlıştır olabilirler. Oysa kanaatler ve inançlar kişiseldir ve onları taşıyana bağlıdır. Değerlendirmenin ayrıntıları için bkz. **KUÇURADI**, İoanna, *Düşünce Özgürlüğü: Nedir Acaba?*, in: *Düşünce Özgürlüğü* (Der: Hayrettin ÖKÇESİZ), İstanbul, 1998, sh: 24.

³⁴⁹ **SANCAR**, Türkan Yalçın, Ceza Hukuku – Politika İlişkisi ve TCK'nın 301. maddesi Bağlamında Düşünce Özgürlüğü Sorunu, in: HFSa Sayı – 15, İstanbul, 2006, sh: 107, 108.

³⁵⁰ **SELÇUK**, Sami, *Düşün Özgürlüğü*, in: HFSa Sayı – 12, İstanbul, 2005, sh: 135.

³⁵¹ **ÖKÇESİZ**, *Düşüncenin Özgürlüğü*, sh: 31.

onurunun bu denli temeli sayabileceğimiz düşünceyi, açıklanmasında neredeyse mutlak bir özgürlüğe doğru korumak arzusu, insanın öz değerine olan inancımızdan kaynaklanır.”³⁵²

İşte bu denli önem atfedilen düşünce özgürlüğü de gerek ulusal gerekse uluslar arası düzlemde ayrıntılı olarak düzenlenmiştir.

Ulusal hukuk düzeni bakımından düşünce özgürlüğüne ilişkin düzenlemeyi Anayasanın 25. maddesinde görmekteyiz.³⁵³ Madde metninde düşünce ile kanaat arasında bir ayrıma gidildiği dikkati çekmektedir. Buradan hareketle bu madde kapsamında dikkate alınan şeyin hangi koşullarda düşünce hangi koşullarda kanaat olduğu sorunu değerlendirilecek olursa bu konuda *Can*'ın tespitinin yerinde olduğunu söylemek gerekir. *Can* düşünceyi süreçsel bir etkinliğin ürünü olarak görmektedir.³⁵⁴ Bu süreçsel etkiliği yani düşünme etkinliğinin gerçekleşebilmesi için mutlak suretle dışarıdan bireye bir bilgi akışının gerçekleşmesi, bireyin de edinmiş olduğu bilgileri içsel bir muhakemeye tabi tutması ve diğer bilgilerle karşılaştırarak sistematize etmesi neticesinde doğrulanıp yanlışlanabilen ve fakat her halükarda temellendirilebilen bir bilgi ortaya çıkmaktadır. Bu süreç sonunda ortaya çıkan bu bilgi düşünce olarak anlam kazanır³⁵⁵.

Maddenin ikinci fıkrasında mutlak bir güvence getirilerek hiç kimsenin hangi sebeple olursa olsun düşünce ve kanaatlerini açıklamaya zorlanamayacağı, beslediği düşünce ve kanaatlerden ötürü kınanamayacağı vurgulanmıştır. Bu düzenlemenin Anayasanın 15. maddesinin ikinci fıkrasına³⁵⁶ gönderme yaptığı ve birinci fıkrada düzenlenen olağanüstü hal,

³⁵² **ÖKÇESİZ**, Düşüncenin Özgürlüğü, sh:31.

³⁵³ **MADDE 25.** – (1) Herkes, düşünce ve kanaat hürriyetine sahiptir. (2) Her ne sebep ve amaçla olursa olsun kimse, düşünce ve kanaatlerini açıklamaya zorlanamaz; düşünce ve kanaatleri sebebiyle kınanamaz ve suçlanamaz.

³⁵⁴ **CAN**, Osman, Düşünceyi Açıklama Özgürlüğü Anayasal Sınırlar Açısından Neler Değişti?, <http://ogrenci.hacettepe.edu.tr/~b0122202/Inetpub/wwwroot/hukuk/anayasahukuk/dusunceyi%20Aciklama%20ozgurugu.htm> (Erişim Tarihi: 18.09.2007)

³⁵⁵ **CAN**, Osman, Düşünceyi Açıklama Özgürlüğü Anayasal Sınırlar Açısından Neler Değişti?, <http://ogrenci.hacettepe.edu.tr/~b0122202/Inetpub/wwwroot/hukuk/anayasahukuk/dusunceyi%20Aciklama%20ozgurugu.htm> (Erişim Tarihi: 18.09.2007)

³⁵⁶ **MADDE 15.** – Savaş, seferberlik, sıkıyönetim veya olağanüstü hallerde, milletlerarası hukuktan doğan yükümlülükler ihlâl edilmemek kaydıyla, durumun gerektirdiği ölçüde temel hak ve hürriyetlerin kullanılması kısmen veya tamamen durdurulabilir veya bunlar için Anayasada öngörülen güvencelere aykırı tedbirler alınabilir.

sıkıyönetim ve savaş halinde dahi bu temel hak ve özgürlük alanına müdahalede bulunulamayacağı düzenlenmiştir. Olağan dönemde ise düşünce özgürlüğünün kullanımı ve sınırlandırılması ise Anayasanın 13. ve 14. maddelerinde düzenlenmiştir. Buna göre Anayasanın 14. maddesi³⁵⁷ hükmüncü düşünce özgürlüğü Devletin ülkesi ve milletiyle bölünmez bütünlüğünü bozmayı ve insan haklarına dayanan demokratik ve lâik Cumhuriyeti ortadan kaldırmayı amaçlayan faaliyetler biçiminde kullanılmayacağı gibi Devlete veya kişilere, Anayasayla tanınan temel hak ve hürriyetlerin yok edilmesini veya Anayasada belirtilenden daha geniş şekilde sınırlandırılmasını amaçlayan bir faaliyette bulunmayı mümkün kılacak şekilde yorumlanamaz. Düşünce özgürlüğünün hangi hallerde sınırlamaya tabi tutulacağına ilişkin Anayasanın 13. maddesi³⁵⁸ bir takım ölçütler vermiştir. Bunlar sınırlamanın Anayasanın sözüne ve ruhuna, demokratik toplum düzeninin ve lâik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamayacağı, ancak kanunla yapılabileceği ve ancak Anayasada belirtilen sebeplerle öze dokunmadan gerçekleştirilebileceğidir.

Düşünce özgürlüğünün uluslar arası platformda nasıl düzenlendiği konusuna gelindiğinde öncelikle AİHS. 9. maddesi ile karşılaşılmaktadır.³⁵⁹ Bu madde düşünce özgürlüğü ile birlikte din ve vicdan özgürlüğünü de güvenceye almaktadır. Ancak maddenin

(Değişik: 7.5.2004-5170/2 md.)Birinci fıkrada belirlenen durumlarda da, savaş hukukuna uygun fiiller sonucu meydana gelen ölümler dışında, kişinin yaşama hakkına, maddî ve manevî varlığının bütünlüğüne dokunulamaz; kimse din, vicdan, düşünce ve kanaatlerini açıklamaya zorlanamaz ve bunlardan dolayı suçlanamaz; suç ve cezalar geçmişe yürütülemez; suçluluğu mahkeme kararı ile saptanıncaya kadar kimse suçlu sayılamaz.

³⁵⁷ **MADDE 14.** – (Değişik: 3.10.2001-4709/3 md.) Anayasada yer alan hak ve hürriyetlerden hiçbiri, Devletin ülkesi ve milletiyle bölünmez bütünlüğünü bozmayı ve insan haklarına dayanan demokratik ve lâik Cumhuriyeti ortadan kaldırmayı amaçlayan faaliyetler biçiminde kullanılamaz.

Anayasa hükümlerinden hiçbiri, Devlete veya kişilere, Anayasayla tanınan temel hak ve hürriyetlerin yok edilmesini veya Anayasada belirtilenden daha geniş şekilde sınırlandırılmasını amaçlayan bir faaliyette bulunmayı mümkün kılacak şekilde yorumlanamaz.

Bu hükümlere aykırı faaliyette bulunanlar hakkında uygulanacak müeyyideler, kanunla düzenlenir.

³⁵⁸ **MADDE 13.** – (Değişik: 3.10.2001-4709/2 md.) Temel hak ve hürriyetler, özlerine dokunulmaksızın yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabilir. Bu sınırlamalar, Anayasanın sözüne ve ruhuna, demokratik toplum düzeninin ve lâik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamaz.

³⁵⁹ **Madde 9** - Düşünce, vicdan ve din özgürlüğü

1. Herkes düşünce, vicdan ve din özgürlüğüne sahiptir. Bu hak, din veya inanç değiştirme özgürlüğü ile tek başına veya topluca, açıkça veya özel tarzda ibadet, öğretim, uygulama ve ayin yapmak suretiyle dinini veya inancını açıklama özgürlüğünü de içerir.

2. Din veya inancını açıklama özgürlüğü, ancak kamu güvenliğinin, kamu düzeninin, genel sağlığın veya ahlakın, ya da başkalarının hak ve özgürlüklerinin korunması için demokratik bir toplumda zorunlu tedbirlerle ve yasayla sınırlanabilir.

düzenleniş tekniği dikkate alındığı zaman düşünce özgürlüğünün aynı maddede düzenlenmesine rağmen din ve vicdan özgürlüğünden daha ayrıcalıklı bir konuma yerleştirildiği görülmektedir. Şöyle ki, maddenin birinci fıkrası düşünce, din ve vicdan özgürlüğünü güvenceye alırken ikinci fıkrada din ve vicdan özgürlüğünün kullanımı bakımından bir takım sınırlamalar getirmiştir. Fakat aynı sınırlamalar düşünce özgürlüğü bakımından getirilmemiştir. Düşünce özgürlüğü bu anlamda mutlak bir güvenceye alınmıştır.³⁶⁰

Her iki düzenlemeden de anlaşılacağı üzere düşünce özgürlüğü içsel bir işlem olup *forum internum* safhasının bir görünümü olarak anlam taşır. Bu nedenle hiçbir sınırlamaya ve devlet müdahalesine elverişli değildir. *Can* bu yönde bir sınırlama ve sair müdahalenin gerçekleşmesi durumunda insan onurunu zedeleyici uygulamaların söz konusu olacağını savunmaktadır. Düşünce özgürlüğü *forum internum* safhasında mutlak bir güvenceyle koruma altına alınmış olmasına karşın, *forum internum* safhasında olgunlaşan düşüncenin *forum externum* safhasına geçişi ile yani dış dünyaya bu düşüncenin paylaşılması ile birlikte artık dar anlamda düşünceyi açıklama geniş anlamda ifade özgürlüğünün kapsamında değerlendirilmesi gerekir.³⁶¹

4.2.1.2.- İfade Özgürlüğü

Her şeyden önce şunun dile getirilmesi gerekmektedir ki, düşünce özgürlüğü ile düşünceyi açıklama özgürlüğü aynı olmamakla birlikte ifade özgürlüğünü de düşünceyi açıklama özgürlüğüne indirgemek oldukça yanlıştır. Çünkü ifade özgürlüğü düşünce olmayan

³⁶⁰ Avrupa'da Düşünce Özgürlüğü – Avrupa İnsan Hakları Sözleşmesinin 10. Maddesine İlişkin İçtihatlar, T.C. Başbakanlık Bası – Yayın ve Enformasyon Genel Müdürlüğü, http://www.byegm.gov.tr/YAYINLARIMIZ/kitaplar/avrupa/bolum_1.htm (Erişim Tarihi: 18.09.2007). Anayasa Mahkemesi de 08.04.1963 tarih ve E. 1963/16, K. 1963/83 sayılı kararında bu noktaya işaret etmektedir. “ *Düşünce ve kanat hürriyeti insanların en tabii haklarından ve herkes istediği gibi düşünmekte, istediği fikre inanmakta serbesttir. Kişinin iç alemi kanunun her çeşit müdahalesinin dışındadır. Ancak, kişinin iç alanında kaldığı sürece mutlak ve sınırsız olan düşünce ve kanaat hürriyeti, toplum hayatını ilgilendirdiği andan itibaren hukukun ve kanunun sahasına girer ve toplumsal yaşayışın gerektirdiği bazı kayıtlamalara bağlanabilir... insanın iç hayatı bakımından mutlak ve sınırsız olan düşünce ve kanaat hürriyetinin, söz, yazı, resim ve saire gibi çeşitli vasıtalarla açığa vurulurken toplumsal yaşayışın sürekliliği (devam ve beka) sağlanmak için belli esaslara ve kurallara bağlanmak suretiyle kayıtlanmasını zorunlu kılar.*” Kararın tam metni için bkz. AYMD, Sayı – 1, 2. Baskı, Ankara, 1992, sh: 199 - 200

³⁶¹ Detaylı bilgi için bkz. CAN, Osman, Düşünceyi Açıklama Özgürlüğü Anayasal Sınırlar Açısından Neler Değiştirdi?, <http://ogrenci.hacettepe.edu.tr/~b0122202/Inetpub/wwwroot/hukuk/anayasahukuk/dusunceyi%20Aciklama%20ozgurlugu.htm> (Erişim Tarihi: 18.09.2007)

şeylerin de açıklanmasını güvence alan bir özgürlük alanıdır.³⁶² Bu bağlamda ifade özgürlüğü düşünceyi açıklama özgürlüğünü de kapsar ancak salt düşünceyi açıklama özgürlüğünden ibaret değildir. Burada ifade özgürlüğü olarak kullanılan tüm ifadeler düşünceyi açıklama özgürlüğünü de kapsar nitelikte geniş anlamıyla ele alınmaktadır. *Kaboğlu*, ifade özgürlüğünün yapısal özelliklerine ilişkin yaptığı gözlemi şöyle özetlemektedir;

1- *İfadenin konusu, düşünce, fikir, kanaat, vicdan, inanç ve din deyimleriyle anlatılan değerlerdir.*

2- *İfade şekli sadece dile getirmekten ibaret olmayıp, savunma, tanıtma, yaratma, anlatma, açıklama, yayma olarak geniş tutulmaktadır.*

3- *İfade araçları yazma, konuşma, görüntü, resim, oyun, örnekleme şeklinde belirtilmiştir. Tek başına veya toplu biçimde olabildiği için, geniş bir özgürlük yelpazesıyla bitişiklik arz etmektedir³⁶³.*

Bu bağlamda ifade özgürlüğünün anayasal dayanağı hatırlanacak olursa, Anayasanın 26. maddesi³⁶⁴ düşünceyi açıklama ve yayma özgürlüğünü düzenlemektedir. Söz konusu maddenin birinci fıkrası birinci fıkrasında düşünce ve kanaatleri açıklama özgürlüğünün koruma alanı, klasik açıklama tarzlarını aşacak biçimde tüm iletişim yollarını kapsamaktadır. Bu nedenle maddenin koruduğu hukuksal alanı ifade özgürlüğü olarak nitelendirmek gerekir. Madde düşünceyi açıklama özgürlüğünün yanında aynı zamanda toplantı ve gösteri yürüyüşü özgürlüğünün, yeni medya olarak nitelendirilebilecek olan internet, dijital veri transferinin,

³⁶² **GORNIG**, Gilbert – Hanno, *Aeusserungsfreiheit und Informationsfreiheit als Menschenrechte*, Berlin, 1988, sh: 142.

³⁶³ **KABOĞLU**, İbrahim, *Pozitif Anayasa Hukukunda Düşünce Özgürlüğünün Sınırları*, in: *Düşünce Özgürlüğü*, sh: 213.

³⁶⁴ **MADDE 26.** – Herkes, düşünce ve kanaatlerini söz, yazı, resim veya başka yollarla tek başına veya toplu olarak açıklama ve yayma hakkına sahiptir. Bu hürriyet resmî makamların müdahalesi olmaksızın haber veya fikir almak ya da vermek serbestliğini de kapsar. Bu fıkra hükmü, radyo, televizyon, sinema veya benzeri yollarla yapılan yayımların izin sistemine bağlanmasına engel değildir.

(Değişik: 3.10.2001-4709/9 md.) Bu hürriyetlerin kullanılması, millî 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.

(Üçüncü fıkra mülga: 3.10.2001-4709/9 md.)

Haber ve düşünceleri yayma araçlarının kullanılmasına ilişkin düzenleyici hükümler, bunların yayımını engellemek kaydıyla, düşünceyi açıklama ve yayma hürriyetinin sınırlanması sayılmaz.

(Ek: 3.10.2001-4709/9 md.) Düşünceyi açıklama ve yayma hürriyetinin kullanılmasında uygulanacak şekil, şart ve usuller kanunla düzenlenir.

uydu yoluyla yayınların alt yapısını içermektedir.³⁶⁵ Ayrıca madde açıkça haber aktarımını da düşünce açıklamasıyla aynı koruma sistemine tabi tutmuştur. Bu açıdan 26. maddenin bir taraftan düşüncelerin ve haberlerin kitle iletişim araçlarıyla yayılmasını, diğer taraftan da düşünce oluşturma özgürlüğünü garanti ettiğini söylemek gerekir.³⁶⁶

Bu nokta itibarıyla Anayasanın 26. maddesinin birinci fıkrası bakımından iki ayrı hareket noktasının varlığı kabul edilmelidir. Bunlar düşünce ve haberlerin açıklanması ve yayılmasıdır. *Forum internum* safhasında şekillenen ve olgunlaşan düşüncelerin *forum externum* safhasına geçişte, ki bu geçişi açıklama ve yayma olarak düşünmek gerekir, 26. maddenin koruma alanda telakki edileceğinde bir şüphe yoktur, ancak salt haber aktarımının da bu kapsamda değerlendirilip değerlendirilemeyeceği sorununa *Can'ın* getirdiği çözüm yerinde ve amaca uygun görülmektedir. *Can'* göre, yalın haber aktarımını düşünce açıklaması biçiminde algılamanın zorluğu ortadadır; ancak bunların da 26. madde kapsamında aynı korumadan yararlandığı açıktır. Bununla birlikte haber yalın olarak aktarılmıyor ve herhangi bir biçimde bu habere bir anlam yükleniyor ve sahiplenilebiliyorsa bu durumda entelektüel katkı sağlandığı için geniş anlamda düşünce kapsamında değerlendirilmelidir. Yine yazar yönlendirici, eleştirel ve bazen de yanıtı içinde olan sorulara yapılan bireysel entelektüel katkı ortada iken, bunları düşünce kavramı içinde değerlendirmeyip düşünce açıklama özgürlüğünün koruma alanına almamanın mümkün olmadığı düşünülmektedir.³⁶⁷

Düşünce, kanaat ve haberlerin açıklanması ve yayılmasının ne tür araçlarla gerçekleştirilebileceği yine birinci fıkrada aktarılmıştır. Buna göre herkes, düşünce ve kanaatlerini söz, yazı, resim veya başka yollarla tek başına veya toplu olarak açıklama ve yayma hakkına sahiptir derken hükmün devamında radyo, televizyon, sinema veya benzeri yollarla yapılan yayımların izin sistemine bağlanmasına engel olmadığını vurgulamaktadır.

Maddenin ikinci fıkrasında ise söz konusu özgürlük alanının hangi gerekçelerle sınırlamaya tabi tutulabileceği ortaya konulmaktadır³⁶⁸. Buna göre millî güvenlik, kamu

³⁶⁵ CAN, Osman, Düşünceyi Açıklama Özgürlüğü Anayasal Sınırlar Açısından Neler Değişti?, <http://ogrenci.hacettepe.edu.tr/~b0122202/Inetpub/wwwroot/hukuk/anayasahukuk/dusunceyi%20Aciklama%20ozgurlugu.htm> (Erişim Tarihi: 18.09.2007)

³⁶⁶ KUZU, Burhan, Düşünceleri Açıklama Özgürlüğü Alanında Geldiğimiz Nokta, in İÜHFİM, İstanbul, 2001, sh: 251.

³⁶⁷ CAN, Osman, Düşünceyi Açıklama Özgürlüğü Anayasal Sınırlar Açısından Neler Değişti?, <http://ogrenci.hacettepe.edu.tr/~b0122202/Inetpub/wwwroot/hukuk/anayasahukuk/dusunceyi%20Aciklama%20ozgurlugu.htm> (Erişim Tarihi: 18.09.2007).

³⁶⁸ İfade Özgürlüğünün sınırlandırılmasına yönelik olarak uluslar arası düzeyde kabul gören bir prensip Amerikan Federal Yüksek Mahkemesi tarafından belirlenen “ açık ve yakın tehlike” prensibidir. Buna göre

düzeni, kamu güvenliği, Cumhuriyetin temel nitelikleri³⁶⁹ 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. Bu sınırlama düzenlemesinin hemen ardından üçüncü fıkrada haber ve düşünceleri yayma araçlarına ilişkin düzenlemelerin, bunların yayımını engellemek kaydıyla, düşüncüyü açıklama ve yayma özgürlüğüne bir sınırlama olarak kabul edilmeyeceği vurgulanmıştır. Bu nokta değerlendirme aşamasında internet özelinde ele alınacaktır.

Uluslar arası düzeyde de AİHS'nin 10. maddesinin ifade özgürlüğünü düzenlediği görülmektedir³⁷⁰. Söz konusu düzenleme de Anayasa md. 26 tarafından getirilen düzenleme ile paralel nitelik taşıdığı dikkati çekmektedir. Tabi bu maddenin ifade özgürlüğü başlığı altında düzenlenmiş olması yukarıda dile getirilen düşüncüyü açıklama özgürlüğü – ifade özgürlüğü ilişkisi bakımından daha kapsayıcı bir görünüme sahip olduğu düşünülebilir. Yine

kişinin veya Devletin korunması bakımından yasaklanmış eylemler varsa sınırlama veya cezalandırma, ancak düşüncenin açıklanması ile bu eylem arasında “açık ve yakın” bir nedensellik bağının bulunabileceği durumlarda mümkündür. Fakat burada dikkat edilecek husus, ileri sürülen düşünce ile onun meydana getirdiği eylem arasında doğrudan ve gerçek bir bağlantının var olmasıdır. 1919 yılında Yargıç Holmes tarafından ile getirilen bu kriterle her tek olayda ifade özgürlüğü bakımından dikkat edilmesi gereken en önemli husus kelimelerin açık ve yakın bir tehlike yaratacak şekilde kullanılıp kullanılmadığıdır. Eğer kullanılan kelimeler açık ve mevcut bir tehlike oluşturuyorsa bu noktada ifade özgürlüğü sınırlandırılmalıdır. Konu ile ilgili ayrıntılı bilgi için bkz. **KUZU**, Düşüncüyü Açıklama Özgürlüğü., sh: 258. Ayrıca ABD Federal Yüksek Mahkemesi'nin açık ve yakın tehlike ölçütü dışında esas aldığı diğer ölçütler ve bunların değerlendirmeleri için bkz. **TURAN**, Mehmet, Düşünce Özgürlüğü ve 1982 Anayasası, Düşünce Özgürlüğü ve 1982 Anayasası”, in: DÜHFD, Sayı 4, Diyarbakır, 1990, sh: 102-105; **ŞAHBAZ**, İbrahim, Karşılaştırmalı Düşüncüyü Açıklama Özgürlüğü, Ankara, 2007, sh:43 v.d.

³⁶⁹ İfade özgürlüğünün bir sınırlama nedeni olarak cumhuriyetin niteliklerine ilişkin ulusal ve uluslar arası değerlendirmeler için bkz. **KOÇAK**, Mustafa, Düşüncüyü Açıklama ve Yayma Özgürlüğünün Bir Sınırlanma Nedeni Olarak “Cumhuriyetin Nitelikleri, <http://www.e-akademi.org/makaleler/mkocak-1.htm>, (Erişim Tarihi: 15.01.2008)

³⁷⁰ **Madde 10 - İfade özgürlüğü (1.)** 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. Bu madde, devletlerin radyo, televizyon ve sinema işletmelerini bir izin rejimine bağlı tutmalarına engel değildir.

2. Kullanılması görev ve sorumluluk yükleyen bu özgürlükler, demokratik bir toplumda, zorunlu tedbirler niteliğinde olarak, 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 yasayla öngörülen bazı biçim koşullarına, sınırlamalara ve yaptırımlara bağlanabilir.

ikinci fıkrada da bu özgürlük alanına hangi şartlarda sınırlama getirilebileceği düzenlenmiştir³⁷¹.

Faklı bir düzenleme olarak Birleşmiş Milletler Siyasi ve Medeni Haklar Sözleşmesinin 19. maddesi³⁷² de ifade özgürlüğüne ilişkin bir düzenleme getirmiştir. Bu düzenleme de yukarıda üzerinde durulan düzenlemeler büyük ölçüde paralellik sağlamakla birlikte bazı noktalarıyla farklılık arz etmektedir. Öncelikle birinci maddesinde kişilerin hiçbir müdahaleye maruz kalmadan fikirlere sahip olma hakkının varlığından bahsetmiştir. Bu yaklaşım düşünce özgürlüğünün ifade özgürlüğü içinde değerlendirilmesi gerektiği yönünde bir fikri yansıtmaktadır. Keza ikinci fıkrada bu özgürlük alanının kullanılmasında kişileri her türlü bilgi ve düşünceyi arama, edinme, ulaşma amacıyla sanatsal ürünler de dahil olmak üzere kendi belirleyecekleri araçları kullanabileceklerini düzenlemiştir. Son olarak da üçüncü fıkrada ifade özgürlüğünün sınırlandırılma sebepleri diğer iki düzenlemeye göre daha sınırlı belirlenmiştir.

4.2.1.3.- Ceza Hukuku Perspektifinden İnternetin Düşünce ve İfade Özgürlüğü ile İlişkisi

Modern toplumun en yaygın ve fonksiyonel kullandığı kitle iletişim araçlarından bir olan internetin düşünce ve ifade özgürlüğü ile olan yakın ilişkisi tartışma götürmezdir.

³⁷¹ A.İ.H.M. ifade özgürlüğü ile ilgili vermiş olduğu kararlarda ifade özgürlüğünün kullanım alanını ve sınırlarını belirlemiştir. Örneğin mahkeme şiddet içermeyen direniş çağrısının yapılabileceğini (İncal/ Türkiye Davası, 9 Haziran 1998), tarihi gerçeklerin taraflı olarak dile getirilebileceğini (Arslan/ Türkiye Davası, 8 Temmuz 1999), şiddet, silahlı mücadele ve isyan çağrısı yapılmaksızın fikirlerin düşmanca bir üslupla olsa dahi kaleme alınabileceğini (Polat/ Türkiye Davası, 8 Temmuz 1999), ifade özgürlüğünün sınır ötesi olduğunu (Akin Derneği/ Fransa Davası, 17 Temmuz 2001) kabul etmiştir. Bununla birlikte bir düşünce açıklamasının nasıl yapıldığı (Karataş/Türkiye Davası, 8 Temmuz 1999), beyanın nasıl bir topluluğa yapıldığı (Gerger/ Türkiye Davası, 8 Temmuz 1999), kutsal ve ahlaki değerlere saldırı niteliğindeki düşünce açıklamalarının koruma kapsamına alınmadığı (Handyside/ İngiltere Davası, 7 Aralık 1976), kin ve nefret arttırmaya yönelik beyanların yasaklanabileceği (Sürek/ Türkiye Davası, 8 Temmuz 1999), terör örgütünü destekleyici açıklamaların yapılamayacağı (Zana/ Türkiye Davası, 25 Kasım 1997), önemsiz dahi olsa gizli bilgilerin ifşa edilemeyeceği (Handjiannastassiou/ Yunanistan Davası, 16 Aralık 1992) gibi önemli sınırlandırmalar da getirilmiştir. Konuy ile ilgili ayrıntılı bilgi için bkz. **BIÇAK**, Vahit, Avrupa İnsan Hakları Mahkemesi Kararlarında İfade Özgürlüğü, Ankara, 2002, sh: 22 v.d.

³⁷² 19. Madde - **İfade özgürlüğü (1.)** Herkesin, bir müdahale ile karşılaşmaksızın fikirlere sahip olma hakkı vardır. **(2.)** 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. **(3.)** Bu maddenin ikinci fıkrasındaki haklar özel bir ödev ve sorumlulukla kullanılır. Bu nedenle bu hak, sadece hukuken öngörülen ve aşağıdaki sebeplerle gerekli olan sınırlamalara tabi tutulabilir: a) Başkalarının haklarına ve itibarına saygı; b) Ulusal güvenliği veya kamu düzenini (ordre public), veya sağlık ve ahlaki koruma.

Yukarıda gerek ulusal gerekse uluslar arası düzenlemelerle çerçevesi belirlenmeye çalışılan bu iki özgürlük alanını internetle olan ilişkileri bakımından ayrı ayrı değerlendirecek olursak;

İnternetin düşünce özgürlüğü ile olan ilişkisi ilk bakışta ifade özgürlüğü ile olan ilişkisinden daha az olduğu izlenimi doğmaktadır. Çünkü düşünce özgürlüğünün içsel bir etkililik olan “düşünme” üzerine kurulu bir özgürlük alanı olduğu dile getirmiştir. Ancak internet de dahil olmak üzere tüm bilgi kaynaklarının kullanımı düşünce özgürlüğü bakımından büyük önem taşımaktadır. Şöyle ki; bir düşünme etkinliğinin gerçekleşebilmesi ve bu etkinlik neticesinde bir ürün olarak düşünce ve/veya kanaatin ortaya çıkabilmesi ancak ve ancak bu etkinliği mümkün kılacak olanaklarının amaca uygun bir biçimde tesisi ve bunların korunması ile ilgilidir. Başka bir anlatımla düşünme mutlak suretle bilgiye ve bilgilerin muhakemesine dayanana bir etkinliktir. Kişinin bilgiye ulaşımı engellendiği veya dezenformasyona tabi tutulduğu bir ortamda bu etkinliği gerçekleştirebilecek alt yapıya ulaşamaz. Bu da aslında bir özgürlük alanının kaynağını ortadan kaldırmak anlamına gelir ki bu durumda düşünce özgürlüğünün de bir anlamı kalmaz. Bu noktadan normatif düzenlemelerle mutlak koruma altına alınan düşünce özgürlüğünün doğasına ve düzenleme amacına uygun olarak kullanılabilmesi için tüm bilgi kaynaklarının da buna uygun düzenlemelere tabi tutulması gerekmektedir. İşte modern toplumun en önemli bilgi kaynağı olan internet de bu anlamda düşünce özgürlüğü bakımından hayati önem taşımaktadır. İnternete ilişkin düzenlemeler yapılırken mutlak suretle düşünce özgürlüğünün gerek ulusal gerekse uluslar arası düzenlemelerle mutlak olarak düzenlendiği dikkate alınarak bu mutlak güvenceyi ortadan kaldıracak şekilde kullanılmasının önüne geçilmelidir. İleride internete ilişkin maddi ceza hukuku düzenlemeleri ve özellikle de internet sùjelerinin ceza sorumluluğu analiz edilirken yine bu temel yaklaşıma atıfta bulunulacaktır.

İnternetin ifade özgürlüğü ile olan ilişkisi çok daha doğrudan bir ilişki olarak yorumlanabilir. Anayasanın 26. maddesinin medya yoluyla düşünce ve haberlerin aktarımını koruduğu, bu haliyle de yeni teknolojik gelişmeler ve bilgi toplumunun iletişim kaynaklı ihtiyaçlarını karşılamaya yönelik bir düzenleme olduğu görülmektedir. Bu yaklaşım tarzı yeni teknolojik gelişmelerin göz ardı edilmeyip bunun düşünce açıklama özgürlüğünün gerekleri içinde değerlendirildiğinin bir kanıtıdır. Bu yüzden düşünceyi açıklama özgürlüğü bakımından salt radyo ve televizyonun değil elektronik bilgi ağı olanaklarının özellikle de internetin kullanılmasının Anayasanın 26. maddesi kapsamında düşünülmesi gerektiği açıktır. Zaten birinci fıkrada “Bu fıkra hükmü, radyo, televizyon, sinema veya benzeri yollarla yapılan yayımların izin sistemine bağlanmasına engel değildir.” derken interneti de bu

kapsama dolaylı olarak dahil etmiş ve internet üzerinden yapılan yayınların da izine tabi tutulması ifade özgürlüğüne bir ihlal olarak görülmektedir. Ancak yukarıda değinildiği üzere bunun ifade özgürlüğüne bir sınırlama olarak algılanması karşısında Anayasanın sınırlamanın sınırı olarak belirlediği kriterlere, ki her şeyden önce sınırlamanın kanunla yapılması ve öze dokunmama, bağlı olarak hareket edilmelidir. Bu açıklamaların önemi şuradan kaynaklanmaktadır; modern ceza hukukunda risk toplumunun ortaya çıkardığı problemleri en etkili bir biçimde çözmek adına artan sayıda soyut tehlike suçlarının düzenlenmesi, önleme kaygısıyla önemli bir risk alanı olarak kabul edilen internete getirilen sınırlamalarda bu ve bundan sonraki özgürlükler için de geçerli olarak öze dokunulup dokunulmadığı tartışmasının yapılması gerekmektedir.

Türk Ceza Hukuku perspektifinden internet ile düşünce ve ifade özgürlüğü ilişkisine bakılacak olursa bir kitle iletişim aracı olarak internet diğer kitle iletişim araçlarının, yani 5237 sayılı TCK md. 6 hükmünce basın yayın araçlarının düzenlendiği noktalarda da söz konusu olacaktır. Bu bağlamda 5237 sayılı TCK'de iki madde internet ile düşünce ve ifade özgürlüğü ilişkisi bakımından örnek olmaları anlamında önem arz etmektedir. Bunlar md. 218 ve md. 301'dir. 218. maddeye göre kamu barışına karşı işlenen suçların³⁷³ basın yayın yoluyla işlenmesi durumunda verilecek ceza yarı oranında arttırılır. Ancak haber verme sınırlarını aşmayan ve eleştiri amacıyla yapılan düşünce açıklamaları suç oluşturmaz. Yine Türklüğü, Cumhuriyeti, Devletin kurum ve organlarını aşağılama suçunun düzenlendiği 301. maddede de eleştiri amacıyla yapılan düşünce açıklamalarının suç oluşturmayacağı düzenlenmiştir.

Özellikle haber verme sınırlarını aşmayan düşünce açıklamaları ile ilgili haberleşme özgürlüğünün inceleneceği kısımda ele alınacağından burada değerlendirilmemektedir. Ancak eleştiri amacıyla yapılan düşünce açıklamaları ile ilgili Yargıtay uygulamalarına bakmak ve bunu internetle ilişkilendirmek yerinde olacaktır.

Yargıtay kararlarında eleştiri amaçlı düşünce açıklamaları konusunda belli bir istikrarın yakalandığından bahsetmek zordur. Örneğin Yargıtay'ın verdiği bir karara göre, karikatür dalında Türkiye'de ün yapan katılanların, etkinlik gösterdikleri meslek alanlarını ve mesleklerini değerlendirmede gerekli olmayan ya da okurların gereksiz merak duygularını doyurmaya yönelik söz ve suçlamaların eleştiri ve haber sınırlarını aşacağı, haber ve bilgiler gerçek olsa bile, bunların eleştiri ve haber sınırları içinde kalmaları için, bilinmesinde

³⁷³ Bu suçlar Halk arasında korku ve panik yaratmak amacıyla tehdit (md. 213), suç işlemeye tahrik (md. 214), suçu ve suçluyu övme (215), halkı kin ve düşmanlığa tahrik veya aşağılama (md. 216), kanunlara uymamaya tahrik (md. 217)

kamu yararının ve halkı aydınlatma işlevinin bulunması gerektiğinin gözetilmesi ve küçük düşürücü suçlamaları haber verme, eleştirme ve bilgilendirme hakları çerçevesine indirgeyen ve eylemi hukuka uygun kılan bir durumun bulunup bulunmadığının değerlendirilip hüküm kurulması gerekir³⁷⁴. Yine başka bir kararında, Türk Silahlı Kuvvetlerine yönelik olarak kendi milletine karşı silah kullanmaktan çekinmeyen, hukuk devletini ortadan kaldırmaya çalışan, bu amaçla elindeki gücü kötüye kullanan bir kurum olduğu yolunda saptamalara yer verildiği, bu saptamaların eleştiri boyutunu aşarak aşağılayıcı ve küçültücü değer yargısı taşıdığına karar verilmiş ve sanığın, bu belgeyi basın mensuplarına vermesi, bu suretle geniş kitlelere ulaşmasını sağlamaya çalışması da söz konusu yazının tahkir ve tezyif kastıyla yazıldığını açıkça ortaya koyduğuna karar vermiştir³⁷⁵. Nihayet Yargıtay'ın yakın zamanlarda vermiş

³⁷⁴ Yargıtay 4. CD., 23.09.1992, E. 1992/5002 – K. 1992/5777 (Kaynak: Kazancı İçtihat Programı - Offline) .

³⁷⁵ “Sanığın, Devletin askeri kuvvetlerini alenen tahkir ve tezyif etmek suçundan beraatine karar verilen somut olayda bu hüküm yüklenen suçun sübuta erdiğinden bahisle bozulmuş, ancak Özel Daire önceki hükmünde direnmiştir. Adana Cumhuriyet Başsavcılığınca, sanık C.Savcısı Sacit K.'nun, herhangi bir ihbar, şikayet dilekçesi veya belge bulunmaksızın, hiçbir soruşturma yapmadan, .sanığın ifadesini almadan, gayri ciddi olarak düzenlediği 28.3.2000 tarihli iddianamenin işleme konulmadığı, adı geçen C.Savcısının hiçbir bilgi vermeden ve yetkisi olmadan bazı basın mensuplarını çağırarak konu hakkında bilgi verdiği, bu görüşmenin bir televizyon kanalının haberlerinde yayınlandığının öğrenildiği belirtilerek, Adalet Bakanlığı Ceza İşleri Genel Müdürlüğüne suç duyurusunda bulunulması üzerine, sanık hakkında soruşturma yapılabilmesi için gerekli izinler verilmiş ve sanık hakkında yapılan soruşturma sonucunda da son soruşturmanın açılmasına karar verilmiştir. Sanık, hazırladığı iddianamede ne kişileri ne de kurumları tahkir ve tezyif gibi niyetin ve ifadenin olmadığını görüleceğini, sadece ordunun gerek Osmanlı, gerekse Türkiye Cumhuriyeti Devleti içinde giriştiği isyanlar ve ihtilallerin halk üzerinde yarattığı korkudan söz edildiğini, bunda da bir tahkir değil tespitin söz olduğunu, tahkir ve tezyifin ancak böyle bir kasıt varsa cezalandırılabileceğini, oğlunu askeri liseye kaydettirmek, kendisinin de subay olarak orduda kalmak için uğraştığı ve eşinin de bir albay kızı olduğu düşünülürse, böyle bir kastın bulunmadığının en azından aile ilişkileri nedeniyle daha iyi anlaşılacağını, 12 yıl avukatlık yaptıktan sonra durumu çok iyi olduğu halde adaletin yerine gelmesine yeterince katkıda bulunamadığını düşünerek bu mesleğe geçtiğini, eğer suçluların cezalandırılmasını istemek suç ise, bu suç işlediğini kabul ettiğini ancak görevini yaptığını ve kimseyi tahkir etmediğine inandığını bildirmiştir. Tanıklardan Adana Hakimi Teyfik Süha M., soruşturmaya konu olayı bir gazetenin temsilcisi Temel E.'in olay günü kendisini telefonla arayıp sorması üzerine öğrendiğini, haberi olmadığını öğrenince bu kişinin söz konusu iddianameyi adliyedeki faks aracılığıyla gönderdiğini, nereden temin ettiğini sorduğunda ise, sanığın, sümen altı olmasını engellemek için basın mensuplarına dağıttığını belirttiğini söylemiştir. Basın mensubu olan tanıklar Mehmet A., Erol Ş. ve Ömer B., sanığın, adliyedeki basın bürosuna gelerek suça konu beş sayfalık iddianamenin bir örneğini fotokopi yoluyla almalarını sağladığını; tanıklar Nazan E., Mazul D., Tefik D., Serdar E., Temel E., Neşet K. ve Murat D. ise randevu alarak evine gittiklerini sanığın, sordukları soruları cevapladığını beyan etmişlerdir. Görüldüğü gibi sanık; yargulamaya konu "iddianame" başlıklı belgeyi kaleme aldıktan sonra bir örneğini basın mensuplarına vermiş, ayrıca içeriği konusunda açıklamalar yapmak suretiyle bu belgenin aleni hale gelmesini sağlamıştır. Olayda "aleniyet" unsurunun gerçekleştiğinde kuşku olmadığına göre, söz konusu belgenin tahkir ve tezyif içermediğinin belirlenmesi gerekmektedir. "Iddianame" başlıklı bu belgede; "...Ancak, bugüne kadar sanık ve arkadaşları hakkında işlem yapılmayışının sebebi, ordunun sahip olduğu ve gerektiğinde kendi milletine karşı kullanmaktan çekinmediği silah gücünün toplum üzerinde yarattığı korkudan başka bir şey değildir. Halbuki demokrasilerde üstün olan sadece hukukun gücüdür. Türkiye'de ise maalesef gücün hukuku egemendir... Türkiye Cumhuriyeti ya gerçek bir hukuk devleti olarak varlığını devam ettirecek ya da yeniden gücün üstünlüğüne boyun eğerek yaşamaya devam edecektir...Türk milletinin kardeş kanı dökülmemesi için orduya karşı bir isyan başlatmayı ne ihtilali ne de muhtırayı haklı gösterebilir...Nitekim bugüne kadarki uygulama, Türkiye'nin bir hukuk devleti değil, asker devleti olduğunu düşündürmektedir. Suçu sivil işlerse cezalandıran, asker işlerse cezalandırmayan bir devletin vatandaş nazarında itibarı kalmaz..." şeklinde ibarelere yer verilmiştir. Gerek belgenin bütünü gerekse açıklanan bu ibareler incelendiğinde, sanık olarak gösterilen kişinin eyleminin niteliğinin belirlenmesinin yapılmadığı, tam tersine Türk Silahlı Kuvvetlerine yönelik olarak kendi milletine karşı silah kullanmaktan çekinmeyen, hukuk devletini ortadan kaldırmaya çalışan, bu amaçla elindeki gücü kötüye kullanan bir kurum olduğu yolunda saptamalara yer verildiği bu saptamaların ise

olduğu bir kararında, eleştiri amaçlı düşünce açıklamasının statik ölçütlerle değil koşul ve duruma görecelendirerek değerlendirilmesi gerektiğini aynen şu ifadelerle ortaya koymaktadır:

“ Yargılama konusu haber ve yorum metinlerindeki eleştiri ve değer yargılarının bir kısmı sert ve çarpıcı bir üslupla dile getirilmiştir. Esasen, eleştirinin sert bir üslupla gerçekleştirilmesi, kaba olması ve nezaket sınırlarını aşması, eleştirenin amacına, psikolojisine, eğitim ve kültür düzeyine bağlı bir olgudur. Ancak kabul edilmelidir ki, basın özgürlüğü belli ölçülerde abartmayı hatta kışkırtmaya başvurmayı da içerir. Gazetecilerin yazılarında kullandıkları deyimler “polemik” niteliğinde olsa da nesnel bir açıklamayla desteklendiğinde bu ifadeler asılsız kişisel saldırı olarak görülemez. Kaldı ki, kamu görevinde bulunan ve talip olanların diğerlerine oranla daha sert eleştirilere muhatap olması da doğal karşılanmalıdır.

Somut olayda haber ve yorumların kaynağı, yapıma nedeni, açıklama yapılıp, hakkında açıklama yapılanların toplumdaki konumları, tüm yazıların içeriği dikkate alındığında sanığın, siyasi bir kişilik olan katılanın görevinden kaynaklanan uygulamalarını dört gün boyunca devam eden yazı dizisinde polemik yaratan ve rahatsız eden bir üslupla sorgulayıp, sert, ağır ve çarpıcı biçimde kamuoyunun bilgisine sunduğu, ancak eylemin katılanın görevinden dolayı aşağılama boyutuna ulaşmadığı anlaşılmaktadır. Bu itibarla C. Başsavcılığının itirazının kabulüne karar verilmelidir.”³⁷⁶

Yargıtay’ın yakın tarihli kararları da eleştiri amacıyla yapılan düşünce açıklamalarının sınırı ile ilgili bir takım değerlendirmeler içermektedir. Örneğin Yargıtay’a göre sanık hakkında, yazı içerisinde “... senin önce oturduğun koltuğu, işgal ettiğin makamı tartışmak lazım. Sen oraya nerden geldin?” ... “Bu insanların okul kapısına tel örgü çektirip başörtülü öğrencileri okula almayan din bezirganlarından öğreneceği hiçbir şey yoktur. Sende zerre

eleştiri boyutunu aşarak aşağılayıcı ve küçültücü değer yargısı taşıdığı anlaşılmaktadır. Sanığın, bu belgeyi basın mensuplarına vermesi, bu suretle geniş kitlelere ulaşmasını sağlamaya çalışması da söz konusu yazının tahkir ve tezyif kastıyla yazıldığı açıkça ortaya koymaktadır. Bu itibarla Özel Dairenin beraate ilişkin hükmünün bozulmasına karar verilmelidir. Çoğunluk görüşüne katılmayan Kurul Başkanı ve Üyeler ise, “Sanık tarafından kaleme alınan yazı bir bütün olarak ele alınıp değerlendirildiğinde, 12 Eylül hareketine yönelik saptamalara yer verildiği, eleştiri niteliğini taşıyan bu saptamaların sanık tarafından Devletin askeri kuvvetlerini tahkir ve tezyif kastıyla yazılmadığı açıktır. Bu nedenle Özel Dairenin beraate ilişkin hükmünün onanmasına karar verilmelidir.” görüşüyle karşı oy kullanmışlardır. **SONUÇ** : Açıklanan nedenlerle Yargıtay 9.Ceza Dairesinin sanığın beraatine ilişkin hükmünün BOZULMASINA, dosyanın yeniden yargılama yapılmak üzere bu Daireye gönderilmesi için Yargıtay C.Başsavcılığına tevdiine, 9.4.2002 günü yapılan birinci müzakerede yasal çoğunluk sağlanamadığından, 16.4.2002 günü yapılan ikinci müzakerede oyçokluğu ile karar verildi.” Yargıtay CGK, 16.04.2002, E. 2002/9-96 – K. 2002/234 (Kaynak: Kazancı İçtihat Programı – Offline)

³⁷⁶ Bkz. Yargıtay CGK, 24.06.2006, E. 2006/4- 242 – K. 2006/18 (Kaynak: Kazancı İçtihat Programı – Offline).

kadar Allah korkusu varsa, çıkıp insanların kafasını karıştırma..." şeklindeki ifade ile mağdurun mesleki bilgisinin yetersiz olduğu vurgulanmaktan öte, mesleki bilgisini kötüye kullandığı, toplumun aklını kasıtlı olarak karıştırmaya çalıştığı ileri sürülmekte, bu suretle mağdur aşağılanarak toplum önünde küçük düşürülmektedir. Bu nedenle sanık tarafından kaleme alınan yazı, içeriği itibarıyla düşünce açıklama özgürlüğünü ve eleştiri sınırlarını aşmış olup, kullanılan ifadeler mağdurun kişiliğine saldırı niteliğindedir³⁷⁷. Düşünce ve ifade özgürlüğü ile ilgili AİHM'nin verdiği kararlara bakılacak olursa da, mahkemenin bu özgürlük alanını oldukça geniş olarak yorumladığı görülmektedir. Mahkeme şiddet içermeyen direniş çağrısının yapılabileceğini (*İncal/ Türkiye Davası, 9 Haziran 1998*)³⁷⁸, tarihi gerçeklerin taraflı olarak dile getirilebileceğini (*Arslan/ Türkiye Davası, 8 Temmuz 1999*)³⁷⁹, şiddet, silahlı mücadele ve isyan çağrısı yapılmaksızın fikirlerin düşmanca bir üslupla olsa dahi kaleme alınabileceğini (*Polat/ Türkiye Davası, 8 Temmuz 1999*)³⁸⁰, ifade özgürlüğünün sınır ötesi olduğunu (*Akin Derneği/ Fransa Davası, 17 Temmuz 2001*)³⁸¹ kabul etmiştir. Bununla birlikte bir düşünce açıklamasının nasıl yapıldığı (*Karataş/Türkiye Davası, 8 Temmuz 1999*)³⁸², beyanın nasıl bir topluluğa yapıldığı (*Gerger/ Türkiye Davası, 8 Temmuz 1999*)³⁸³, kutsal ve ahlaki değerlere saldırı niteliğindeki düşünce açıklamalarının koruma kapsamına alınmadığı (*Handyside/ İngiltere Davası, 7 Aralık 1976*)³⁸⁴, kin ve nefret arttırmaya yönelik beyanların yasaklanabileceği (*Sürek/ Türkiye Davası, 8 Temmuz 1999*)³⁸⁵, terör örgütünü destekleyici açıklamaların yapılamayacağı (*Zana/ Türkiye Davası, 25 Kasım 1997*)³⁸⁶, önemsiz dahi olsa gizli bilgilerin ifşa edilemeyeceği (*Handjiannastassiou/ Yunanistan Davası, 16 Aralık 1992*)³⁸⁷ gibi önemli sınırlandırmalar da getirilmiştir

³⁷⁷ Bkz. Yargıtay CGK, 20.03.2007, E: 2007/4-65 – K: 2007/70 (Kaynak: Kazancı İctihat Programı, Offline)

³⁷⁸ **BIÇAK**, İfade Özgürlüğü, sh: 30.

³⁷⁹ **BIÇAK**, İfade Özgürlüğü, sh: 31.

³⁸⁰ **ŞAHBAZ**, Düşünceyi Açıklama Özgürlüğü, sh: 109.

³⁸¹ **BIÇAK**, İfade Özgürlüğü, sh: 39.

³⁸² **ŞAHBAZ**, Düşünceyi Açıklama Özgürlüğü, sh: 96.

³⁸³ **ŞAHBAZ**, Düşünceyi Açıklama Özgürlüğü, sh: 86.

³⁸⁴ **BIÇAK**, İfade Özgürlüğü sh: 40.

³⁸⁵ **BIÇAK**, İfade Özgürlüğü sh: 28.

³⁸⁶ **ŞAHBAZ**, Düşünceyi Açıklama Özgürlüğü, sh: 68.

³⁸⁷ **BIÇAK**, İfade Özgürlüğü, sh: 41.

Gerek ulusal gerekse uluslar arası mahkeme kararları ışığında kanaatimizce eleştiri amaçlı düşünce açıklamalarının temel ölçütünün özgürlükten yana geniş yorumlanarak hareket edilmesi gerekmektedir. Bu tarz bir yorumlama AİHM'nin içtihatlarında ortaya konulan yaklaşımlar çerçevesinde gerçekleştirilmelidir. Bu anlamda bir düşünce açıklamasının sadece eleştiri amaçlı yapıp yapılmadığının incelenmesi, düşünce ve ifade özgürlüğüne getirilmek istenen ayrıcalıklı konumu sınırlama manasına gelir. İnternetin ulaşılmış olduğu nokta göz önünde bulundurulduğunda, internet ortamına aktarılacak içeriklerin önsel bir denetimden geçmesinin teknik açıdan çok zor ve hatta imkansız olması ve bizatihi internetin sunduğu gizlilik ve anonimlik güvencelerinin³⁸⁸ kullanıcılarda doğurduğu cesaret özellikle her türden düşüncenin ifade edilebilmesine imkan vermektedir. Bu durumda kimi çevrelerce büyük bir tehlike olarak kabul edilmektedir. Ancak bu tehlikelere getirilecek tedbirler düşünce ve ifade özgürlüğünü kullanılamaz hale getirecek konumda olmamalıdır. Bunun en önemli örneklerinden biri ABD'de yaşanmıştır. ABD'de 1996 yılında düzenlenen İletişim Ahlakı Yasası'nda bazı hükümlerinin Federal Anayasa'nın ifade özgürlüğünü güvence altına alan hükümlerine aykırı olduğu ve yasada yer alan “müstehcen yayın”, “ahlaksızlık” gibi ifadelerin aşırı derece müphem ve geniş kavramlar olduğu, ayrıca bu durumun ceza normunun belirliliğine ters düştüğü iddiasıyla iptal istemiyle dava açılmıştır. Federal Yüksek Mahkeme de anılan gerekçeler ışığında yasanın ilgili maddesini iptal etmiştir. İptal kararının gerekçesi de yukarıda ifade edilmeye çalışılan internet ile düşünce ve ifade özgürlüğü ilişkisinin bir özeti niteliğindedir.

“Bir kitle iletişim aracı olarak internet, hükümetlerin müdahalesine karşı korunmalıdır. İnternet üzerindeki yayınlarla ilgili düzenlemenin bulunmaması kuşkusuz bir kaos yaratmıştır. Ancak unutmamak gerekir ki, internetin gücü de bu kaostan kaynaklandığı gibi Anayasa'da belirlenen düşünceyi açıklama özgürlüğü de aynı kaosa dayanmaktadır. Demokratik toplumlarda özgür fikir alışverişinin sağlayacağı toplumsal yarar, internette sansürün sağlayabileceği toplumsal yararlarla karşılaştırılamayacak kadar önemlidir.”³⁸⁹

4.2.2. – Haberleşme Özgürlüğü

Haberleşme özgürlüğü arasında tarihsel süreç bakımından bir öncelik sonralık ilişkisinin olduğu kabul edilebilir. Şöyle ki; matbaanın icadından sonra haber, düşünce ve

³⁸⁸ GEDİK, Ömer, Türkiye'de İnternet Özgürlüğü ve 5651 Sayılı Kanun, in: MÜHFHAD, C: 14, S: 1-2, İstanbul, 2008, sh: 181 – 182.

³⁸⁹ YILDIZ, Sevil, Suçta Araç Olarak İnternetin Teknik ve Hukuki Yönden İncelenmesi, Ankara, 2007, sh: 115.

kanaatlerin kamuyla paylaşılması için yazılı materyaller haline getirilmesi ve bu suretle bir kitle iletişim aracı olarak kullanılması ile, bu kullanımın güvenceye alınabilmesi için tüm gelişmeler basın özgürlüğü kapsamı altında yaşanmıştır. Ancak geçen yüzyıldan bu yana sinema, radyo, televizyon ve internet gibi yeni kitle iletişim araçlarının etkin rol oynamaya başlamasıyla birlikte, sadece basın yolu ile iletişim kurmaya ilişkin bir kavram olan basın özgürlüğü kavramı yetersiz kalmış, ve bu modern iletişim araçlarını da kapsayan yeni bir kavrama gereksinim duyulmuştur.³⁹⁰ İşte haberleşme özgürlüğü kavramı, bu gereksinimleri karşılamaya yönelik bir kavram olma özelliği taşır.

Yukarıda da ifade edildiği üzere haberleşme imkanlarının her geçen gün gelişmesi ve bu gelişmeye paralel olarak yeni haberleşme araçlarının kullanılır olması dolayısıyla söz konusu özgürlük alanını daha kapsamlı düzeyde ele almakta fayda vardır. Bu bağlamda *İçel/ Ünver* haberleşme özgürlüğünü “*haber, düşünce ve kanuların basın, radyo – televizyon, sinema ve internet gibi kitle haberleşme araçları ile serbestçe alınması ve yayılması*” şeklinde tanımlamışlardır³⁹¹. Ancak bu tanımla haberleşmenin sadece kitlesel boyutu esas alınmış, örneğin iki kişi arasında telefon, mektup, e- mail gibi kişiye özel haberleşme araçları kullanarak gerçekleştirilen haber, düşünce ve kanı aktarımının haberleşme özgürlüğü güvencesi dışında tutulduğu izlenimi doğmaktadır. Dolayısıyla kanaatimizce bahse konu tanımda “kitle haberleşme araçları” yerine “her türlü haberleşme araçları” kavramı kullanılacak olursa haberleşme özgürlüğünün kapsayıcı niteliğine daha uygun olacaktır. Tanım şu haliyle “kitle haberleşme özgürlüğü”nün isabetli bir şekilde belirlemiştir³⁹².

Özellikle bu tespit internet teknolojisi esas alındığı zaman daha da net bir biçimde görülmektedir. Çünkü daha sonra da değinileceği üzere, internet sadece bir kitle haberleşme aracı değil, kullanıcılarının salt kendi inisiyatiflerinde çalışan haberleşme imkan ve programları (e- mail, eş zamanlı sohbet programları gibi) ile bireye özgü haberleşme aracı olarak da kullanılabilir. Bu da çift yönlü bir haberleşme özgürlüğünü mümkün kılmaktadır. Ancak kişiler arası haberleşme özgürlüğü bir özel yaşam unsuru olarak özel hayatın gizliliğine ilişkin bölümde değerlendirileceği için bu kapsam da kitle haberleşme ile sınırlı tutulmuştur.

³⁹⁰ **SINAR**, İnternet, sh:47.

³⁹¹ **İÇEL/ ÜNVER**, Kitle Haberleşme Hukuku, sh: 24.

³⁹² *Gedik de İçel/ Ünver'in* bu tanımını “Kitle İletişim Özgürlüğü” tanımı olarak ele almıştır. Bkz. **GEDİK**, Türkiye’de Kitle İletişim Özgürlüğü, sh: 34.

Haberleşme özgürlüğünün bu iki yönü arasında en kapsamlı ve etkili olanı kitle haberleşme özgürlüğüdür. Kitle haberleşme özgürlüğü, bu özgürlüğün kullanıldığı araçlara bağlı olarak anlam kazanan bir özgürlük alanıdır. Kitle haberleşmeden bahsedebilmek için, herhangi bir içeriğin kitlesel yayılımını mümkün kılacak araçlara ihtiyaç vardır. Bu çerçevede basın, radyo – televizyon, sinema, internet gibi araçlar vasıtasıyla gerçekleşen bir haberleşme etkinliği kitle haberleşme olarak belirtilebilir. Bu bağlamda özellikle günümüzde kitle haberleşme özgürlüğü, kullanılan aracın özgürlüğü olarak kullanılmaya başlamış, bununla birlikte her araç kendi rejimini oluşturma yönelimine girmiştir³⁹³. Buna örnek olarak “basın özgürlüğü – basın rejimi”, “radyo televizyon özgürlüğü – radyo televizyon rejimi” ve “nihayet “ internet özgürlüğü – internet rejimi” ilişkisi gösterilebilir. Özellikle basın özgürlüğü kitle haberleşme ile ilgili özgürlük alanları içinde en çok üzerinde durulan alandır. *Salihpaşaoğlu’na* göre basın özgürlüğü genel olarak haberlerin, düşüncelerin, yorumların, analizlerin, eleştirilerin serbestçe basılması, yayımlanması ve dağıtılması olarak tanımlanmaktadır³⁹⁴. 5187 sayılı Basın Kanunu’nun 3. maddesinde de basın özgürlüğü bilgi edinme, yayma, eleştirme, yorumlama ve eser yaratma hakkını da içerir şekilde düzenlenmiştir³⁹⁵.

Haberleşme özgürlüğü ile düşünce ve ifade özgürlüğünü aralarında önemli bir ilişki mevcuttur. Çünkü günümüzde düşünceyi ifade etmenin en yaygın ve etkin yolu kitle iletişimidir. Düşünce ve ifade özgürlüğü olmadıkça basın ve haberleşme özgürlüğünün bir anlamı kalmaz. Bu bakımdan düşünce ve ifade özgürlüğünün amaca uygun bir tarzda kullanılabilmesi için bu özgürlük alanlarının koruma altına alınması gerekmektedir.³⁹⁶ *Can*, haberleşme özgürlüğünü düşünce ve ifade özgürlüğü bakımından bir türev özgürlük olarak kabul ederken³⁹⁷, *Lampe* de haberleşme (iletişim) özgürlüğü ile düşünce – ifade özgürlüğü arasında çok önemli bir bağlantı olduğu savunmaktadır. Hatta *Lampe* daha da ileri giderek iletişim özgürlüğü ile hukuk arasındaki ilişkiyi şöyle ifade etmektedir:

³⁹³ Ayrıntılı bilgi için bkz. **İÇEL/ÜNVER**, Kitle Haberleşme Hukuku, sh: 23-24. Ayrıca bu ayrımın karşılaştırmalı hukuktaki görünümü takip etmek için bkz. **GEDİK**, Kitle İletişim Özgürlüğü, sh: 51 v.d.

³⁹⁴ **SALİHPAŞAOĞLU**, Basın Özgürlüğü, sh: 27.

³⁹⁵ Basın kavramı ve rejimi, bir kitle haberleşme unsuru olarak ikinci bölümde özellikle internet özelinde ve 5237 sayılı TCK md. 6’da yapılan “basın yayın yolu ile” tanımı çerçevesinde incelenecektir.

³⁹⁶ **İÇEL/ ÜNVER**, Kitle Haberleşme Hukuku, sh: 49-50.

³⁹⁷ **CAN**, Osman, Anayasa Değişiklikleri ve Düşünceyi Açıklama Özgürlüğü, www.anayasa.gov.tr/eskisite/anyarg19/can.pdf (Erişim Tarihi: 18.09.2007).

*“Hukuk, insan tininin dışı vurumu olarak hem insan tininin doğal özgürlüğünde temellenir hem de insan tininde mevcut olan kültürel sınırlar tarafından belirlenir. Hukuk, insan tininin iletişim özgürlüğünün bir ürünüdür. İletişim özgürlüğü olmadan hukuk da olmaz; bu özgürlüğün yok edilmesiyle hukuk da yok edilir; bu özgürlüğün zedelenmesi bile hukuku zedeler. Bu nedenle hukuk bu özgürlüğü korumak durumundadır.”*³⁹⁸

Yukarıda genel olarak çizilen çerçeve ışığında haberleşme özgürlüğünün unsurlarına bakılacak olursa, dört adet unsur göze çarpmaktadır. Bunlardan birincisi haber, kanı, bilgi ve düşüncelere serbestçe ulaşabilme hakkıdır. Haberleşme özgürlüğünden bahsedebilmek için öncelikli öneme sahip olan bu hak yurttaşlar tarafından haber alma, yayıncılar tarafından işe haber kaynağına ulaşma hakkı olarak tezahür eder. İkinci unsur ise düşünce ve kanıları serbestçe açıklayabilme hakkıdır. Bu hak, haberleşme özgürlüğü ile yukarıda açıklanan ifade özgürlüğü arasında köprü vazifesi görmektedir. Bu anlamda ifade özgürlüğünün kullanım alanı çerçevesinde yorum ve eleştiri yapma hakkını da kapsadığı kabul edilebilmektedir. Uygulamada yorum ve eleştiri hakkının sınırsız bir hak olmadığı ve belli şartlar altında kullanılabilmesine ilişkin birçok karar rastlamak mümkündür³⁹⁹. Üçüncü olarak haber

³⁹⁸ LAMPE, İfade Özgürlüğü, sh: 128.

³⁹⁹ Yargıtay 4. CD, 05.02.2007, E. 2004/13822 – K. 2007/1140 “Basın yoluyla işlenen suçlarda hukuka uygunluk nedenleri (ceza sorumluluğunu kaldıran nedenler) arasında yer alan ve kaynağını Anayasanın 28. ve devamı maddelerinden olan, "hakkın kullanılması" kapsamındaki haber verme ve eleştiri hakkının söz konusu olabilmesi için yapılan basın açıklamasının gerçek ve güncel olması, verilisinde kamu ilgi ve yararının bulunması ve olay ile olayın anlatılışı arasında fikri bağ bulunması gerekir. Bu unsurlardan birinin dahi gerçekleşmemesi haber verme ve eleştiri hakkını ortadan kaldırır ve fiili hukuka aykırı kılar”; Yargıtay HGK, 25.09.2002, E. 2002/4-615 – K. 2002/619 “Anayasanın 28. maddesindeki basının özgür olduğu güvencesi ve bu ilkeyi güçlendiren 5680 sayılı Basın Yasasının 1. maddesindeki düzenleme üzerinde durulmasında yarar vardır. Bu düzenlemede basının özgürce yayın yapmasının güvence altına alındığı görülmektedir. Basına sağlanan bu güvencenin nedeni ise; toplumun sağlıklı, mutlu ve güven içinde yaşayabilmesidir. Bu da Kişilerin dünyada ve özellikle içinde yaşadığı toplumda meydana gelen ve toplumu ilgilendiren konularda bilgi sahibi olması ile olanaklıdır. Kısacası basın, olayları izleme, araştırma, değerlendirme, yayma ve böylece kişileri bilgilendirme, öğretme, aydınlatma, yönlendirme yetki ve sorumluluğuna sahiptir. Bunun içindir ki basının yayın yaparken, yaptığı yayından dolayı eyleminin hukuka aykırılık teşkil edip etmediğinin değerlendirme ölçütleri genel anlamda hukuka aykırılığa ilişkin ölçütlerden farklı ele alınmalıdır. Ne var ki basının bu ayrılık taşıyan konumu ve özgürlüğü, tüm özgürlüklerde olduğu gibi sınırsız değildir. Bundan dolayıdır ki, basının bu özgürlüğü yayınlarında gerek Anayasanın Temel Hak ve Özgürlükler, bölümünde yer alan ve gerekse MK.nun 24 ve 25. maddelerinde ve özel yasalarda güvence altına alınmış bulunan kişilik haklarına saldırıda bulunmamak ve saygı göstermek, gibi ilkelerle sınırlıdır. Diğer taraftan, basının özgürlüğü ile kişilerin, kişilik değerlerinin karşı karşıya geldiği, hukuk düzenince koruma altına alınan yararların birbirine karşı çatışma içinde bulunduğu durumda temel ölçüt kamu yararı olmalıdır. Başka bir anlatımla yayın salt toplumun yararı gözetilerek yapılmalıdır. Bu yayın yapılırken objektif sınırlar içinde kalmalıdır. Ayrıca basının haber verme hakkı, gerçeklik, geçerlilik, güncellik, toplumsal ilgi, konu ile ifade arasında düşünsel bağlılık temel ilkelerine dayanmalıdır. Basın objektif sınırlar içinde kalmak suretiyle olay ve konu ile ilgili olan, görünen, bilinen herşeyi araştırıp olayları olduğu biçimi ile yayınlamalıdır. Buradaki gerçeklik somut gerçeklik olarak değil, o anda belirlenen ve var olan, orta düzeydeki kişilerce de yayının amacının anlaşılmasını ortaya koyacak bir gerçeklik, eş söyleyişle olayın haber yapıldığı andaki belirli biçimine uygunluk şeklinde anlaşılmalıdır. Yayının ancak

düşünce ve kanıların serbestçe yayma hakkından bahsetmek gerekmektedir. *İçel/Ünver* bu hakkın basın yönünden yazıların bir ön kontrole tabi tutulmadan basılabildesini gerektirdiği gibi, basılmış eserlerin de serbestçe dağıtılabildesini zorunluluğunu kapsadığını ifade etmektedirler. Bunun aksine bir tutumla doğrudan veya dolaylı olarak sansürü gündeme getirir ki gerek ulusal gerekse uluslar arası alanda basının sansüre tabi tutulamayacağını içeren “*sansür yasağı*” ihlal edilmiş olur⁴⁰⁰. Bilindiği üzere sansür, haber, düşünce ve bilgilerin basımı, dağıtımı, açıklanması safhalarından önce ön denetime tabi tutulması anlamına gelmektedir⁴⁰¹.

Anayasanın 26. maddesinde düzenlenen düşünceyi açıklama ve yayma özgürlüğünün haberleşme özgürlüğü ile olan ilişkisi bakımından yapılabilecek değerlendirmeler için yukarıda yapılan değerlendirmelere atıf yapılmakla yetinilecektir.⁴⁰²

Anayasanın 27. maddesinde⁴⁰³ düzenlenen bilim ve sanat özgürlüğünün haberleşme özgürlüğü ilişkisi de yine düşünceyi açıklama ve yayma özgürlüğü ile paralel olduğu gözlemlenmektedir. Çünkü söz konusu maddede herkesin bilim ve sanatı serbestçe öğrenme açıklama ve yayma özgürlüğüne sahip olduğunu ortaya konulmuştur. Burada “yayma” bir özgürlük alanı olarak kabul edildiği için bilim ve sanatın yayılmasını mümkün kılacak olan araçlar da bu kapsam içinde değerlendirilmelidir. Bu anlamda haberleşme özgürlüğü bu

maddi gerçekliği saptandıktan sonra verilebileceği şeklindeki düşüncenin kabul edilmesi halinde, haber verme ve konuyu aydınlatma hakkının özü sınırlandırılmış olur. Zira maddi gerçeğin araştırılıp ortaya çıkarılması çok zaman alacak ve bu durumda haberin güncelliği de ortadan kalkacaktır. Önemli olan olayların doğması ve bunların kamuya aktarılmasıdır. Bu ilkeleri gözetilen yayının Anayasa'ya, Basın Kanunu'na ve dolayısıyla hukuka uygun olduğu ve kişilik değerlerine saldırı teşkil etmeyeceği kabul edilmelidir”. (Kazancı İçtihat Programı – Offline)

⁴⁰⁰ Yargıtay 4. HD, 28.04.1997, E. 1987/2077 – K. 1987/3267 “*Genel hatlarıyla basının görevi, umumi yararlar açısından toplumu ilgilendiren ya da toplumun ilgilenmesi gereken konularda halkı, gerçekleri yansıtmak suretiyle ve objektif bir biçimde aydınlatmak, çeşitli sorunlarla ilgili eleştiri, yorum ve uyarılarla fertleri düşünceye sevk etmek, bilinçlendirmek, kamu görevlilerini harekete geçirmek ve daha önemlisi; kamu gücünü elinde tutanlar üzerinde toplumun denetimine aracı olmaktır. Basın, kamu görevi niteliğindeki bu denli etkili ve kapsamlı fonksiyonunu hiç bir baskı ve karşı koymaya maruz kalmadan ve çekinmeden yerine getirebilmesi için yasal kaynağı olan bir güce dayanmalıdır ki, bu güç Anayasanın 28. maddesinin öngördüğü “basın özgürlüğü”dür”. (Kazancı İçtihat Programı – Offline)*

⁴⁰¹ **SALİHPAŞAOĞLU**, Basın Özgürlüğü, sh:35.

⁴⁰² Bkz. Düşünce – İfade Özgürlüğü ve İnternet

⁴⁰³ **MADDE 27.** – (1) Herkes, bilim ve sanatı serbestçe öğrenme ve öğretme, açıklama, yayma ve bu alanlarda her türlü araştırma hakkına sahiptir. (2) Yayma hakkı, Anayasanın 1 inci, 2 nci ve 3 üncü maddeleri hükümlerinin değiştirilmesini sağlamak amacıyla kullanılamaz. (3) Bu madde hükmü yabancı yayınların ülkeye girmesi ve dağıtımının kanunla düzenlenmesine engel değildir.

düzenlemede dolaylı olarak güvenceye alınan bir özgürlük alanı olarak dikkati çekmektedir.

404

Haberleşme özgürlüğünün anayasal görünümü anlamında en önemli maddelerden biri de 28. maddedir. 28. maddenin ilk fıkrasına göre basın hürdür ve sansür edilemez. Aynı fıkranın devamında basım evi kurmak için izin ve mali teminat şartının konamayacağı belirtilmiştir. Böylece sansür yasağının konulması suretiyle özgürlükçe, demokratik rejimlerin standartlarına ulaşıldığı söylenebilir. 28. maddenin ikinci fıkrasında ise devlete bir görev yüklenmiştir. Buna göre devlet haberleşme özgürlüğü kapsamında basın ve haber alma özgürlüklerini sağlayacak tedbirleri alacaktır. Kuşkusuz devletin alacağı bu tedbirler müdahalede bulunmak şeklinde değil özgürlüğün kullanımını kolaylaştırıcı yasal düzenlemeleri sağlamak şeklinde olmalıdır. *Özek'e* göre, özgür bilgi dolaşımını engelleyen her olgu sansür olarak kabul edilmelidir. Dolayısıyla haberin kaynağına ulaşmaktan, haberin alıcıya vardığı sürece kadar, idari, kanuni, yargısal eylemlerle yapılan her türlü özgür bilgi sınırlaması sansür anlamına gelir⁴⁰⁵.

Haberleşme Özgürlüğünün uluslar arası hukuk bakımından nasıl düzenlendiğine gelinecek olursa yine yukarıda düşünce ve ifade özgürlükleri için yapılan açıklamalara paralel bir eğilimin varlığından bahsedilebilir. Şöyle ki; Avrupa İnsan Hakları Sözleşmesi md. 9 (Düşünce, Vicdan ve Din Özgürlüğü) ve md. 10 (İfade Özgürlüğü), Birleşmiş Milletler İnsan Hakları Bildirgesi md. 18 ve md. 19 , Medeni ve Sosyal Haklar Uluslar Arası Sözleşmesi md. 18 ve md.19 gerek düşünce özgürlüğü gerek ifade özgürlüğü ve gerekse basın ve haberleşme özgürlüğü bakımından ortak hükümleri içermektedir. Çünkü bu özgürlük alanları tabiatları gereğince birbirlerini tamamlayıcı niteliktedirler. Düşünceyi açıklama özgürlüğünün bir kullanım biçimi olan basın özgürlüğü, haberlerin, düşünce ve kanaatlerin izne ve sansüre tâbi olmaksızın basın yolu ile serbestçe yayılabilmesi olarak tanımlanabilir. Zaman içerisinde haberlerin, düşünce ve kanaatlerin radyo, televizyon (bunlara yakın geçmişte internet de eklenmiştir) gibi basın dışındaki kitle iletişim araçları ile de yayılabilmesi sonucunda hepsini içeren bir üst kavram olarak "haberleşme özgürlüğü" tercih edilmiştir.⁴⁰⁶ Bu yüzden basın ve haberleşme özgürlüğünün uluslara arası hukuktaki temel düzenlemeleri bakımından da bundan önceki açıklamalara göndermede bulunmak hatalı olmaz.

⁴⁰⁴ CAN, Osman, Anayasa Değişiklikleri ve Düşünceyi Açıklama Özgürlüğü, www.anayasa.gov.tr/eskisite/anyarg19/can.pdf (Erişim Tarihi: 18.09.2007)

⁴⁰⁵ GEDİK, Kitle Haberleşme Özgürlüğü, sh: 88'den naklen.

⁴⁰⁶ İÇEL, Kayıhan, Haberleşme Özgürlüğü, in: İÜHFM, C:41, S:1-2, İstanbul, 1975, sh:

4.2.2.1.- Ceza Hukuku Perspektifinden İnternetin Haberleşme Özgürlüğü İle İlişkisi

Her şeyden önce 5237 sayılı TCK md. 6/1- g'de tanımlanan şekliyle, bir suçun basın-yayın aracılığıyla işlenmesinde kullanılan araçlar her türlü yazılı, görsel, işitsel ve elektronik kitle iletişim araçlarıdır. Bu çerçevede internetin de bir kitle iletişim aracı olarak kabul edildiğinden şüphe yoktur. Gerçekten madde metninde “elektronik kitle iletişim aracı” ifadesi özellikle interneti kapsam dahiline sokmak için kullanılmıştır. Ancak şu haliyle internetin elektronik bir kitle iletişim olarak kabul edilmeyeceği tartışma götürülebilir. Çünkü internet sadece elektronik olmayıp elektromanyetik, dijital öğeleri de barındırmaktadır. Ancak normun düzenlenme amacından bu tabirin internet için kullanıldığı kabul edilmelidir.

Daha önce düşünce ve ifade özgürlüğü ile ilgili açıklamalarda özellikle haber verme sınırları ve eleştiri amacıyla yapılan düşünce açıklaması kriterlerinin bu alana ilişkin hak kullanımı sınırlarını ortaya koyduğu ve haberleşme özgürlüğünü de yakından ilgilendirdiği ifade edilmiştir. Bu yönde Yargıtay'ın birçok kararına rastlanmaktadır. Yargıtay verdiği bir kararında, haber verme ve eleştiri hakkının söz konusu olabilmesi için yapılan basın açıklamasının gerçek ve güncel olması, verilisinde kamu ilgi ve yararının bulunması ve olay ile olayın anlatılışı arasında fikri bağ bulunması gerektiği ortaya konulmuştur⁴⁰⁷. Başka bir kararında ise, gazetede haberin gerçeklik derecesini, yapılan ve yapılacak harcamaların

⁴⁰⁷ “Basın yoluyla işlenen suçlarda hukuka uygunluk nedenleri (ceza sorumluluğunu kaldıran nedenler) arasında yer alan ve kaynağını Anayasanın 28. ve devamı maddelerinden olan, "hakkın kullanılması" kapsamındaki haber verme ve eleştiri hakkının söz konusu olabilmesi için yapılan basın açıklamasının gerçek ve güncel olması, verilisinde kamu ilgi ve yararının bulunması ve olay ile olayın anlatılışı arasında fikri bağ bulunması gerekir. Bu unsurlardan birinin dahi gerçekleşmemesi haber verme ve eleştiri hakkını ortadan kaldırır ve fiili hukuka aykırı kılar. Somut olayda; G. Gazetesi adlı 18.01.2002 günlü gazetede "Esrarengiz mektuplar" başlıklı yazıda Alanya'dan postaya verilmiş isimsiz mektupların G. kişiler tarafından yazılmış olduğu belirtilerek mektupların içeriğinde "Belediye Başkanı B. A.'un parti yandaşlarıyla birlikte Belediyeyi soyup soğana çevirdiği... seni makam hırsız seni... senin gibi üç beş hırsızın yüzünden... bu hırsızlar Ş. Ç., E. A., Ö. G. ve İ. H.'den spor kulübü kanalı ve aktarılan paraları başkan ve 3-5 hırsız yerse (Ş.Ç., Ö.G, E.A, A.B.) Yine Ö. G. S. geceleri belediyeye hayali mazot verip milyarlar götürürse... yeni yapılan Pazar yeri ve fuar alanında aynı hırsızlara yada birinci derece yakınlarına sahte fatura karşılığı yerler verirse...yalnızca sit alanı hayalini imar planı için Kerim B.'a ödenen 300 milyar! Geçersiz iptal edilecek bir plan. Parayı başkanla bölüşebilmek için bu plan şart. Belediye fare çiftliği oldu. Anası da babası da B. A.-Ş. Ç. Yavruları ise çok..." biçimindeki yazıda içerik itibarıyla, haber sınırını aşan, muhataplarını küçük düşürecek nitelikte soyut suçlama ve iddialara yer verildiği, bu nedenle sanığın eyleminin haber verme özgürlüğü sınırının aşılması suretiyle hakaret suçunu oluşturduğu gözetilerek; 5237 Sayılı Yasanın 7/2, 5252 Sayılı Yasanın 9/3. madde ve fıkraları uyarınca 765 ve 5237 sayılı TCY.larının ilgili hükümlerinin karşılaştırılıp sanık yararına olan yasa hükümleri saptanarak sonucuna göre hüküm kurulması zorunluluğu, **SONUÇ** : Bozmayı gerektirmiş ve katılanlar Ş. Ç., B. A., Ö. G. ve E. A. vekili ile O Yer Cumhuriyet Savcısının temyiz nedenleri ile tebliğnamedeki düşünce yerinde görüldüğünden HÜKMÜN BOZULMASINA, yargılamanın bozma öncesi aşamadan başlayarak sürdürülüp sonuçlandırılmak üzere dosyanın esas/hüküm mahkemesine gönderilmesine oy birliğiyle karar verilmiştir.” Yargıtay 4. CD, 05.02.2007, E. 2004/ 13822 – K. 2007/ 1140 (Kazancı İçtihat Programı – Offline).

kaynaklarının yazıda belirtilen mahiyetini arařtırmak, büyük ölçüde doğrulandıđı takdirde güncellik, okuyucunun gereksiz merak duygularını doğurma yerine, bilinmesinde kamu yararı bulunması, kamuoyunun aydınlatılması, işlenen suç ile içerdıđi düşünce arasındaki bağlantının varlıđı açılarından değerlendirilmek suretiyle, yazının haber verme çerçevesinde ve bu haberin çerçevesini ařtıđı takdirde eleřtiri bağlamında kalıp kalmadıđının tartışılmadan yetersiz gerekçe ile hüküm kurulması hatalı bulunmuřtur⁴⁰⁸.

Haber verme hakkının sınırları ile ilgili sadece Yargıtay'ın Ceza Daireleri deđil, Hukuk Dairelerinin de verdiđi kararlara rastlanmaktadır. Örneđin Yargıtay Hukuk Genel Kurulu verdiđi bir kararında haber verme sınırını řöyle belirlemektedir;

“Basının haber verme hakkı, gerçeklik, geçerlilik, güncellik, toplumsal ilgi, konu ile ifade arasında düşünsel bađlılık temel ilkelerine dayanmalıdır. Basın objektif sınırlar içinde kalmak suretiyle olay ve konu ile ilgili olan, görünen, bilinen herřeyi arařtırıp olayları olduđu biçimi ile yayınlamalıdır. Buradaki gerçeklik somut gerçeklik olarak deđil, o anda belirlenen ve var olan, orta düzeydeki kişilerce de yayının amacının anlaşılmasını ortaya koyacak bir gerçeklik, eř söyleyiřle olayın haber yapıldıđı andaki belirli biçimine uygunluk řeklinde anlaşılmalıdır. Yayının ancak maddi gerçekliđi saptandıktan sonra verilebileceđi řeklindeki düşüncenin kabul edilmesi halinde, haber verme ve konuyu aydınlatma hakkının özü sınırlandırılmış olur. Zira maddi gerçeđin arařtırılıp ortaya çıkarılması çok zaman alacak ve bu durumda haberin güncelliđi de ortadan kalkacaktır. Önemli olan olayların doğması ve bunların kamuya aktarılmasıdır. Bu ilkeleri gözetken yayının Anayasa'ya, Basın Kanunu'na ve dolayısıyla hukuka uygun olduđu ve kişilik deđerlerine saldırı teřkil etmeyeceđi kabul edilmelidir.”⁴⁰⁹

⁴⁰⁸ Yargıtay 4. CD, 10.11.1997, E. 1997/ 9060 – K. 1997/ 9712. Aynı yönde başka bir karar olarak; “Demokratik toplumlar, temel hak ve özgürlüklere dayanan toplumlardır. Bu tür toplumlarda Devletin görevi, temel hak ve özgürlükleri korumak ve geliřtirmektir. Temel hak ve özgürlükle arasında düşünce ve kanaati açıklama özgürlüđünün önemli bir yeri bulunmaktadır. Bu özgürlüđün kullanılabilmesinin en önemli yollarından birisi de basındır. Geneli ilgilendiren ya da ilgilendirmesi gereken tüm olaylar hakkında, halkı objektif ve gerçekleri yansıtabilecek biçimde aydınlatmak, çeřitli sorunlar üzerinde kamuoyunu düşünmeye çağırarak tarzda tartışmalara açmak, onu toplumsal ve siyasal oluşumlar üzerinde doğru ve gerçeđe uygun bilgilerle donatmak, yöneticileri eleřtirmek, uyararak ve bu yöntemlerle denetlemek, ayrıca içinde yařadıđı toplumun ve tüm insanlıđın sorunları konusunda bireyi bilinçlendirmek durumunda olan basına, bu ödevlerini yerine getirirken ihtiyaç duyacađı bir kısım haklar da tanınmıştır. Bunlar bilgi edinme, yayma, eleřtirme, yorumlama ve eser yaratma haklarıdır. Temelini Anayasanın 28. vd. maddelerinden alan ve 5187 sayılı Basın Yasasının 3. maddesinde düzenlenen bu haklar, basın yoluyla işlenen suçlarda, hukuka uygunluk nedenlerini oluşturur. Bilgiyi yayma, eleřtirme ve yorumlama haklarının kabulü için açıklama, eleřtiri veya deđer yargısı biçimindeki bilginin gerçek ve güncel olması, açıklanmasında kamunun ilgi ve yararının bulunması, açıklanış řekli ile konusu arasında düşünsel bir bađ bulunması, açıklamada “küçültücü” sözlerin kullanılmaması gerekir.” Yargıtay CGK, 11.07.2006, 2006/ 4-162-18 (Kazancı İřtihat Programı – Offline).

⁴⁰⁹ Yargıtay HGK, 25.09.2002, E. 2002/ 4- 615 – K. 2002/619 (Kazancı İřtihat Programı – Offline).

Yargıtay Hukuk Genel Kurulu vermiş olduğu bir başka karara göre, haber olduğu biçimi ile verilmeli ve kişisel katkı yer almamalıdır. Gerek yazılı ve gerekse görsel basın bu işlevini yerine getirirken, özellikle yayının gerçek olmasını, yayında kamu yararı bulunmasını, toplumsal ilginin varlığını, konunun güncelliğini ve haber verilirken özle biçim arasındaki dengeyi de korumalıdır. Bu ilke ve kurallar gözetilmeden yapılan yayın hukuka aykırılığı oluşturur ve böylece kişilik hakları saldırıya uğramış olur⁴¹⁰. Yine Yargıtay Hukuk genel Kurulunun haber verme özgürlüğünün sınırları konusunda yakın tarihte vermiş olduğu bir kararında basın özgürlüğü ile kişilik haklarının karşı karşıya kaldığı durumlarda bu iki değerden birinin tercih edilmesi gerektiğinde önceliği daima kamu yararı kıstasına göre belirlemek gerektiği belirtilmiştir.⁴¹¹

Yukarıda verilen kararlar çerçevesinde basın yayın aracılığıyla gerçekleştirilen eleştiri amaçlı düşünce açıklaması eylemi ve haber verme etkinliği kapsamında belirlenen tüm kriterler, söz konusu eylemlerin internet aracılığıyla gerçekleştirilmesinde de aynen kullanılmalıdır. İnternetin multimedya kimliği, daha geniş kitlelere daha çabuk erişebilmesi ve etki alanını daha geniş olması diğer kitle haberleşme araçları ile internet arasında internetin aleyhine bir farklılık yaratılmasına sebebiyet veremez. Burada önemli olan bir hususun altı çizilmelidir. Şayet bir açıklama yukarıda mahkeme kararlarıyla da belirlenen ölçütlere uyum göstermediği takdirde, bu açıklamanın başka bir temel hak ve özgürlüğün koruma alanında olmadığı bir ön kabul olarak kabul edilemez. Dolayısıyla haber verme sınırını aşılması otomatik bir cezalandırılabilme koşulu olarak düşünülmemelidir. Haber verme sınırı aşan ifadenin/ açıklamanın ifade özgürlüğü başta olmak üzere diğer özgürlük alanlarının koruma kapsamında bulunup bulunmadığı değerlendirilmelidir.

Bu özgürlük alanı ile internet ilişkisi incelerken 28 Mayıs 2003 tarihli Avrupa Konseyi Bakanlar Komitesi'nin 840. toplantısında kabul edilen "İnternette İletişim Özgürlüğü

⁴¹⁰ Yargıtay HGK, 14.12.2005, E. 2005/ 4- 719 – K. 2005/ 719 (Kazancı İçtihat Programı – Offline).

⁴¹¹ "Dava, yayın yoluyla kişilik haklarına saldırı iddiasına dayalı manevi tazminat talebine ilişkindir. Basın özgürlüğü ile kişilik hakları karşı karşıya geldiğinde, bu iki değerden birinin üstün tutulması gerekir. Bunun için temel ölçüt kamu yararadır. Yayın, yalnızca toplum yararı gözetilerek yapılmalıdır. Basın, objektif sınırlar içinde yayın yapmalıdır. Yayın gerçek olmalı, toplumsal ilgi, güncellik gözetilmeli ve özle biçim arasındaki denge korunmalıdır. Yayınlanmasında kamu yararı bulunan gerçek ve güncel bir haberin özle biçim arasındaki denge korunarak verilmesi halinde hukuka aykırılık ortadan kalkacağından basın sorumlu tutulamaz. Dosya kapsamından, davalı yazarın davacının kitabını kamuoyuna duyururken içeriğini eleştirdiği, eleştirilerini çarpıcı sözlerle ifade ettiği, yayın gerçek ve güncel olduğu gibi özle biçim arasındaki dengenin de korunduğu anlaşılmaktadır." Yargıtay CGK, 19.03.2008, E: 2008/4- 263 – K: 2008/262, Kaynak: Kazancı içtihat Programı-Online, Erişim Tarihi: 11.01.2009, Saat: 12:20)

Deklarasyonu” ile belirlenen temel ilkeleri ortaya koyarak açıklanması yerinde olacaktır.⁴¹² Söz konusu deklarasyonun birinci maddesi üye devletler tarafından internet içeriklerine diğer içerik dağıtım araçlarına getirilen düzenlemeler dışında herhangi bir sınırlama getirilmemesini düzenlerken internetin diğer kitle iletişim araçlarından farklı olmadığı vurgulanmak istenmiştir. Deklarasyonun önemli maddelerinden 3. maddede devletin internet içeriklerine ilişkin önceden denetimde bulunmaması gerektiğini vurgulamıştır. Buna göre ;

“Kamu kurumları, genel filtreleme veya engelleme tedbirlerine başvurarak, İnternette bilgi ve diğer iletişimlere, sınırlara bakılmaksızın, kamunun erişimini engellememelidirler. Ancak bu durum, çocukların korunması için, özellikle okul ve kütüphaneler gibi çocukların erişim sağlayabileceği yerlerde filtreleme sistemlerinin kurulmasına engel teşkil etmez.

İnsan Hakları ve Temel Özgürlüklerin Korunması Sözleşmesinin 10 uncu maddesinin 2 inci paragrafında yer alan tedbirlere bağlı kalmak kaydıyla, yetkili ulusal otoritelerin söz konusu içeriğin yasa dışılığı konusunda geçici veya nihai bir karar vermesi halinde, bu içeriğin kaldırılması veya siteye erişimin engellenmesi yönünde önlemler alınabilir.”

Yine deklarasyonun 6. maddesinin *“Servis Sağlayıcıların İnternet İçeriğinden Dolayı Sınırlı Sorumluluğu”*nu düzenleyen üçüncü paragrafında göre Servis sağlayıcıların işlevlerinin daha geniş olduğu ve 3. kişilerden kaynaklanan içeriği depoladıkları durumlarda, eğer servis sağlayıcılar onların (bilgi veya servislerin) ulusal hukukta tanımlandığı üzere yasadışı özelliklerinden veya bir zarara uğrama iddiası karşısında faaliyetin veya bilginin yasa dışılığını ortaya çıkaran olaylardan veya koşullardan haberdar olur olmaz bilgiye veya servislere erişimi önlemek veya bunları kaldırmak için süratle hareket etmezlerse, üye devletler servis sağlayıcıları müşterek sorumlu tutabilirler. Ancak hemen dördüncü paragrafında bir önceki paragrafta belirtildiği üzere servis sağlayıcıların ulusal hukuk uyarınca yükümlülüklerini tanımlarken, her şeyden önce kullanıcıların bilgiye ulaşmadaki benzer hakları kadar, bilgiyi ulaşılabilir hale getirenlerin ifade özgürlüğüne de saygı göstermek için yeterli özen gösterilmesi gerektiği açıkça vurgulanmıştır.

Yukarıda aktarılan düzenlemeler şunu göstermektedir ki internet artık hem ulusal hem de uluslar arası hukuk düzleminde etkili bir kitle iletişim aracı olarak kabul edilirken diğer

⁴¹² Deklarasyonun tam metni için bkz. http://www.ivhp.org.tr/pages/infDetail.php?a_id=34&c_id=7 (Erişim Tarihi: 20.09.2007, Saat: 14:00).

kitle iletişim araçları için kabul gören hak ve özgürlüklerin internet için de söz konusu olduğu görülmektedir.

Türk Ceza Kanunu bakımından internetin bir kitle haberleşme aracı olarak kabulü çerçevesinde özel kısımda yer alan ve haberleşme özgürlüğünü güvence altına alan suç tipleri bakımından da internetin öncelikli olarak ele alınması gerektiği anlaşılmaktadır. Keza buna ilişkin değerlendirmeler üçüncü bölümde özel suç tiplerinin internet açısından incelenmesinde ele alınacaktır.

5.- SUÇA ETKİ EDEN NEDEN OLARAK ALENİYET UNSURUNUN İNTERNET ARACILIĞIYLA İŞLENEN SUÇLAR BAKIMINDAN DEĞERLENDİRİLMESİ

5.1.- Genel Açıklamalar

5237 sayılı TCK md. 6/1-g'ye göre internetin bir kitle haberleşme aracı olarak basın-yayın yoluyla suç işlemede elverişli araç olduğu her somut olayda yeniden değerlendirilip somut olayda hangi bağlamda bir araç olarak kullanıldığına bakmak gerekir. Şayet bir kitle haberleşme aracı olarak kullanıldıysa kanunun açık hükmü gereği 5237 sayılı TCK'de yer alan ve basın yayın aracılığıyla işlenmesi mümkün olan her suçta kullanılabilir.

Bilindiği üzere 5237 sayılı TCK'de basın yayın yolu ile işlenmesi mümkün olan birçok suç tipi mevcuttur. Özellikle içerik suçu olarak ifade edilebilecek intihara yönlendirme, şerefe karşı işlenen suçlar, özel yaşamın gizliliğine karşı işlenen suçlar, kamu barışı aleyhine işlenen suçlar gibi suçlarda, suç teşkil eden içeriğin çok sayıda kişinin bilgisine sunulması, daha açık bir ifade ile çok sayıda kişi tarafından erişilebilir kılınması suçun mağdur üzerinde yarattığı olumsuz etkinin daha da büyümesine neden olmaktadır. Günümüzün internet teknolojisindeki önü alınamaz gelişme klasik basın- yayın araçlarıyla kıyaslanamaz bir hızda her türlü içeriğin kitlelere ulaşmasını mümkün kılmaktadır⁴¹³. Bu nedenle içerik suçu olarak değerlendirilen birçok suçta, suçun basın yayın yoluyla işlenmesi ağırlatıcı neden olarak düzenlenmiştir.

Ancak bu yöndeki eğilime paralel olarak suçun alenen işlenmesinin de nitelikli bir hal veya doğrudan bir suç unsuru olarak düzenlenmesi gerek 5237 sayılı TCK'nin görüşmeleri

⁴¹³ AKGÜL, İnternet Yasakları ve Hukuk, sh: 358.

esnasında gerekse tasarının kanunlaşmasının ardından sıkça eleştirilmiş bir konu olmuştur. Özellikle basın çevrelerinden yükselen eleştirilerin temelinde suçun basın-yayın yoluyla işlenmesinde aleniyetin gerçekleştiği, buna rağmen ayrıca suçun alenen işlenmesinin farklı bir ağırlaştırıcı neden olarak düzenlenmesinin ceza adaleti bakımından büyük zararlara sebebiyet vereceği düşüncesi ve kaygısı etkili olmuştur⁴¹⁴. Nitekim 29.05.2006 tarih ve 5377 sayılı Kanunla birçok maddede aynı anda yer alan “suçun basın – yayın yoluyla işlenmesi” ve “suçun alenen işlenmesi” nitelikli unsurları ile ilgili şu ortak gerekçeyle değişiklik yapılmıştır:

“Suçun basın ve yayın yoluyla işlenmesi hali de, aleniyetin gerçekleşiş şekillerinden birini oluşturmaktadır. İntihara teşvik suçuyla ilgili olarak aleniyet bir nitelikli unsur olarak belirlendiği için, söz konusu suçun basın yayın yoluyla işlenmesi, bu suç açısından ayrı bir nitelikli unsur olarak görülmemiştir.”

Her ne kadar tüm TCK sistemini etkileyecek bir değişiklik gibi görünse de bazı maddelerde halen her iki durum da nitelikli unsur olarak muhafaza edilmektedir. Bu eleştiri, üçüncü bölümde özel suç tiplerine bağlı yapılacak yorumlar ile detaylandırılacağı için burada üzerinde durulmayacaktır. Ancak şu haliyle bile önemli bir değişikliği barındıran bu yaklaşım farkının basın- yayın aracı olarak klasik kitle haberleşme araçları gazete, dergi, televizyon, radyo bakımından doğuracağı etki açık ve tartışılmazdır. Ancak bir basın- yayın aracı olarak kullanılabilen internet için bir takım tereddütler doğmaktadır. Bu tereddütlerin çoğu internetin karma yapısından ve teknolojik gelişmeler karşısında koruduğu dinamik yapısından kaynaklanmaktadır. Bu nedenle aleniyet kavramının internet açısından değerlendirilmesi, aleniyetin nitelikli bir unsur olarak bulundurulduğu suçlarda araç olarak kullanılıp kullanılmayacağını ortaya koyacaktır.

5.2.- Aleniyet Kavramı

Gerek 5237 sayılı gerekse 765 sayılı TCK’de aleniyet ayrı bir tanım olarak yapılmamıştır. Dolayısıyla kanun koyucunun kavram olarak aleniyet tercihini tespit etmek güçtür. Ancak gerek uygulama gerekse doktrin 765 sayılı TCK’deki bir hükümde yapınla düzenlemeyi kanunun bütününe etkiler tarza bir aleniyet çerçevesi çizdiğini ve bu çerçevenin de 5237 sayılı TCK dönemi uygulamalarına etki ettiği düşünülmektedir. Söz konusu madde

⁴¹⁴ YILDIZ, Ali Kemal, 5237 Sayılı Türk Ceza Kanunu, İstanbul, 2007, sh:184.

“Askerleri kanuna itaatsizliğe veya yeminlerini bozmaya teşvik etmek” suçuna ilişkin 153. maddedir. Bu maddeye göre suç teşkil eden fiiller

- a- Matbuat vasıtasıyla veya herhangi bir propaganda vasıtasıyla,
- b- Umumi veya umuma açık bir mahalde ve birden ziyade kişinin huzurunda,
- c- Toplanılan mahal veya içtimaa iştirak edenlerin adedi veya toplantının mevzuu ve gayesi itibari ile hususi mahiyeti haiz olmayan bir içtimada işlenmiş olursa Ceza Kanununun tatbikinde aleni olarak işlenmiş sayılır.

Görüldüğü üzere kanun koyucu 765 sayılı TCK md. 153 ile suçun alenen işlenmesinin çerçevesini belirlemiştir. Ancak bu belirlemenin sadece bahsi geçen madde için mi yoksa tüm TCK için mi geçerli olduğuna ilişkin tartışmalar mevcuttur⁴¹⁵. Bir görüşe göre, burada çizilen çerçeve aleniyet kavramının tanımlaması niteliğinde ve genel hükümler dairesinde düzenlenmesi gereken bir husustur. Kanun koyucu bunu özel hükümlerde düzenleme tercihinde bulunduğuna göre bu düzenleme sadece md. 153 için geçerlidir⁴¹⁶. Bu görüşü karşısında olan bir başka görüş ise iki argümanla tezlerini savunmaktadırlar. Birincisi maddenin sonunda “...*Ceza Kanununun tatbikinde alenen işlenmiş sayılırlar.*” demek suretiyle kanun koyucu bu aleniyet tespitini sadece ilgili maddeyle sınırlı tutmayıp, aleni işlenmesi düzenlenmiş tüm suç tipleri için geçerli kılmıştır⁴¹⁷. İkincisi ise aleniyetin genel hükümlerde tanımlanması gerektiği itirazına yöneliktir. Buna göre 765 sayılı TCK Özel Hükümlerde düzenlenen birçok suç tipinde, Genel Hükümlerde tanımlanmamış birçok kavramın gerek madde içinde gerekse madde gerekçesinde tanımlandığı, dolayısıyla bir kanunda tüm tanımların aynı maddede toplanmasının bir zorunluluk olarak ortaya konulamayacağını ifade etmektedirler⁴¹⁸.

Bununla beraber, bazı yabancı kanunlarda da aleniyete ilişkin bir takım tespitler yapıldığı görülmektedir. Örneğin Fransız Ceza Hukuku md. 23’de aleniyetin, “*herkese açık*

⁴¹⁵ SANCAR, Türkan Yalçın, Alenen Tahkir ve Tezyif Suçları, 2. Baskı, Ankara, 2006, sh: 171.

⁴¹⁶ “... 153. maddedeki aleniyeti tarif eden fıkra hükmü, ancak bu maddede yazılı suça münhasır olup diğer maddelere şamil değildir. Çünkü sözü geçen fıkra umumi hükümler kısmında veya müşterek fasılda yer almamıştır. 153. maddenin suçun alenen işlenmesi halinde uygulanacak ceza gösterildikten sonra buradaki aleniyetten maksadın ne olduğu belirtilmek amacıyla maddeye ilave edilmiştir. Binaenaleyh diğer maddelerdeki aleniyet unsurunun bu fıkraya göre değil, umumi kaide ve prensiplere göre tayini iktiza eder (I. CD. 25. 9.1945, 2547/2056)”. SANCAR, Alenen Tahkir ve Tezyif Suçları sh. 171, 58 numaralı dipnottan naklen.

⁴¹⁷ SANCAR, Alenen Tahkir ve Tezyif Suçları sh. 172.

⁴¹⁸ SANCAR, Alenen Tahkir ve Tezyif Suçları sh. 173.

yerlerde veya toplantılarda söylenen söz, haykırış veya tehditlerle yahut sözü geçen yerlerde satılan dağıtılan satışa arz edilen veya teşhir olunan yazı veya basılı eserlerle yahut halkın görmesine teşhir edilen duvar ilanı ve afişlerle” gerçekleştirileceği düzenlenmiştir. Bunun dışında İtalyan Ceza Hukuku md. 266/son hükmünce, bir hareket şu üç durumdan birinin varlığı halinde aleni sayılacaktır.

- 1.Suç, basın aracılığı ile veya herhangi bir propaganda aracı ile işlenmişse;
- 2.Suç umumi veya umuma açık bir mahalde ve birden fazla kimsenin önünde işlenmişse ,
- 3.Suç toplanılan yer veya toplantıya katılanların sayısı veya toplantının konusu ve amacı bakımından özel nitelikte olmayan bir toplantıda işlenmişse, alenidir.

Ayrıca Avusturya Ceza Kanununun md. 69’da aleniyet “doğrudan doğruya geniş bir şahıs kitlesi tarafından algılanabilecek hareketler” olarak tanımlanırken, Brezilya Ceza Kanunu md. 233’de “ umumi yer, halka açık yer veya herkesin bakabileceği yer” şeklinde ifade etmiştir. Arjantin Ceza Kanunu md. 129’a göre ise özel yerlerde işlenen fiillerin istenmeden görülmesi halinde de eylem alenen gerçekleşmiş kabul edilir.

Doktrinde de aleniyet ile ilgili bir çerçeve çizme girişimlerine rastlanmaktadır. Örneğin *Erem/ Toroslu*’ya göre, kanunda sadece alenen teriminin kullanılması ve bunun dışında suçun işlendiği mahalli belirleyen hususlara hiç yer verilmemesi alenen deyiminin geniş kapsamda anlaşılmasının sebebiyet vermektedir⁴¹⁹. *Centel/ Zafer/ Çakmut* da, aleniyet için aranan temel ölçütün fiilin belli olmayan ve birden fazla kişiler tarafından algılanma olanağının bulunmasıdır⁴²⁰. Fiilin belirsiz sayıda kişiler tarafından işitilebilecek, görülebilecek ve algılanabilecek bir ortamda veya çok sayıda kişinin öğrenmesini sağlayacak herhangi bir araçla işlenmesi durumunda aleniyet gerçekleşmiş olur. *Tezcan/ Erdem/ Önok* ise, bir suçun oluşmasında fiilin belirsiz sayıda kişi tarafından algılanabilir kılınmasını aleniyet için yeterli görmüşlerdir⁴²¹.

Konuyla ilgili Yargıtay’ın bir çok kararda aleniyete ilişkin tartışmalarda bulunduğu görülmektedir. Örneğin bir kararında sövme içerikli bir yazının bir sokak duvarına yazılması

⁴¹⁹ EREM, Faruk/ TOROSLU, Nevzat, Türk Ceza Hukuku Özel Hükümler, 8. Baskı, Ankara, 2000, sh: 226.

⁴²⁰ CENTEL, Nur/ ZAFER, Hamide/ ÇAKMUT, Özlem, Kişilere Karşı İşlenen Suçlar, C: 1, İstanbul, 2007, sh: 243 – 244.

⁴²¹ TEZCAN, Durmuş/ ERDEM, Mustafa Ruhan/ ÖNOK, Murat, Ceza Özel Hukuku, 4. Baskı, Ankara, 2006, sh: 359.

olayında, sokağın herkesin bulunabileceği umumi bir yer olmasından dolayı aleniyet unsurunun gerçekleştiği kabul edilmiştir⁴²². Yargıtay vermiş olduğu başka bir kararında ise çok sayıda kişinin anlamasını sağlayabilecek koşullar altında işlenmiş suça, açıklıkla alenen işlenmiş gözü ile bakılacağını ve açıklığın varlığı için çok kimsenin sövmeden haberdar olmasının olanaklı bulunması yeterli olduğunu ifade etmiştir⁴²³. Buna karşın bir apartman holünde⁴²⁴ veya bir derslikte⁴²⁵ işlenen hakaret suçlarında Yargıtay, suçun işlendiği yer bakımından aleniyetin oluşmadığına karar vermiştir.

Gerek doktrin gerekse Yargıtay uygulamaları şunu açık bir şekilde ortaya koymaktadır ki, bir suçun alenen işlenebilmesi için belirsiz sayıda kişi tarafından suç teşkil eden eylemin bilinebilir olması gerekmektedir. Burada dikkati çeken husus 5237 sayılı TCK'de de arandığı üzere belirsiz sayıda kişinin bizzat suç teşkil eden eylemi bilmeleri gerekmemektedir. Bilinebilir olmak yani olanaklılık esastır. Örneğin bir gazeteyi o gün çok az kişi okumuş olabilir ve hatta hiç kimse okumamış olabilir. Ancak bir hakaretin herkesin erişebileceği bir gazetede yayınlanmış olması aleniyet unsurunun gerçekleşmesi için yeterlidir. Ayrıca belli sayıda kişinin bu hakareti okumuş olması aranmaz. İşte bu noktada bir hususun daha altının çizilmesi gerekmektedir. O da aleniyet ile ihtilat arasındaki farktır.

⁴²² “Sanık Süleyman, diğer sanıklar İbrahim ve Gürhan'ın azmettirmesi sonucu müsnet suçu işlediği anlaşılacakla mahkemenin kabulünde isabetsizlik görülmediğinden tebliğnamenin 2 nolu bozma düşüncesine iştirak edilmemiştir. Dosya içeriğine göre sair temyiz itirazları yerinde görülmemiştir. Ancak; sövme içeren sözlerin yazıldığı mahallin, umumi bir yer olan sokakta gelip geçen herkesin rahatlıkla görebileceği duvar olduğu ve bu durumuyla yazıların TCK.nun 480/4. fıkrasında gösterilen (teşhir olunmuş yazı) niteliğinde olduğu cihetle, sanığın eyleminin TCK.nun 482/son madde ve fıkrasına uyduğu gözetilmeden aynı yasanın 482/3. madde ve fıkrasına göre hüküm kurulması,...” Yargıtay 2. CD., 13.02.2004, E. 2002/17162 – K. 2004/2271. (Kazancı İçtihat Programı - Offline)

⁴²³ Bkz. Yargıtay CGK, 13.02.1984, E. 1983/2- 344 – K. 1984/70 (Kaynak: Kazancı İçtihat Programı - Offline.)

⁴²⁴ “Sanığın nüfus kaydına uygun sabıka kaydının getirilmemesi aleyhe temyiz olmadığından boza nedeni yapılmamıştır. Dosya içeriği itibariyle sair temyiz itirazları yerinde görülmemiştir. Ancak, Tanık Ahmet'in beyanından sanığın müştekiye ait aleni olmayan evin holünde sövdüğü anlaşılacakla, sanığın TCK.nun 482/2. maddesi yerine aynı maddenin 3. fıkrası ile tecziyesine karar verilmesi;...” Yargıtay 2. CD, 03.07.2003, E. 2001/39230 – K. 2003/8078. (Kaynak: Kazancı İçtihat Programı – Offline)

⁴²⁵ “Temyiz isteğinin reddi nedenleri bulunmadığından işin esasına geçildi. Vicdani kanunun oluştuğu duruşma sürecini yansıtan tutanaklar, belgeler ve gerekçe içeriğine göre yapılan incelemede başkaca nedenler yerinde görülmemiştir. Ancak; 1- Sanık müdafininin 30.10.2002 tarihli oturum ve dilekçesindeki TCY'nin 59. maddesinin uygulanması isteği hakkında karar verilmemesi, 2- Okul dersliğinin herkese açık yerlerden olmadığı ve sövme suçunun aleniyet öğesinin oluşmadığı gözetilmeden, yetersiz gerekçeyle TCY'nin 482/2 maddesi yerine 482/3 maddesinin uygulanması,...” Yargıtay 4. CD., 24.11.2004, E. 2003/ 11951 – K. 2004 – 11346 (Kaynak: Kazancı İçtihat Programı – Offline)

5.3.- Aleniyet İle İhtilat Arasındaki Fark

İleride 5237 sayılı TCK md. 125 kapsamında hakaret suçunun internet açısından değerlendirilmesinde de ayrıntılarıyla ortaya konulacağı üzere ihtilat, hakaret içerikli bir ifadenin mağdurun gıyabında en az üç kişinin bilgisi dahilinde olacak şekilde ifşa edilmesidir. Dikkat edilecek olursa ihtilat aynı maddede ağırlaştırıcı neden olarak düzenlenmiş aleniyetten çok temel iki nokta bakımından ayrılmaktadır. Birincisi ihtilat gıyapta hakaret için bir zorunlu unsurdur ikincisi de mutlak suretle en az üç kişinin hakaret içerikli ifadeye muttali olması gerekir⁴²⁶. Ancak aynı suçun alenen işlenmesinde aleniyet bir zorunlu unsur değil nitelikli unsurdur. Ayrıca aleniyet için belli sayıda kişinin hakaret içerikli ifadeyi bilmesi aranmamakta, ifadenin bilinebilir olması yetmektedir. Yargıtay'ın uygulamaları da bu yöndedir⁴²⁷.

⁴²⁶ **TARHAN**, Emine Ülker, Yeni Türk Ceza Yasasında Tehdit ve Hakaret Suçları, Ankara, 2007, sh: 310.

⁴²⁷ "5816 Sayılı Kanununun 1 inci maddesinde Atatürk'ün hatırasına alenen hakaret eden veya söven kimse hakkında ceza tayin, ve tertip edilmiştir. İşbu hakaret ve sövme suçunun tekevvün ve tahakkuku için madde metninde açıkça yazılı olduğu üzere hakaret veya sövmenin alenen vukuu کافی olup ayrıca ihtilat unsurunun aranacağını istidlal ve istihraca medar kanuni bir kayıt ve sarahat yoktur. Esasen cezalı kanunlarda kanunun açık hükmü haricinde yorum yoluyla, bir suç unsuru ihdas ve ilavesine hukuken cevaz ve imkan bulunmamaktadır. Maddedeki hakaret ve sövme tabirleri, Atatürk'ün hatırasına karşı işlenen fiili tayin ve tebarüz ettirme maksadiyle konmuştur. Mücerret bu tabirler ele alınarak aleniyetten başka, aynı zamanda Türk Ceza Kanununun 480 ve 482 nci maddelerinde olduğu gibi ihtilaf unsurunun da bulunması iktiza eylediğini düşünmek, 5816 Sayılı Kanunun sarahatına ve maksadı tedvinine aykırı düşer. Nitekim Türk Ceza Kanununun Devletin şahsiyetine karşı cürümler babının ikinci faslında; Büyük Millet Meclisi, Hükümetin ve Adliyenin manevi şahsiyeti, Türkiye Cumhuriyeti kanunları gibi manevi yüksek varlıklara karşı işlenen fiillere taalluk eden 159 ve 160 nci maddeler yalnız aleniyet unsurunu ihtiva etmekte, şimdiye kadar cari tatbikatta bu kabil fiillerin tekevvünü için aleniyetten ayrı olarak ihtilat unsurunun mevcudiyeti aranmamaktadır. Aksinin düşünülmesi takdirinde, Türk Milletine malolan ve inkılaplarıyla sembolleşen Atatürk'ün hatırasına hakaret veya sövme Türk Ceza Kanununun 488 inci maddesi muvacehesinde lalettayin olmuş bir kimsenin hatırasından daha az teminatlı bir durum yaratacak ve 5816 Sayılı kanunun 1 inci maddesini işlemez bir hale koyacaktır. Netice: 5816 Sayılı Kanununun 1 inci maddesine temas eden Atatürk'ün hatırasına alenen hakaret veya sövme suçlarının tekevvününde aleniyetten başka ayrıca ihtilat unsurunun aranmasına lüzum bulunmadığına ilk toplantıda reylerin üçte ikisini geçen ekseriyetle 13.6. 1960 tarihinde karar verildi." Yargıtay İBKG, 13.06.1960, E. 1959/6 – K.1960/11;

"Dosyaya, oluşa ve mevcut delillere göre: Bursa Endüstri Meslek Lisesi mezunu, Edirne Vali Muavininin oğlu olup, halen İstanbul Yıldız Mimarlık ve Mühendislik Akademisinde memur statüsünde teknisyen olarak çalışan ve suç tarihinde 241. Piyade Alayında çavuş rütbesiyle askerlik görevini yapan sanıklardan Musa Ürcüment Kösem'in, İstanbul'da yıllık iznini kullanıp Lüleburgaz'daki kat'asına asker elbiseli dönerken, yanında bulunan arkadaşları er Nihat Şanlı ile sohbet ederken subayları kastederek "bunların hepsi kendini beğenmiş ot kafalı heriflerdir.. Bizim Binbaşı keleşin biridir.. Tümen komutanı Korgeneral olacağım diye götüne yurttu.. Hepsini kafaya aldım, hepsi bana gebe. Bunların menfaat karşılığı yapamayacakları şey yoktur" diye subayları kastederek "Eğitim yürüyüşü onlara zor geliyor. Ama Tümen Komutanı olmasa hiçbirşey yapamazlar, yine de bir kısmı eğitime falan çıkmıyor" ve yine bir rütbeliden bahsederken "Evde çocuklarına söz geçiremez, burada bizi kırar geçirir, kendisi evde çocuklara bakarken karısı onunla bununla dolaşır" şeklinde sözleri söylediği, önlerindeki sırada yalnız başına sivil kıyafette oturan, İstih ve İ.K.k.Ş.Md. Kurmay Kd. Yzb. Hikmet Ergin tarafından duyulmuş, sanıkların hüviyetlerini ve izin kağıtlarını alan Hikmet Ergin bağlı bulunduğu Komutanlığa ihbarda bulunmuştur. Ceza Genel Kurulunun 5.12.1966 gün, 276-456 ve 27.4.1981 gün, 91-159 sayılı kararlarında da açıklandığı gibi aleniyet suçun, herkesin görebileceği bir yerde işlenmesi anlamındadır. Aleniyet ile ihtilatı birbirine karıştırmamak lazımdır. İhtilat: TCK. 480 ve 482. maddelerinde hükme bağlanmış tahkir ve sövme suçlarının ikiden fazla kişiye duyulup bilgi edinilecek şekilde işlenmesidir. Şu hale göre ihtilatın niteliği, fiilin başkaları tarafından duyulup, bilgi edinilecek şartlar içinde işlenmesidir. Aleniyette ise esas olan

5.4.- Aleniyet Unsuru Bakımından İnternet Yayıncılığı

Tüm bu açıklamalar karşısında internet ortamında yapılan yayınların 5237 sayılı TCK çerçevesinde aleniyeti sağlayıp sağlamadığına bakılacak olursa, öncelikle internetin klasik basın yayın araçları ile aynı kapsamda düşünülmesi ve 29.05.2006 tarih ve 5377 sayılı yasa ile açıkça bir suçun basın yayın yoluyla işlenmesinin aleniyeti mümkün kılacağına kabulü karşısında internet ortamında gerçekleştirilen yayınların aleni olabileceği düşünülmelidir. Ancak bu düşünce internetteki her yayının aleniyeti gerçekleştirmeye elverişli olduğu sonucunu doğurmaz. Çünkü aleniyetin varlığı için mutlak suretle belirsiz sayıda kişi tarafından öğrenilebilecek, edinilebilecek yani vakıf olunabilecek olması gerekmektedir. Konu internet açısından irdelenecek olursa, bir içeriğin internet ortamına aktarılmasından sonra, içeriğe erişimde herhangi bir tahdit söz konusu değil ise, yani kamusal erişilebilirlik mümkün ise söz konusu içerik bakımından aleniyet mevcuttur. Doğal olarak da bu içerik aracılığıyla suç teşkil eden bir davranışta bulunulmuş ise, suç alenen işlenmiş bir suç olarak değer görecektir. Özellikle 5237 sayılı TCK md. 6'da suçun basın ve yayın yoluyla işlenmesi konusunda elektronik kitle iletişim araçlarının da sürece dahil edilmesi ve 5651 sayılı Kanun ile internet yayıncılığının çerçevesinin belirlenmesi ile birlikte, 2000'li yılların başında Yargıtay kararlarına da yansıyan ve internet ortamında gerçekleştirilen yayınların durumuna ilişkin tereddütlerin ortadan kalkmasına önemli ölçüde yardımcı olmuştur.⁴²⁸

şey suçun başkaları tarafından görülüp işitilebilecek surette işlenmesidir. İhtilat unsurunda hedef, saldırılan "kişilerce duyulması ve bilgi edinilmesi" olduğu halde aleniyette, umumi bir yerde işlenen fiilin başkaları tarafından görülüp işitilmesi şart olmayıp, görülüp işitilebilir olması yeterli sayılır. SONUÇ : Beyanlarının samimiyetinden kuşku duyulması için herhangi bir neden bulunmayan tanık Kurmay Yüzbaşı Hikmet Ergin'in (Sanığın otobüs içerisinde diğer yolcuların rahatlıkla duyabilecekleri bir ses tonu ile konuştuğunu) açıkça belirtmesi, sanığın sarfettiği tahkir ve tezyif edici sözlerin askeri kuvvetlerin tümüne raci olduğunun açıkça anlaşılması karşısında, C. Başsavcılığı itirazının reddine karar verilmelidir. Çoğunluk görüşüne katılmayan 8. Ceza Dairesi Başkanı Orhan Erdoğan: (Yolcu otobüsünde yanyana oturan iki kişi arasında geçen bir özel konuşmayı merak ile izleyip dinlemek suretiyle edinilen ve bir kişinin tekelinde kalmış bilgi, aleniyetin ve aleniyete çıkarma kastının varlığını göstermez. Olayda aleniyet çıkarma ögesi yoktur) diyerek; diğer üyeler ise: (itirazın haklı nedenlere dayandığını) ileri sürerek, C. Başsavcılığı itirazının kabulü gerektiği yolunda oy kullanmışlardır." Yargıtay CGK, 31.01.1983, E. 1983/482 – K. 1983/ 18 (Kaynak: Kazancı İçtihat Programı – Offline).

⁴²⁸ "Cumhuriyeti, askeri kuvvetleri, emniyet muhafaza kuvvetlerini, adliyenin manevi şahsiyetini tahkir ve tezyif etmek suçundan sanık Coşkun Ak'ın TCY.nin 159/1, 59, 159/1, 59, 159/1, 59, 159/1, 59, 71. maddeleri uyarınca 40 ay ağır hapis cezasıyla cezalandırılmasına ilişkin İstanbul 4. Ağır Ceza Mahkemesince 27.03.2001 gün ve 225-56 sayı ile verilen hükmün sanık vekili tarafından temyiz edilmesi üzerine, dosyayı inceleyen Yargıtay 9. Ceza Dairesince 25.10.2001 gün ve 1854-2649 sayı ile; "1- Gerçeğin kuşkuya yer vermeyecek şekilde belirlenmesi açısından öncelikle sanığın adı geçen şirkette konumunun ne olduğu, foruma internet ortamında elektronik posta ile gönderilen suçlamaya konu yazılara müdahale etme görev ve yetkisinin bulunup bulunmadığı, müdahale etme yetkisinin bulunmaması halinde bu yetkinin kime ait olduğu hususunun ilgili kurumdaki gerekli bilgi ve belgeler de sağlanarak saptanması; 2- Mahkemece üniversitelerin bilgisayar ve ceza hukuku kürsülerinden seçilecek internet konusunda uzman bilirkişi kurulu ile keşif yapılarak Superonline A.Ş.nin

Ancak özellikle klasik kitle haberleşme araçlarında rastlanmayan ve internetin yapısından kaynaklanan özellikler dolayısıyla aleniyetin gerçekleşip gerçekleşmediği hususunda bir takım soru işaretleri oluşabilir. Örneğin bir forum sayfasına veya bir gazetenin web sitesindeki yorum kısmına hakaret niteliğindeki bir içeriği yazmak isteyen bir kullanıcı, bunun ancak üyelikle mümkün olabileceğini görürse veya söz konusu içeriklerin ancak o web sitesine üye olan kişiler tarafından okunabileceği söz konusuysa, burada karşılaşılan durum kamusal erişilebilirlik bakımından bir tehdit olarak mı algılanmalıdır? Başka bir ifade ile, hakaret içeriğinin sadece o site üyeleri tarafından görülebilir olması aleniyeti engeller mi? *Kanaatimizce* bu konuyu geniş değerlendirmek isabetli olacaktır. Yukarıda aktarılan

bir internet servis sağlayıcı mı, erişim sağlayıcı mı yoksa her iki fonksiyona birlikte mi sahip olduğu, internet servis sağlayıcı olması durumunda sahibinin kim olduğu, ayrıca dava konusu yazının yayımlandığı forumun ve web sitesi sisteminin bir işletene (moderatör) bağlı olup olmadığı hususlarının saptanmasından sonra sanığın hukuki durumunun takdir ve tayini gerekirken eksik soruşturma ile hüküm kurulması" isabetsizliğinden, Daire Üyelerinden Ş. Erol'un, "Sanık Coşkun Ak hakkında merkezi İstanbul'da bulunan Yapı Kredi Bankasının bir yan kuruluşu olan Superonline Uluslararası Elektronik Bilgilendirme ve Haberleşme Anonim Şirketinin internet bölümler koordinatörü olduğu, bu sıfatı ile sisteme bağlı internet kullanıcılarından gelen yoğun istem üzerine internet ortamında; (Forum: Tartışma Platformu) başlıklı bir sayfa düzenleyerek internet kullanıcılarının hizmetine sunduğu, 26.5.1999 tarihinde başlayan yeni sayfa konusu (Türkiye'de insan hakları ihlalleri) olarak belirlenip bu sayfaya gelen mesajlar ile Cumhuriyeti tahkir ve tezyif etmek, askeri kuvvetleri tahkir ve tezyif etmek, emniyet kuvvetlerini tahkir ve tezyif etmek, adliyenin manevi şahsiyetini tahkir ve tezyif etmek suçlarının işlendiği iddiası ile TCK.nun 159/1. maddesinin dört kez uygulanması istemiyle kamu davası açılmıştır.

*Sanık Yapı Kredi Bankasının bir yan kuruluşu olan Superonline Uluslararası Elektronik Bilgilendirme ve Haberleşme Anonim Şirketi İnteraktif Bölümler Koordinatörü olduğunu kabul etmiştir. Mesajları okuduğunu suç unsuru görmediğini, bir vatandaş tarafından ihtarla rağmen sayfayı kapatmayarak dört gün daha bilgisi dahilinde açık tuttuğunu açıklamış bu sayfanın kapatılması için de hiçbir makam veya yetkiliye müracaat etmediği anlaşılmıştır. Yargıtay 4. Hukuk Dairesinin de belirlediği gibi internetteki yayınlar nedeni ile yapılacak işlem konusunda henüz yasal bir düzenleme bulunmamaktadır. **Bu durumda genel hukuk kurallarının uygulanması gerekmektedir. Sanık açmış olduğu sayfayı suç teşkil eden mesajları gördüğü halde iptal etmemek suretiyle yüklenen suçları işlemiştir. Ayrıca bahsi geçen sayfanın internet kullanıcılarına açık bırakılması ile de suçun aleniyet unsuru gerçekleşmiştir. Ortada başkaca araştırılması gereken bir husus bulunmadığından; toplanan delillere, mahkemenin gösterdiği gerekçeye mesajların içeriklerine, incelenen dosya kapsamına nazaran mahkemece verilen karar usul ve yasaya uygun olduğundan onanması görüşü ile sayın çoğunluğun kararına katılamıyorum" şeklinde kullandığı karşı oy ve oyçokluğu ile hükmün bozulmasına karar verilmiştir.** Yerel Mahkeme ise 12.03.2002 gün ve 18-72 sayılı ile; "Sanığın şirketteki konumunun kendisinin açık beyanlarından da anlaşılacağı üzere merkezi İstanbul'da bulunan Yapı Kredi Bankasının bir yan kuruluşu olan Super Online Uluslararası Elektronik Bilgilendirme ve Haberleşme A.Ş.nin internet bölümününün koordinatörü olduğu, internet kullanıcılarından gelen yoğun istek üzerine söz konusu sayfayı açtığı, sayfayı kapatmak ve açmanın kendi elinde olduğu, sayfaya gelen mesajları okuduğu, bir vatandaşın ihtarına rağmen suç unsuru görmediğinden sayfayı kapatmadığı gibi, kapatılması yönünde hiçbir makam ve yetkiliye başvurmadığı, yüklenen suçlu işlediği, olayda bilirkişinin bilgisine başvurulmasını gerektiren bir durumun söz konusu olmadığı, bu nedenle bozma ilamında belirtilen hususların araştırılmasına yer olmadığı" gerekçesiyle önceki hükmünde direnmiş, ancak bu kez TCY.nun 159. maddesi 4744 sayılı Yasa ile değiştirilmiş olması nedeniyle sanık lehine olan bu değişikliği uygulamak suretiyle sanığın TCY.nun 159/1, 59, 159/1, 59, 159/1, 59 ve 647 sayılı Yasanın 4. maddeleri uyarınca sonuç olarak 6.000.000 lira ağır para cezasıyla cezalandırılmasına karar vermiştir. Yargıtay CGK, 15.10.2002, E: 2002/9-172 – K: 2002/360 (Kaynak: Kazancı İçtihat Programı – Online, Erişim Tarihi: 22.03.2009, Saat: 09:00).*

örneklerde suç teşkil eden bir içeriğin ilgili web sayfasına yüklenmesinde veya yüklenen içeriklerin görülmesinde üyelik şartının aranması aleniyet açısından *prima facie* bir engel olarak görülebilir. Ancak burada ikili bir ayrım çerçevesinde tartışmak gerekir. Bu ayrımı ortaya koyması anlamında *Niggli*'nin internet aracılığıyla gerçekleştirilen ırk ayrımcılığı ve yabancı düşmanlığı eylemlerini incelerken yapmış olduğu değerlendirmeyi anlamlı buluyoruz. Yazara göre, sohbet odalarında, haber ve tartışma forumlarında açıklanan her şeyin kural olarak aleni değerlendirileceği, şifre üzerinden erişimin ön görülmüş olması durumunda ise, bu şifrenin her isteyene ya da belli koşullar taşıyan kişilere verilip verilmediğine bakılmalıdır. Şayet bu şifre ve benzeri erişimi koşullandıran unsurlar o an isteyen herkes tarafından edinilebiliyorsa, bu durumlarda aleniyetin engellenmediği kabul edilmelidir. Şayet söz konusu içeriğe erişimi mümkün kılacak unsurlar o an için her isteyen tarafından edinilemiyorsa, sadece daha önceden edinilebilen unsurlarla bilgiye erişim sağlanabiliyorsa burada aleniyetin engellendiği kabul edilebilir⁴²⁹.

Örneğin bir forum sitesindeki yorumları görebilmek o an, forum yöneticisi tarafından belirlenen bilgi formunun doldurulması ve bunun sonunda kullanıcıya verilecek kullanıcı adı ve şifre aracılığıyla mümkünse, bu işlem aleniyeti engellemez. Bu tür üyelik işlemleri, son yıllarda internet ortamında işlenen suçları önlemek ve interneti daha güvenli kılmak için kullanıcıların kayıt altına almaktan ibaret işlemlerdir. Ancak internet üzerinden yayınlanan ve daha önceden gerçekleştirilecek bir takım işlemler ile kullanıcıya verilen kullanıcı adı veya şifresi aracılığıyla erişimi mümkün olan içerikler bakımından, o an erişimi sağlayacak unsurları temin edememe durumu söz konusu ise, artık burada bir kamusal erişilebilirlikten bahsetmek mümkün değil. Haliyle bu şartlarda gerçekleştirilen internet yayınları aleniyet içerisinde değerlendirilemez. Bu noktada akıllara bir soru daha gelmektedir. Şayet internette kullanılan arama motorlarıyla yapılan bir tarama esnasında hakaretamiz bir ifadenin geçtiği bir verinin varlığı tespit edilse ve fakat o veriye ulaşılacak istendiğinde o an aşılamayacak bir erişim engeliyle karşılaşılsa (örneğin yukarıda verilen örnek bağlamında abonelik temeline dayanan bir üyelik gibi) burada aleniyetten bahsetmek mümkün olabilecek midir? Kanaatimizce burada ikili bir değerlendirme yapmak isabetli olacaktır. Öncelikle, örnek üzerinden gitmek gerekirse, ilgili arama motorunun tespit ettiği hakaretamiz içerikli verinin bir bütünlük içerisinde belli bir kişiye karşı yöneltildiği, kısmi olarak yansıtılan haliyle dahi anlaşılıyorsa, burada hakaret suçunun alenen işlendiğinin kabul edilmesi gerekecektir. Ancak böyle bir belirlenim gerçekleştirilemiyorsa burada artık bir o verinin bütününe

⁴²⁹ Bkz. **NIGGLI**, Irk Ayrımcılığı ve Internet, sh: 277.

değerlendirilmesi önem arz edecektir. Bütününe erişimin sınırlandırılması hali de söz konusu veri için aleniyetin de engellendiği sonucunu beraberinde getirecektir.

Son olarak da internet yayıncılığı bakımından aleniyet ve ihtilat arasındaki ilişkiye bir örnek özerinde değinmek yerinde olacaktır. Yukarıdaki örnek ile aynı çerçeveden hareket etmek adına internet ortamında işlenen hakaret suçu üzerinden hareket edilecek olursa, bir forum veya paylaşım sitesinde yayınlanmak üzere hakaret içerikli bir iletinin gönderilmesi ve fakat bu iletinin ilgili sitenin moderatörleri tarafından, aynı zamanda içerik sağlayıcının cezai sorumluluğunu gerektirecek bir içeriğe sahip olması nedeniyle, engellenmesi ve o fümurda veya paylaşım sitesinde yayınlanmaması durumunda nasıl bir değerlendirme yapmak gerekecektir? Kanaatimizce böyle bir durum, ileride ayrıntısıyla değinileceği üzere, neticesi harekete bitişik bir suç olan hakaret suçunun klasik görünümünün internet teknolojisi bağlamında farklılaştığı görüntüsünü ortaya koymaktadır. Çünkü kural olarak neticesi harekete bitişik suçlarda teşebbüs söz konusu değildir. Ancak olayda hakaretimiz ifadeyi gönderen kişinin eylemi, kendi hakimiyet alanı ve inisiyatifinin dışında neticeye ulaşmadan yarıda kesildiği için burada teşebbüs aşamasında kalmış bir hakaret suçundan bahsedilebilir. Ancak bu iletiyi ilgili internet ortamında yayınlamayan moderatörlerin sayısı bir değil de üç ve daha fazlaysa, *kanaatimizce* artık burada ihtilat düzeyinde gerçekleşmiş bir hakaret suçundan bahsedilebilir.

6.- SUÇA İŞTİRAK HÜKÜMLERİ BAĞLAMINDA İNTERNET SÜJELERİNİN KONUMLARI VE CEZAI SORUMLULUKLARI

6.1.- Genel Açıklamalar

İnternet aracılığıyla işlenebilen suçların her geçen gün artış göstermesi ve çeşitlilik kazanmasıyla, bu suçlarla mücadele konusunda salt TCK hükümlerinin yeterli olmadığı yönündeki haklı yaklaşım tarzı özellikle internet hizmetinin sağlanması sürecinde bir takım fonksiyonları bünyelerinde barındıran süjelerin ceza hukuku sorumluluklarının açık bir şekilde ortaya konulmasını elzem kabul etmiştir⁴³⁰. Keza Avrupa ülkelerinde ve Amerika'da yıllar öncesinden başlayan bir süreçte, özellikle internet aracılığıyla işlenen içerik suçları

⁴³⁰ Bkz. 1.8.- Değerlendirme: Modern Ceza Hukuku Teorisinde İnternet Suçluluğunun Yeri ve Türk Hukukundaki Yansımaları .

bakımından internet sjeleri olarak kabul edilen ierik saęlayıcı, erişim saęlayıcı, yer saęlayıcı ve toplu kullanım saęlayıcıların ykmllk ve sorumluluklarının hem Ceza Kanunlarında hem de zel kanunlarla belirlendięi ve bu suretle gvenli internet kullanımı konusunda saęlam adımlar atıldıęı grlmektedir⁴³¹.

lkemizde de, ge bile kalınmıř olsa, internet sjelerinin sorumlulukları 5651 sayılı Kanunla belirlenmiřtir. Bu kanunla kabul edilen ve ařaęıda nakledilecek olan kriterler erevesinde internet ortamında iřlenen sularla mcadele imkanları olduka artmıř ve en nemlisi de ceza sorumluluęunun ykleneceęi sjenin tespiti kolaylařmıřtır⁴³². Keza 5651 sayılı Kanunun 1. maddesinde kanunun amacı, “*ierik saęlayıcı, yer saęlayıcı, erişim saęlayıcı ve toplu kullanım saęlayıcıların ykmllk ve sorumlulukları ile internet ortamında iřlenen belirli sularla ierik, yer ve erişim saęlayıcıları zerinden mcadeleye iliřkin esas ve uslleri dzenlemektir*” řeklinde ifade edilerek internet sjeleri odaklı bir mcadele planı hazırlandıęı grlmektedir. Ancak dikkat edilecek olursa ilgili madde internet ortamında iřlenebilen tm sularla mcadeleyi bu kanun kapsamında ele almamıřtır. Yasa koyucunun “*İnternet ortamında iřlenen belli sular*” demek suretiyle bir tercih yaptıęı anlařılmaktadır. Hem ilgili kanunun adı hem de 1. maddenin yaptıęı atfa karřılık geldięi anlařılan 8. maddedeki katalog⁴³³ řunu aık bir řekilde ortaya koymaktadır ki, 5651 sayılı kanun internet

⁴³¹ İnternet ortamında iřlenen sulardan doęan ceza sorumluluęuna iliřkin olarak Almanya’daki dzenlemelerle ilgili bkz. **ERMAN**, Barıř, Almanya Hukukunda İnternette Kaynaklanan Ceza Sorumluluęu, in: İHFMM, C: 59, S: 1-2, İstanbul, 2001, sh: 203 v.d.; Fransa’daki dzenlemeler ile ilgili bkz. **KANGAL**, Zeynel, Fransa’da İnternet Yoluyla İlenen Sulardan Doęan Ceza Sorumluluęu, in: İHFMM, C:59, S: 1-2, sh: 227 v.d.. Ayrıca bkz. **MAHMUTOęLU**, Fatih S., Karřılařtırılmal Hukuk Bakımından İnternet Sjelerinin Ceza Sorumluluęu, in: İHFMM, C: 59, S: 1-2, sh: 39 v.d.

⁴³² **KETİZMEN**, Biliřim Suları, sh: 23 v.d.

⁴³³ **MADDE 8-** (1) İnternet ortamında yapılan ve ierięi ařaęıdaki suları oluřturduęu hususunda yeterli řphe sebebi bulunan yayınlarla ilgili olarak erişimin engellenmesine karar verilir:

a) 26/9/2004 tarihli ve 5237 sayılı Trk Ceza Kanununda yer alan;

- 1) İntihara ynlendirme (madde 84),
- 2) ocukların cinsel istismarı (madde 103, birinci fıkra),
- 3) Uyuřturucu veya uyarıcı madde kullanılmasını kolaylařtırma (madde 190),
- 4) Saęlık iin tehlikeli madde temini (madde 194),
- 5) Mstehcenlik (madde 226),
- 6) Fuhuř (madde 227),
- 7) Kumar oynanması iin yer ve imkn saęlama (madde 228),

suları.

b) 25/7/1951 tarihli ve 5816 sayılı Atatrk Aleyhine İřlenen Sular Hakkında Kanunda yer alan sular.

(2) Eriřimin engellenmesi kararı, soruřturma evresinde hkim, kovuřturma evresinde ise mahkeme tarafından verilir. Soruřturma evresinde, gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısı tarafından da erişimin engellenmesine karar verilebilir. Bu durumda Cumhuriyet savcısı kararını yirmidrt saat iinde hkimin onayına sunar ve hkim, kararını en ge yirmidrt saat iinde verir. Bu sre iinde kararın onaylanmaması halinde tedbir,

ortamında işlenen içerik suçlarına yönelmiştir. Dolayısıyla tarafımızca önerilen diğer sınıflandırma olan müdahale suçları bu kanun kapsamında ele alınmamıştır.

5651 sayılı Kanunun ikinci maddesinde internet sùjelerinin tanımları yapılmıştır. Buna göre; kullanıcılarına internet ortamına erişim olanağı sağlayan her türlü gerçek veya tüzel kişiler *erişim sağlayıcı*, internet ortamı üzerinden kullanıcılara sunulan her türlü bilgi veya veriyi üreten, deęiştiren ve sağlayan gerçek veya tüzel kişiler *içerik sağlayıcı*, hizmet ve içerikleri barındıran sistemleri sağlayan veya işleten gerçek veya tüzel kişiler *yer sağlayıcı* ve nihayet kişilere belli bir yerde ve belli bir süre internet ortamı kullanım olanağı sağlayan ise *topluluk kullanımı sağlayıcı olarak* tanımlanmıştır. Şimdi sırayla, Kanunun deęimiyle, bu internet sùjelerinin yükümlülük ve sorumlulukları konusunda 5651 sayılı Kanunun ön gördüğü çerçeve ele alınacaktır.

6.2.- İçerik Sağlayıcının Sorumlulukları

Cumhuriyet savcısı tarafından derhal kaldırılır. Koruma tedbiri olarak verilen erişimin engellenmesine ilişkin karara 4/12/2004 tarihli ve 5271 sayılı Ceza Muhakemesi Kanunu hükümlerine göre itiraz edilebilir.

(3) Hâkim, mahkeme veya Cumhuriyet savcısı tarafından verilen erişimin engellenmesi kararının birer örneęi, gereęi yapılmak üzere Başkanlığa gönderilir.

(4) İçerięi birinci fıkrada belirtilen suçları oluşturan yayımların içerik veya yer sağlayıcısının yurt dışında bulunması halinde veya içerik veya yer sağlayıcısı yurt içinde bulunsan bile, içerięi birinci fıkranın (a) bendinin (2) ve (5) numaralı alt bentlerinde yazılı suçları oluşturan yayımlara ilişkin olarak erişimin engellenmesi kararı re'sen Başkanlık tarafından verilir. Bu karar, erişim sağlayıcısına bildirilerek gereęinin yerine getirilmesi istenir.

(5) Erişimin engellenmesi kararının gereęi, derhal ve en geç kararın bildirilmesi anından itibaren yirmidört saat içinde yerine getirilir.

(6) Başkanlık tarafından verilen erişimin engellenmesi kararının konusunu oluşturan yayını yapanların kimliklerinin belirlenmesi halinde, Başkanlık tarafından, Cumhuriyet başsavcılığına suç duyurusunda bulunulur.

(7) Soruşturma sonucunda kovuşturmaya yer olmadığı kararı verilmesi halinde, erişimin engellenmesi kararı kendiliğinden hükümsüz kalır. Bu durumda Cumhuriyet savcısı, kovuşturmaya yer olmadığı kararının bir örneęini Başkanlığa gönderir.

(8) Kovuşturma evresinde beraat kararı verilmesi halinde, erişimin engellenmesi kararı kendiliğinden hükümsüz kalır. Bu durumda mahkemece beraat kararının bir örneęi Başkanlığa gönderilir.

(9) Konusu birinci fıkrada sayılan suçları oluşturan içerięin yayından çıkarılması halinde; erişimin engellenmesi kararı, soruşturma evresinde Cumhuriyet savcısı, kovuşturma evresinde mahkeme tarafından kaldırılır.

(10) Koruma tedbiri olarak verilen erişimin engellenmesi kararının gereęini yerine getirmeyen yer veya erişim sağlayıcılarının sorumluları, fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde, altı aydan iki yıla kadar hapis cezası ile cezalandırılır.

(11) İdarî tedbir olarak verilen erişimin engellenmesi kararının yerine getirilmemesi halinde, Başkanlık tarafından erişim sağlayıcısına, onbin Yeni Türk Lirasından yüzbin Yeni Türk Lirasına kadar idarî para cezası verilir. İdarî para cezasının verildięi andan itibaren yirmidört saat içinde kararın yerine getirilmemesi halinde ise Başkanlığın talebi üzerine Kurum tarafından yetkilendirmenin iptaline karar verilebilir.

(12) Bu Kanunda tanımlanan kabahatler dolayısıyla Başkanlık veya Kurum tarafından verilen idarî para cezalarına ilişkin kararlara karşı, 6/1/1982 tarihli ve 2577 sayılı İdarî Yargılama Usulü Kanunu hükümlerine göre kanun yoluna başvurulabilir.

5651 sayılı Kanunu 4. maddesinde içerik sağlayıcının sorumluluğu düzenlenmiştir. Buna göre içerik sağlayıcının internet ortamında sunduğu her türlü içerikten sorumlu bulunmaktadır⁴³⁴. Bu kanun anlamında internet ortamı kavramından haberleşme ile kişisel veya kurumsal bilgisayar sistemleri dışında kalan ve kamuya açık olan internet üzerinde oluşturulan ortam anlaşılmaktadır. Dolayısıyla her ne kadar internet aracılığıyla kurulmuş olsun, haberleşme amaçlı kullanılan programlar aracılığıyla yapılan içerik yayımı bu kanun anlamında internet ortamında kabul edilmemektedir. Yine aynı şekilde bireysel veya kurumsal sistemleri de internet ortamı dışında tutulmuştur. Buradan hareketle bir içerik sağlayıcısının oluşturduğu ve yayınladığı içerikten sorumlu tutulabilmesi için bu içeriğin yukarıda sayılanların dışında ve kamuya açık olan web sitelerinde yayınlanması veya yayılması gerekmektedir. Bu tespitten hareketle kanun koyucunun belirlediği internet ortamı tanımının eksik olduğu ve hatalı uygulamalara neden olabileceği vurgulanmalıdır. Yukarıda da ifade ettiğimiz gibi kamuya açıklık aleniyet unsuru bakımından önem arz edecek bir husustur⁴³⁵. Kamuya açık olmadan belli sayıda bir kitleye ve ya doğrudan özel bir kişiye internet aracılığıyla gönderilen bir içeriğin suç teşkil etmesi durumunda, kanunun internet ortamı tercihinden dolayı içerik sağlayıcısının sorumluluğuna gidilemeye tehlikesi ortaya çıkabilir. Bunun dışında içerik sağlayıcının internet ortamına sunduğu veri bakımından da herhangi bir sınırlamaya gidilmemiştir. Herhangi bir web sitesinde yer alan herhangi veriyi oluşturan ve o veri üzerinde tasarrufta bulunan kişi bundan dolayı sorumludur⁴³⁶. İçerik olarak bu verinin bir makale, bir haber yorumu, bir resim veya bir ses olmasının hiçbir önemi ve farkı yoktur.

Kanunun 4. maddesiyle internet ortamına aktarılan her türlü içerikten sorumlu tutulan içerik sağlayıcı başka bir içeriğe ilişkin olarak sağladığı bağlantı nedeniyle kural olarak sorumlu tutulamaz. Şöyle ki, bir içerik sağlayıcı, başka bir içerik sağlayıcıya ait ve internet ortamında yer alan herhangi bir içeriğe ilişkin bağlantı sağlarsa yani teknik anlamıyla link verdiği taktirde salt bu eyleminden dolayı, link verdiği içeriğin sebep olduğu suçtan dolayı sorumlu tutulmamaktadır⁴³⁷. Ancak ifade edildiği üzere bu bir kuraldır ve bu kuralın istisnası da link verilen içeriğin sahiplenilmesidir. Başka bir anlatımla, bir içerik sağlayıcının başka bir

⁴³⁴ TAŞKIN, Şaban Cankat, Bilişim Suçları, Bursa, 2008, sh: 149.

⁴³⁵ Bkz. 6.3.- Aleniyet Unsuru Bakımından İnternet Yayıncılığı.

⁴³⁶ DÜLGER, İnternete Erişimin Engellenmesi, sh: 1485.

⁴³⁷ TAŞKIN, Bilişim Suçları, sh: 150.

içerik sağlayıcıya ait olan içerikten sorumlu olabilmesi için link verdiği içeriği benimsediği ve bu doğrultuda kullanıcıyı özellikle o içerikle buluşturma gayesinin açıkça anlaşılması gerekmektedir. Örneğin bir içerik sağlayıcı, haber verme sınırları içerisinde kalarak yasa dışı bir faaliyete ilişkin verileri barındıran başka bir web sitesine link sağladığı durumda, sadece bu bağlantı dolayısıyla bağlantı kurulan linkin içeriğini sahiplendiği anlamı çıkmaz. Bu yönlendirmenin yapılaş tarzı itibariyle hedef tutulan içeriğin yönlendirici içerik sağlayıcısı tarafından da kabul edildiğinin açık olarak anlaşılması gerekmektedir⁴³⁸.

Böyle bir netlik söz konusuysa içerik sağlayıcı genel hükümlere göre sorumlu olacaktır. Ancak bu düzenleme doktrinde genel hükümlerle ifade edilmek istenilenin bu yasanın genel hükümleri mi, ceza kanununun genel hükümleri mi yoksa borçlar kanununun genel hükümleri mi kastedildiğinin anlaşılmadığı ve bir içerik sağlayıcısı tarafından kendi web sitesinde açık bir biçimde bir diğer sitenin içeriğinde yer alan belli bir içeriği benimsemediği söylenmedikçe benimseme ve ulaşmayı amaçlamanın hangi ölçütlere göre belirleneceğinin ve nasıl ispat edileceğinin şüpheli olduğu gerekçesiyle önemli eleştirilere maruz kalmıştır⁴³⁹.

6.3.- Yer Sağlayıcının Sorumlulukları

5651 sayılı Kanunun 5. maddesinde yer sağlayıcının sorumluluğu düzenlenmiştir. Buna göre görevi yalnızca bir internet sayfasına “barındırmak” olan yer sağlayıcısının yer sağladığı internet sayfalarının içeriğini denetlemek ya da hukuka aykırı bir etkinlikte bulunup bulunmadığını belirlemek gibi bir yükümlülüğü yoktur⁴⁴⁰. Bu düzenlemeyi isabetli bulan *Dülger’e* göre, aksine bir düzenleme ile yer sağlayıcıları hizmet verdiği milyonlarca verinin içeriği hakkında bilgi edinmek ve bundan sorumlu tutmanın hem fiziken imkansız hem de adaletsiz olacaktır⁴⁴¹.

⁴³⁸ **KETİZMEN**, Bilişim Suçları, sh: 29.

⁴³⁹ **DÜLGER**, İnternete Erişimin Engellenmesi, sh: 1486.

⁴⁴⁰ **TAŞKIN**, Bilişim Suçları, sh: 150.

⁴⁴¹ **DÜLGER**, İnternete Erişimin Engellenmesi, sh: 1486.

Yer sağlayıcının içerikten sorumlu olabilmesi için 5651 sayılı kanunun 8. ve 9⁴⁴². maddesi gereğince içerikten haberdar edilmesi ve ayrıca teknik olarak da içeriği kaldıracabilecek durumda olmasına rağmen kaldırmaması gerekmektedir. Burada önemli olan bir ayrıntı yer sağlayıcıların 5651 sayılı Kanunun 8.ve 9. maddeleri uyarınca, suç teşkil eden içeriğe ilişkin uyarılmaları yetmemekte, bu uyarının gereğini yapabilecek teknik kapasiteye sahip olmaları gerekir. Bu kapasite standartları bakımından optimum bir seviyenin belirlenmesi amacıyla yer sağlayıcıları bu kanunla birlikte 24.10.2007 tarih ve 26680 sayılı Resmi Gazetede yayımlanan Telekomünikasyon Kurumu Tarafından Erişim Sağlayıcı Ve Yer Sağlayıcılara Faaliyet Belgesi Verilmesine İlişkin Usul Ve Esaslar Hakkında Yönetmeliğe göre bir faaliyet belgesi almak durumundadırlar⁴⁴³. Bu faaliyet belgesinin almaması durumunda yer sağlayıcının faaliyetleri Telekomünikasyon Kurumu tarafından durdurulmaktadır.

6.4.- Erişim Sağlayıcının Sorumlulukları

Erişim sağlayıcının yükümlülükleri ise kanunun 6. maddesinde oldukça geniş bir biçimde düzenlenmiştir. Bu düzenleme dikkatle incelendiği takdirde erişim sağlayıcının iki esas görevinin olduğu görülmektedir. Bunlardan birincisi herhangi bir içerik sağlayıcının yayınladığı hukuka aykırı içerikten 5651 sayılı Kanunun 8. ve 9. maddelerine göre haberdar

⁴⁴² **MADDE 9-** (1) İçerik nedeniyle hakları ihlâl edildiğini iddia eden kişi, içerik sağlayıcısına, buna ulaşamaması halinde yer sağlayıcısına başvurarak kendisine ilişkin içeriğin yayından çıkarılmasını ve yayındaki kapsamından fazla olmamak üzere hazırladığı cevabı bir hafta süreyle internet ortamında yayımlanmasını isteyebilir. İçerik veya yer sağlayıcı kendisine ulaştığı tarihten itibaren iki gün içinde, talebi yerine getirir. Bu süre zarfında talep yerine getirilmediği takdirde reddedilmiş sayılır.

(2) 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. Sulh ceza hâkimi bu talebi üç gün içinde duruşma yapmaksızın karara bağlar. Sulh ceza hâkiminin kararına karşı Ceza Muhakemesi Kanunu hükümlerine göre itiraz yoluna gidilebilir.

(3) Sulh ceza hâkiminin kesinleşen kararının, birinci fıkraya göre yapılan başvuruyu yerine getirmeyen içerik veya yer sağlayıcısına tebliğinden itibaren iki gün içinde içerik yayından çıkarılarak hazırlanan cevabın yayımlanmasına başlanır.

(4) Sulh ceza hâkiminin kararını bu maddede belirtilen şartlara uygun olarak ve süresinde yerine getirmeyen sorumlu kişi, altı aydan iki yıla kadar hapis cezası ile cezalandırılır. İçerik veya yer sağlayıcının tüzel kişi olması halinde, bu fıkra hükmü yayın sorumlusu hakkında uygulanır.

⁴⁴³ Yönetmeliğe erişmek için http bkz. <http://www.mevzuat.adalet.gov.tr/html/27643.html> (Erişim Tarihi: 10. 01. 2009, Saat: 23:00)

edilmesi durumunda ve teknik olarak erişimi engelleme olanağı bulunduğu takdirde erişimi, söz konusu hukuka aykırı içeriğe erişimi engellemektir⁴⁴⁴.

Erişim sağlayıcının ikinci temel yükümlülüğü ise daha çok güvenlikle ve bilişim suçlarının soruşturulmasını kolaylaştırmak ile ilgilidir. Buna göre erişim sağlayıcı 5651 sayılı Kanunun uygulanmasına ilişkin yönetmelikte açıklanan internet trafiğine ilişkin bilgileri en az altı ay en çok iki yıl olmak üzere saklamakla ve bu bilgilerin doğruluğunu, gizliliğini ve bütünlüğünü korumakla yükümlüdür⁴⁴⁵. Doktrinde bu yükümlülüğün kişisel verilerin korunması bakımından, internet hareketliliğine ilişkin verilerin bu kadar uzun süre tutulması, bu süreler sonrasında söz konusu verilerin güvenli bir şekilde imha edilmesinin kontrolünde yaşanacak güçlükler ve bu verilerin süresi içerisinde kötüye kullanılması ihtimalinin ağırlığı dolayısıyla sakıncalı olduğu ifade edilirken, aynı zamanda erişim sağlayıcıya ek maliyet getirmesi düzenlemenin olumsuz yönüyle suçlarla mücadelede önemli bir işlem göreceği olması ise olumlu karşılanmaktadır⁴⁴⁶.

6.5.- Toplu Kullanım Sağlayıcının Sorumlulukları

Özellikle son yıllarda artış gösteren internet kafelerin suç işlemek için kullanılmaya başlanması nedeniyle 5651 sayılı Kanunda bu işletmeler toplu kullanım sağlayıcı başlığı altında ele alınmış ve bunlara ilişkin sorumluluk düzenlemeleri 7. maddede yapılmıştır. Buna göre ticari amaçlı toplu kullanım sağlayıcıların etkinlikte bulunabilmesi için mahalli mülki amirden izin almaları gerekmektedir⁴⁴⁷. Bu yükümlülüğe uymayan toplu kullanım sağlayıcıya mülki amirlik tarafından 3000. TL'den 15.000. TL'ye kadar idari para cezası öngörülmüştür.

Tüm toplu kullanım sağlayıcıların ticari amaçlı olsun veya olmasın suç içerikli web sitelerine veya uygulamalara genel nitelikli erişimin engellenmesi konusunda sorumlulukları vardır. Bu amaçla da sağlayıcılarının bilişim sistemlerine gerekli yazılımları ve güvenlik duvarlarını yüklemelerin gerekmektedir.

⁴⁴⁴ ERGÜN, İsmail, Siber Suçların Cezalandırılması ve Türkiye'de Durum, Ankara, 2008, sh: 54.

⁴⁴⁵ TAŞKIN, Bilişim Suçları, sh: 151.

⁴⁴⁶ "Buna benzer bir düzenleme İngiltere'de rastlanmaktadır. Buna göre güvenlik gerekçesiyle İnternet Servis Sağlayıcılar İngiltere'de kullanıcı detaylarını ve telefon verisini 12 ay; e- mail verilerini 6 ay ve web etkinliklerini 4 gün boyunca saklama ve istenildiğinde soruşturma makamlarıyla paylaşmak zorundadır." . TAŞKIN, Bilişim Suçları, sh: 152'den naklen.

⁴⁴⁷ Konu ile ilgili detaylı düzenlemelerin yapıldığı 01.11.2007 tarihli İnternet Toplu Kullanım Sağlayıcı Hakkında Yönetmelik'e erişmek için bkz. <http://www.mevzuat.adalet.gov.tr/html/27649.html> (Erişim Tarihi: 10.01.2009, Saat: 23:00)

6.6.- İnternet Süjelerinin Ceza Sorumlulukları Bakımından Bir Uygulama Örneği Olarak Compu-Serve Davası

Davaya konu olan olayda sanık, “CompuServe-Amerika” şirketinin bir bağlı şirketi olan “CompuServe – Almanya”nın sorumlusudur. Bu bağlı şirket, CompuServe – A.B.D. şirketinden faaliyeti için maddi bir ödenek almaktadır. Bu ödenek suç tarihi itibariyle CompuServe – A.B.D.nin, bağlı şirketi olan CompuServe – Almanya şirketinin sorumlu olduğu alandan elde ettiği gelirlerin %31’ini oluşturmaktaydı⁴⁴⁸.

CompuServe- Almanya şirketi sunduğu hizmetten dolayı, CompuServe- A.B.D. firmasının Almanya’daki kullanıcılarına, hakim şirketin (CompuServe- A.B.D.) News-Server’inde kayıtlı bulunan şiddet içerikli ve çocuk ve hayvan pornografisi ile ilgili görüntülere ulaşabilmelerine imkan sağlamıştır. Hakim şirket olan CompuServe- A.B.D. ise kullanıcılarına hem yabancı hizmetleri hem de kendi hizmetlerini sunmaktaydı.

Almanya’daki kullanıcılarla girişilen hizmet sözleşmesi bakımından sözleşmenin tarafı sadece CompuServe- A.B.D. şirketi olmuştur. CompuServe – Almanya ile Almanya’daki Compu Serve - A.B.D.’nin müşterileri arasında hiçbir sözleşmesel ilişki bulunmamaktadır. CompuServe – Almanya’nın görevi, CompuServe – A.B.D.’nin Almanya’daki müşterileri için bir erişim noktası (bağlantı noktası) oluşturmaktır. Kullanıcı Almanya’da kendine en yakın erişim noktasından bağlantı sağlayabilmekteydi. Daha sonra bu noktadan, bağlı şirket ve hakim şirket arasındaki sabit hat vasıtasıyla herhangi bir geçerlilik kontrolüne tabi olmaksızın hakim şirketin Amerika’daki hesap merkezine bağlanmaktaydı. CompuServe- A.B.D., üyelik denetiminin sonrasında kendi veri merkezinden en yakın internet bağlantı noktası üzerinden Almanya’daki müşterilerinin internete girişini sağlamaktaydı⁴⁴⁹.

1995 yılının Kasım ayında Münih Soruşturma Makamı sanığa, CompuServe- A.B.D. Server’inde çocuk pornografisi içerikli haiz beş haber grubu tespit edildiğini bildirmiştir. Aralık 1995’de yine sanığa, internette pornografik ve gençler açısından tehlikeli içerikleri gösterilen 282 haber grubunu bir liste halinde sunmuştur. Sanık bu listeyi, listede

⁴⁴⁸ HONG, CompuServe Davası, sh: 323.

⁴⁴⁹ HONG, CompuServe Davası, sh: 324.

belirtilen içeriklerin silinmesi veya engellenmesi talebiyle birlikte hakim şirket olan CompuServe- A.B.D.'ye göndermiştir. CompuServe- A.B.D.de bunun üzerine 22 aralık 1995 – 13 Şubat 1996 tarihleri arasında bu haber gruplarının çok büyük bir bölümünü engellemiştir.

CompuServe- A.B.D., ebeveynlerin bu tarz gençlere zarar verici (tehlikeli) içerikleri engelleme imkanı veren “Çocuk Koruma – Software” ini piyasaya sürmesinden sonra , bu engellenen haber grupları Şubat ayının ortasından itibaren yeniden serbest bırakmıştır⁴⁵⁰.

Davaya bakan yerel mahkeme olan Münih Sulh Ceza Mahkemesi bu olayla ilgili CompuServe-Almanya sorumlusu sanık hakkında mahkûmiyete karar vermiştir. Mahkemeye göre Tele Hizmetler Kanunu (THK) uyarınca bir erişim sağlayıcı doğrudan internete giriş hizmeti sunmalıdır ve kendine özgü müşterileri olmalıdır. Eğer on-line servis sağlayıcısının kullanıcısı ile sabit hat üzerinden online servis sağlayıcısı arasındaki bağlantıyı sağlayan bir erişim noktasını sağlıyorsa; bu hizmet sunucusu erişim sağlayıcısı olarak kabul edilmemektedir. Bu bağlamda Mahkeme, Alman CompuServe Şirketinin sorumlusunu THK md. 5/3 de yer alan sorumsuzluk esasına göre değil, 5/2 inci maddede düzenlenen sorumluluk üzerinden mahkûmiyet kararı vermiştir. THK md. 5/2 de düzenlenen sorumluluk esasına dayanabilmek için, özellikle THK md. 5/2’de kullanılan “Haberdar Olmak” ve “Beklenebilir Olmak” kavramlarının yorumlanması ve THK md. 5/3’ün reddedilmesi gerekmektedir.⁴⁵¹

⁴⁵⁰ HONG, Compuserve Davası, sh: 326.

⁴⁵¹ THK. §5 – Sorumluluk

- 1- Servis sağlayıcılar, kullanıma hazır tuttıkları kendi içeriklerinden genel kurallara göre sorumludurlar.
- 2- Servis sağlayıcılar, kullanıma hazır tuttıkları yabancı içeriklerden, sadece bunların içeriklerini bildikleri ve bunların engellenmesinin, teknik olarak mümkün ve kendilerinden beklenebilir olduğu durumda sorumludurlar.
- 3- Servis sağlayıcılar, salt erişim sağladıkları yabancı içeriklerden sorumlu değildirler. Yabancı içeriklerin, kullanıcı sorgusu nedeniyle otomatik ve kısa süreli olarak bulundurulması erişim sağlamasına geçerlilik kazandırır.
- 4- Servis sağlayıcılar, hukuka aykırı içeriklerden Telekomünikasyon Yasası'nın 85. paragrafı uyarınca iletişim sırrının korunması kapsamında haberdar oldukları ve erişimin engellenmesinin teknik olarak olanaklı ve kendilerinden beklenebilir olduğu durumlarda, söz konusu içeriklerin kullanımının önlenmesine ilişkin genel düzenlemeden doğan yükümlülükler saklıdır.

THK bu esnada Bilişim ve İletişim Servisleri Yasası ile reforma tabi tutulmuştur (2002). Alman Teleservisler Kanununda internet süjelerinin sorumluluğunun nasıl düzenlendiğine ilişkin olarak bkz. **ERMAN**, Almanya Hukukunda İnternette Kaynaklanan Ceza Sorumluluğu, sh: 205.

Münih Sulh Ceza Mahkemesi tarafından sanığın mahkumiyetine ilişkin olarak THK md. 5/2 hükmüne dayanılarak verilen karar oldukça tartışılmıştır. Alman doktrininde sanığın THK md. 5/3 hükmüne beraat etmesi gerektiği düşüncesi hakimdi. Bu da , THY md. 5/3 bağlamında sanığın eyleminin “*sadece yabancı içeriklerin kullanımını mümkün kılan girişi sağlaması*”ndan ibaret olduğu ve içerik üzerinde herhangi bir tasarrufta bulunmadığı düşüncesine dayandırılmaktaydı. Ancak Münih Sulh Ceza Mahkemesi CompuServe – Almanya’yı kendine özgü kullanıcıları olmadığı ve ağa girişi sağlamadığı için THK md. 5/3 bağlamında bir giriş sağlayıcısı olarak addedilmemiştir.

THK md. 5/2’ye göre hizmet sunucusunun – ki burada erişim sağlayıcı olarak anlamak gerekiyor - sorumluluğuna gidilebilmesi için, yabancı içeriklerin engellenebilmesinin teknik açıdan mümkün ve beklenebilir olması bir zorunluluktur. Münih Sulh Ceza Mahkemesi CompuServe- Almanya’yı hakim şirket olan CompuServe- A.B.D.’nin bir yan şirketi olarak değil aksine hakim ve bağlı şirketin oluşturduğu bir bütünün içinde değerlendirdiği için, yukarıda bahsedilen ve CompuServe – A.B.D. için aranan zorunlulukları CompuServe – Almanya için de aramıştır.

Bunun yanında Münih Sulh Ceza Mahkemesi hakim şirket olan CompuServe – A.B.D.’nin tehlike kaynaklarına karşı doğrudan müdahalede bulunmasına yönelik bir garanti yükümlülüğünün varlığını kabul etmesine rağmen, pozitif bir eylem olarak sanığın iştirakinin söz konusu olduğu düşüncesinden hareketle sanığın garanti yükümlülüğü ile hiç ilgilenmemiştir.

Münih Sulh Ceza Mahkemesi’nin çok ciddi eleştirilerle karşılaşmış olan kararına karşın yapılan temyiz başvurusu neticesinde Münih Eyalet Mahkemesi THK md. 5/3’e göre sanığın beraatine karar vermiştir. Mahkeme sanığın yöneticisi olduğu CompuServe – Almanya hakim şirket olan CompuServe – A.B.D.’ne tamamıyla tabi olduğu ve bu nedenle kendine özgü bir eylem iradesine sahip olmadığı için Münih Sulh Ceza Mahkemesinin sanığın iştirakine ilişkin tespiti reddedilmiştir. Ayrıca ihmal suretiyle iştirak hususunda da, hakim şirket olan CompuServe – A.B.D.’ye tabi olan bağlı şirketin eylem iradesinin eksikliği sebebiyle sanığın bir garanti sorumluluğu reddedilmiştir. Sanığın 13.02.1996 tarihinden sonra hart pornografiye yönelik malzemenin yayılmasını isteyerek gerçekleştirip gerçekleştirmediği

kesin bir şekilde ispat edilemeyeceği için, Al. C.K. md. 184'te düzenlenen suç tipi bakımından sanığa herhangi bir ceza öngörülmemiştir⁴⁵².

6.7.- TCK'ye Hakim İştirak Sistemi İçinde İnternet Søjelerinin Konumu

Tüm bu açıklamalar ve uygulama örneğinin ardından 5651 sayılı Kanun çerçevesinde sorumlulukları belirlenmiş olan internet søjelerinin 5237 sayılı TCK'de düzenlenen iştirak sistemi içinde nasıl bir konum alabilecekleri üzerine bir deęerlendirmede řu tespitleri yapmak mümkündür.

i.- Öncelikle içerik 5651 sayılı Kanun çerçevesinde sorumluluk alanı belirlenen içerik sağlayıcı bakımından deęerlendirilecek olursa, tanım itibariyle içerik sağlayıcı internet ortamına her türlü içerięi aktaran ve üzerinde tasarrufta bulunan bir internet søjesi olarak, suç teşkil edecek bir içerięin internette yayınlanması ile doğrudan fail olarak cezai müeyyidenin tarafı olacaktır. Bilindięi üzere kanunumuzda açık bir tanım verilmemiş olsa bile doğrudan fail, sergiledięi davranış ile suç olarak belirlenen tipe uygun eylemin objektif ve sübjektif unsurlarını bizzat gerçekleştiren kişidir. Dolayısıyla örneğin bir içerik sağlayıcı olarak bir haber portalındaki habere hakaretamiz bir yorum yazan kişi veya bir web sitesine halkı kin ve düşmanlığa sevk edecek bir metin yayınlayan kişi veya aynı şekilde bir video paylaşım sitesine çocuk pornografisi görüntülerini haiz bir videoyu yükleyen kişi doğrudan fail olarak kabul edilecektir.

Doğrudan faillik sadece icrai hareketler sergileyenler tarafından deęil ihmali hareketle bu ve benzeri suç neticelerinin doğmasına sebebiyet veren kişiler için de geçerli olacaktır. Örnek vermek gerekirse internette içerik yayınlanması herhangi bir moderatör denetimine ve iznine baęlı tutularak işlenen bir web sitesinin moderatörü, kendisine web sitesinde yayınlanmak üzere ulaştırılan ve suç teşkil eden bir veriyi yükümlü olduęu denetim görevini ifa etmesine rağmen web sitesinde yayınlanırsa doğrudan fail olarak kabul edilir ancak burada dikkat edilmesi gereken husus, suç içerikli veriyi bir web sitesinde yayınlanması için ilgili möderatöre gönderen kişi ile moderatör arasında suç işlemeye yönelik bir fikir birliği durumu

⁴⁵² HONG, Compuserve Davası, sh: 330.

söz konusu olmamalıdır. Çünkü böyle bir fikir birliğinin mevcudiyeti halinde 5237 sayılı TCK md. 37/1⁴⁵³,de düzenlenen birlikte faillik durumu söz konusu olacaktır.

Buna göre suç teşkil eden bir içeriğin internet ortamına aktarılması ve bu suretle yayınlanması konusunda ortak bir iradeyi paylaşan ve teknik gerekliliği yerine getirmek üzere birlikte hareket eden içerik sağlayıcılar birlikte faillik hükümleri gereğince her biri o suçun faili olarak değerlendirilecektir. Bu bağlamda üzerinde düşünülmesi gereken bir husus 5651 sayılı Kanunun içerik sağlayıcıların link verdikleri içerikten dolayı sorumlu tutulmalarına ilişkin düzenlemenin suça iştirak bakımından nasıl anlaşılmasının isabetli olacağıdır. *Kanaatimizce*, başka bir içerik sağlayıcıya ait olan ve internette hali hazırda yayınlanan suç içerikli bir veriye link vermek suretiyle erişim imkanı tanıyan bir içerik sağlayıcı, şayet suç teşkil eden o içeriğin sağlayıcısıyla internet ortamında yayınlanma ve erişilebilir kılma konularında ortak bir irade üzerinde hareket etmekteyse, bu durumda her iki içerik sağlayıcı bakımından md. 37/1 hükmünce birlikte faillik müessesesini işletmek gerekecektir⁴⁵⁴. Ancak her iki içerik sağlayıcı arasında böyle bir ortak irade söz konusu değilse, her ne kadar link veren içerik sağlayıcı suç teşkil eden içeriği internet ortamına aktarmamış olsa da link vermek suretiyle erişilebilir kılma fonksiyonunu üstlenmesi hasebiyle içeriği internet ortamına taşıyan içerik sağlayıcı ile birlikte doğrudan fail olarak ele alınmamalıdır.

Bunun dışında doğrudan aynı örnek üzerinden hareket edildiği takdir de, link vermek suretiyle içeriğe erişimi sağlayan içerik sağlayıcının, birlikte failliğin söz konusu olmadığı durumlarda, yayınlanan ve suç içerikli bir veriye erişim imkanı vermesinin doğrudan failliği

⁴⁵³ **Madde 37 - (1)** Suçun kanunî tanımında yer alan fiili birlikte gerçekleştiren kişilerden her biri, fail olarak sorumlu olur.

(2) Suçun işlenmesinde bir başkasını araç olarak kullanan kişi de fail olarak sorumlu tutulur. Kusur yeteneği olmayanları suçun işlenmesinde araç olarak kullanan kişinin cezası, üçte birden yarısına kadar artırılır.

⁴⁵⁴ Bu noktaya benzer bir konuda Yargıtay'ın verdiği bir karar dikkat çekicidir. Her ne kadar bir hukuk uyumsuzluğu için dahi olsa ceza sorumluluğunun tespiti için göz önünde bulundurulabilir bir nitelik taşıdığı kanaatindeyiz.

“Bir dava dosyasına sunulan dilekçelerin herhangi bir yorum yapılmaksızın aynen yayımlanması halinde, hukuka aykırılık unsurunun varlığından söz edilemez ve böylesi bir yayın tazminatla sorumlu tutulmayı gerektirmez. Ancak, aynen yayımlanan dilekçe metinleri, ilişkin buldukları davanın karşı tarafına veya üçüncü kişilerin kişilik haklarına yönelik açık ve ağır bir saldırı niteliğindeki söz ve ifadeleri içeriyor ise, böyle bir dilekçenin yayımlanması, dilekçe sahibinin eylemine katılma (iştirak) niteliğinde görülür ve hukuk düzenince tasvip edilemez. Böyle bir durumda, yayımı yapan, salt başkasınca yazılmış bir dilekçeyi haber konusu yaptığını savunarak, sorumluluktan kurtulamaz”. (Yargıtay HGK, 18.04.2007, E: 2007/4- 221 – K: 2007/213, Kaynak: Kazancı İçtihat Programı – Online, Erişim Tarihi: 22.03.2009, Saat: 16:00)

mi yoksa 5237 sayılı TCK md. 39⁴⁵⁵, da düzenlenen yardım etmeyi mi gündeme getireceği konusudur. *Kanaatimizce*, sadece yayınlanması suretiyle suç teşkil edecek bir içeriğin link verilmek suretiyle erişilebilir kılınması durumunda, o linki veren içerik sağlayıcının doğrudan fail olarak kabul edilmesi gerekmektedir. Zira md. 39/2 c.3'de bir eylemin yardım etme sayılabilmesi için suçun işlenmesinden önce veya işlenmesi sırasında yardımda bulunmak gerekmektedir. Örnek durumda ise, suç teşkil eden bir içeriği internet ortamına taşıyan içerik sağlayıcı, o içeriği yayınlamaya başladığı anda suç tamamlanmış olur. Bu andan itibaren, o içeriğe erişimi sağlamak suretiyle yayınlamasına katkıda bulunulan eylemin sahibi olarak link veren içerik sağlayıcı, link vermek suretiyle dolaylı bir yayın faaliyeti icra ettiğinden o içerikten dolayı doğrudan fail olarak değerlendirilmelidir. Ancak söz konusu içeriğin sadece yayınlanması suç teşkil etmemekle birlikte başka bir suçun işlenmesine, anılan maddede sayılan 1. ve 2. koşullar çerçevesinde, yardım eden içerik sağlayıcı bir suç ortaklığı türü olan yardım etmekten sorumlu tutulabilir. Söz konusu yayının içeriği itibariyle bu suç ortaklığı azmettirmeye⁴⁵⁶ de dönüşebilir.

ii.- Yer sağlayıcının ve erişim sağlayıcının sorumlulukları çerçevesinde, başka bir içerik sağlayıcının suç içerikli verilerini bünyesinde barındırması veya erişiminin sağlanması durumu için yapılacak tüm açıklamalar yukarıdaki link veren içerik sağlayıcının durumu ile

⁴⁵⁵ **Madde 39** - (1) Suçun işlenmesine yardım eden kişiye, işlenen suçun ağırlaştırılmış müebbet hapis cezasını gerektirmesi hâlinde, onbeş yıldan yirmi yıla; müebbet hapis cezasını gerektirmesi hâlinde, on yıldan onbeş yıla kadar hapis cezası verilir. Diğer hâllerde cezanın yarısı indirilir. Ancak, bu durumda verilecek ceza sekiz yılı geçemez.

(2) Aşağıdaki hâllerde kişi işlenen suçtan dolayı yardım eden sıfatıyla sorumlu olur:

a) Suç işlemeye teşvik etmek veya suç işleme kararını kuvvetlendirmek veya fiilin işlenmesinden sonra yardımda bulunacağını vaat etmek.

b) Suçun nasıl işleneceği hususunda yol göstermek veya fiilin işlenmesinde kullanılan araçları sağlamak.

c) Suçun işlenmesinden önce veya işlenmesi sırasında yardımda bulunarak icrasını kolaylaştırmak.

⁴⁵⁶ **Madde 38** - (1) Başkasını suç işlemeye azmettiren kişi, işlenen suçun cezası ile cezalandırılır.

(2) Üstsoy ve altsoy ilişkisinden doğan nüfuz kullanılmak suretiyle suça azmettirme hâlinde, azmettirenin cezası üçte birden yarısına kadar artırılır. Çocukların suça azmettirilmesi hâlinde, bu fıkra hükmüne göre cezanın artırılabilmesi için üstsoy ve altsoy ilişkisinin varlığı aranmaz.

(3) Azmettirenin belli olmaması hâlinde, kim olduğunun ortaya çıkmasını sağlayan fail veya diğer suç ortağı hakkında ağırlaştırılmış müebbet hapis cezası yerine yirmi yıldan yirmibeş yıla kadar, müebbet hapis cezası yerine onbeş yıldan yirmi yıla kadar hapis cezasına hükmolunabilir. Diğer hâllerde verilecek cezada, üçte bir oranında indirim yapılabilir.

aynıdır. Burada özellikli olabilecek bir durum gerek yer sağlayıcı gerekse erişim sağlayıcı açısından, kendilerine suç içerikli bir verinin internet ortamından çıkarılması veya erişiminin engellenmesi yolunda yapılan bildirimlere riayet etmeyerek söz konusu içeriği barındırmaya devam edilmesi veya erişiminin mümkün kılınması halinde söz konusu olacaktır. *Kanaatimizce* bu gibi durumlarda takip edilmesi gereken tutum yine link veren içerik sağlayıcıda olduğu gibi suç teşkil eden verinin niteliğinin ve içeriğinin birinci derece dikkate alınmasıdır. Buna bağlı olarak söz konusu içeriğin internet ortamından çıkarılması veya internet erişiminin engellenmesi yönündeki uyarıya riayet etmemenin anlamlandırılması gerekmektedir.

7.- İNTERNET ORTAMINDA İŞLENEN SUÇLARA YÖNELİK UYGULANACAK HUKUKUN TESPİTİ SORUNU

7.1.- Genel Açıklamalar

İnternet ortamında işlenen suçlara hangi hukukun uygulanacağı problemi en temel sorunlardan birini teşkil etmektedir. Daha önce de ifade edildiği üzere klasik anlamda ulusal hukuk kültürünün bir ürünü olan ve prensip olarak o ülkenin hukuksal sınırları dahilinde uygulama alanı bulan ceza hukuku, modern toplumun en önemli bileşenlerinden biri olan internet teknolojisinin gelmiş olduğu nokta ve bu teknolojinin yansımaları itibariyle özellikle uygulanabilirlik açısından birçok tartışmayı bünyesinde barındırmaktadır. Belki de bu tartışmaların son yıllarda sıkça gündeme gelmesinde ulusal ceza hukuku sistemlerinde özellikle internet ortamında işlenen suçlara karşı hangi hukukun uygulanacağına dair açık bir hükmün tesis edilmemiş olmasının payı büyüktür.

Keza Türk Ceza Hukukunda ileride de ortaya konulacağı üzere halen somut bir düzenlemeye gidilmemiştir. Bu da internet ortamında işlenen suçlara ilişkin uygulamada birçok problemin ortaya çıkmasına sebebiyet vermektedir. Ancak sorun sadece Türk Hukukunun bir sorunu olmanın ötesinde uluslar arası/ ulusal üstü bir sorundur. Şöyle ki; her ne kadar ceza hukuku sistemimizde bu problemin çözümü konusunda eksiklikler olsa da, bu sorun sadece ulusal düzenlemelerle aşılabilecek bir sorun değildir. Nasıl ki internet suçluluğu ile ulusal sınırlar dahilinde yürütülen mücadele bir noktadan sonra yetersiz kalıyor ve uluslar arası işbirliği bir gerekliliğe dönüşüyorsa, iç hukukta eksikliklerin giderilmesi için

atılan adımlar da bir noktaya kadar netice vermektedir. Uluslar arası yeknesaklık sağlanmadığı sürece bu problemler açıktan veya gizli mevcudiyetlerini sürdüreceklerdir.

İnternet ortamında işlene suçlara uygulanacak hukukun tespiti sorununa Türk Hukuku perspektifinden bakmadan önce konu ile ilgili olarak Almanya Ceza Hukukundaki düzenleme ve tartışmalardan örnekler vermek suretiyle soruna derinlik kazandırmak yerinde olacaktır.

7.2.- Alman Ceza Hukukunda İnternet Ortamında İşlenen Suçlara Uygulanacak Hukukun Tespiti Sorununa İlişkin Tartışmalar

Doğası gereği sınırları aşan karakteri internet ortamında işlenen suçlar bakımından öncelikle uluslar arası ceza hukuku prensiplerinin ortaya konulmasını zorunlu kılmaktadır. Almanya’da ceza hukukunun yer yönünden uygulanabilirlik ölçütleri Al. CK. §3 ila 7 ve § 9 hükümleri çerçevesinde ele alınmaktadır. Mülkilik prensibinin düzenlendiği §3 alman hukukunun uygulanabilirlik anlamında temel prensibini yansıtır⁴⁵⁷. Buna göre devlet, egemenlik alanı içerisinde işlenmiş olan bütün suçlar için fail ve/veya mağdur/suçtan zarar gören kişinin tabiiyetine bakmaksızın alman ceza hukukunun uygulanması gerekmektedir. Bağlantı noktası olarak suçun işlendiği yeri esas alan bu prensip § 9 ile yakın ilişki içerisinde. Başka bir anlatımla, § 9’a göre suçun işlendiği yer olarak hem eylemin gerçekleştiği hem de tipik neticenin doğduğu yer esas kabul edilmektedir. Bu hüküm “Ubiquitätsprinzip” olarak kabul görmektedir.⁴⁵⁸

Faile göre şahsilik prensibinin düzenlendiği § 5/ 3a, 5b, 8,9,11a, 12, 14a, 15 hükümleri çerçevesinde alman hukukunun uygulanabilirliği bakımından bağlama noktası olarak failin vatandaşlığı esas alınmıştır. Bu bağlamda devletin anayasal organlarını tahkir etmek suçu, eylem yabancı bir ülkede işlenmiş olsa dahi faile göre şahsilik prensibinin işletildiği bir örnek olarak kabul edilebilir. Keza bu eylemin yabancı bir ülkeden yüklenen verilerle internet ortamında işlenmesi düşünüldüğünde konuyla ilişkisi daha açık bir şekilde görülmektedir.

⁴⁵⁷ COLLARDIN, Markus, Straftaten im Internet, in: CR, 1995, sh: 618 vd.

⁴⁵⁸ Ubiquitätsprinzip ile ilgili detaylı değerlendirme için bkz. ESER, Albin, Internet und Internationales Strafrecht, in: Rechtsfragen des Internet und der Informationsgesellschaft: Symposium der rechtswissenschaftlichen Fakultäten der Albert-Ludwigs-Universität Freiburg und der Städtischen Universität Osaka, Heidelberg, 2002, sh: 308 v.d.

§ 5’de düzenlenen koruma prensibi de kimin tarafından işlendiğine bakılmaksızın devletin iç hukuk menfaatlerini korumak amacıyla işlettiği bir prensip olarak görülmektedir. Bu prensibe örnek olarak da internette Al. CK. § 90 kapsamında başbakana karşı aşağılayıcı, tahkir edici ifadelerin kullanılması dolayısıyla § 5/3b çerçevesinde ulusal hukukun uygulanması kabul edilmektedir.⁴⁵⁹

Yine §6/ 1-8’de düzenlenen evrensellik ilkesi de suçun işlendiği yere, failin ve mağdurun vatandaşlığına bakılmadan ortak düşmana karşı mücadele edilmesi yaklaşımından hareketle tesis edilmiş bir hükümdür. Bu hüküm çerçevesinde, örnek olarak internet aracılığıyla hart pornografi içerikli verilerin yayılması suçu (§ 184/3) karşısında uygulanacak hukukun tespitinde evrensellik prensibi esas kabul edilecektir.⁴⁶⁰

Bir başka prensip de § 7/2 hükmü çerçevesinde ikame ceza yargısı prensibidir. Buna göre faili elinde bulunduran devlet suçun işlendiği ülkeyi temsilen yargı yetkisi kullanmaktadır. Bu prensibin uygulanabilmesi için failin ülkede ele geçirilmesi, mülklik ve diğer ilkelere göre yargı yetkisine sahip olan devletin veya hukuki nedenlerle kovuşturma yetkisinin kullanılmaması veya kullanılmak istenmemesi gerekir.

Alman ceza hukukunun uygulanabilirliği açısından temel prensibi teşkil eden mülklik prensibi suçun işlendiği yerin tespiti sorunu ile de yakından ilgilidir. Bu bakımdan Al. CK. § 3’ü, Al. CK. § 9 /1’de yapılan düzenlemeler olmadan ele almak eksiklidir. Çünkü Al. CK. § 9/1, § 3 gereğince alman ceza hukukunun uygulanabilirliğinin tespitinde bağlam noktalarını ortaya koymaktadır. Bu değerlendirme internet ortamında işlenen suçlar bakımından da önem arz etmektedir. Al. CK. § 9/1 dört adet bağlama noktası belirlemiştir⁴⁶¹. Bunlar;

- a- fiilin icra edildiği yer (§ 9/1-1)
- b- ihmali suçlarda yerine yükümlülüğün yerine getirilmesi gereken yer (§9/1-2)
- c- suç unsurlarını barındıran tipik neticenin gerçekleştiği yer (§9/1-3)
- d- failin tasavvuru gereğince suçun gerçekleşmesi gereken yer (§9/1-4)

⁴⁵⁹ **ESER**, Internet und Internationales Strafrecht , sh.:309.

⁴⁶¹ **SIEBER**, Ulrich, Internationales Strafrecht. Das Territorialitätsprinzip der §§3, 9 StGB im globalen Cyberspace, in : NJW, 1999, sh: 2065.

O halde internet ortamında işlenen suçlar bakımından, suç teşkil eden eylemde Al. CK § 9/1 mucibince bağlama noktası Almanya ise, suç Almanya’da işlenmiş sayılır ve Alman Ceza Hukuku uygulanır.

Bu noktada anılan bağlama noktaları çerçevesinde suçun işlendiği yerin tespiti bakımından Alman doktrininde ortaya konan farklı yaklaşımları aktarmakta yarar vardır. Kimi yazarlar Al. CK. § 9/1-3 çerçevesinde getirilen bağlama noktasının özellikle internette işlenen suçlar bakımından sorunlu bazı neticelere neden olabileceği dile getirilmektedir. Şöyle ki; anılan hükme göre özellikle internet yayınları bakımından neticenin gerçekleştiği mekanın Almanya olduğu kabul edilmesi gerektiği söylenmektedir. Çünkü internette yayımlanan yasak içerikli bilgilere Almanya sınırları dahilinde topraklarında ulaşıldığı takdirde, her ne kadar söz konusu eyleme vücut veren hareket ülke dışında gerçekleştirmiş olsa dahi, neticenin gerçekleştiği yer Almanya olduğu için alman hukuku internet üzerinden ulaşılabilen ve tipe uygun eyleme vücut verebilen her içeriğe ilişkin ceza hukuku uygulamalarında kullanılabilir.⁴⁶²

Bu durum günümüz uluslar arası hukuk açısından sakıncalı sonuçlara vücut verebilir. Çünkü böyle bir durumda Almanya dünya üzerindeki tüm internet ortamında işlenen suç için uygulanabilirlik iddiasına sahip olacaktır ki bu da diğer ülkelerin egemenlik yetkisini hiçe sayan bir tutuma sebebiyet verecektir. Alman makamlarının *Bremer’in* ifadesiyle “Dünya Polisliğine” soyunması anlamına geleceği tespitine *Hilgendorf* şu ifadelerle destek vermektedir.

“Politik olarak bu görüş savunulamaz zira alamn hukuku tüm dünyada uygulanabilir değildir. Ve suç konusu olan fiillerde everensel takip ilkesinin güvencesine tabi değildir. Alman hukukunun internet yolu ile bu neviden “globalleşmesi” yabancı devletleri Almanya’ya tabi kılan ve “ Dünya Alman varlığında ihya olacaktır” şiyarının çağcıl bir versiyonu olarak görünmektedir. Diğer devletlerin de internet üzerinden işlenen suçları kovuşturmaya teşebbüs etmeleri ve kendi ceza hukuklarının uygulanma alanını bu kadar genişletmek çabaları; epey kaygı verici bir düşüncedir. Buna rağmen düzenleme yapmak isteyenler kendi ceza kanunları için de uluslar arası hukukunun sınırlarını tanıyan bir anlayışa kavuşmalıdırlar. Tüm bu sebeplerden ötürü alman hukukunun internet üzerindeki uygulama alanını sınırlayan bir düzenleme makul gözükmektedir.”

⁴⁶² HILGENDORF, Eric, Yeni Medya, sh: 273- 274.

Bu anlamda Al. CK §9/1'in tahdidi bir yoruma tabi tutulması gerektiği inancı Alman doktrininde birçok yazar tarafından ifade edilmiştir. Bu yönde Alman ceza hukukunun uygulanması alanında anılan hükme sınırlayıcı bir bakış açısıyla “ amaçsal ilgi (*finale Interesse*)” yaklaşımı ortaya konulmuştur. Buna göre bir internet ortamında işlenen bir özellikle bir içerik suçuna karşı alman hukukunun uygulanabilirliğinden bahsedebilmek için , suç teşkil eden hareket (hukuka aykırı verinin internete yüklenmesi) Almanya dışından gerçekleşmiş olsa dahi, neticenin bizzat ve özellikle Almanya'da meydana gelmesi gerekmektedir.⁴⁶³

Fakat bu yaklaşım, özellikle internet ortamında gerçekleştirilmiş bir hareketin Almanya'da bir etki yaratacak neticeye yönelik olduğunun tespitinin çok zor olması dolayısıyla eleştirilere maruz kalmıştır. Çünkü böyle bir kriterden hareket etmek, aynı zamanda suç teşkil eden eylemde özel bir kastın aranmasını zorunlu kılmaktadır. Peki bu kastın tespitinde hangi kriter esas alınmalıdır? Bu kriterler arasında, söz konusu verinin almanca olması gibi amaca uygun olmayan ve gerçekçilikten uzak kriterlere başvurulması söz konusu değerlendirmeyi daha da tartışılır kılmıştır⁴⁶⁴.

Hilgendorf, uygulanabilirlik ile ilgili olarak yukarıda özet halinde sunulan öneri ve eleştiriler karşısında, söz konusu muammayı netliğe kavuşturmak için en sağlıklı çözümü § 9/1-3 hükmünün Almanya'da doğan her suç neticesi bakımından değil, sadece ilgili suça ait bağlamdaki tipik neticenin doğması halinde uygulanabilir olmasında görmektedir.

İnternet ortamında işlenen suçların zarar veya tehlike suçu olmasının uygulanabilirlik açısından ne gibi bir etkisinin olduğu sorunu da yine Al. CK. §9/1-3 çerçevesinde üzerinde durulan sorunlardan biri olmuştur. Zarar suçları bakımından önemli bir sıkıntı görünmese de tartışma somut ve soyut tehlike suçları açısından yapılmaktadır. Buna göre somut tehlike suçları bakımından, artık somutlaşan bir tehlike durumunun varlığından hareketle, tehlikenin bir neticeye dönüştüğü kabul edilerek, somut tehlike suçları bakımından uygulanabilirliğin

⁴⁶³ COLLARDIN, Straftaten im Internet, sh: 621.

⁴⁶⁴ “Ancak öncelikle belirtmeliyiz ki; anılan genel geçerlilik prensibini eylemin subjektif yönü bağlamında sınırlandırmaya yönelik çabalar, § 9/1-3 hükmü dikkate alındığında zaten Alman Hukukunun tüm suç tipleri bakımından evrensel uygulamasının mümkün olmaması sebebiyle hatalı temellere sahiptirler” HILGENDORF, Yeni Medya, sh: 274.

tartışıldığı noktada aynı netice suçlarında olduğu gibi Al. CK. §9/1-3 hükmünün esas alınabileceği dile getirilmektedir⁴⁶⁵.

Soyut tehlike suçlarına dair durum ise bayağı tartışmalıdır. Hatta Alman Ceza hukukunun uygulanabilirliği üzerine önemli davalardan biri olan *Toeben* Davasında soyut bir tehlike suçunda netice yerinin var olup olmadığı hususunu açık bıraktığı görülmektedir. Ancak *Hilgendorf'a* göre, soyut tehlike suçları isimlerini, kanun koyucunun herhangi bir tehlike durumunu soyutlamasından almaktadırlar. Bu sebeple soyut tehlike veya soyut tehlikelilik tabirleri pek isabetli değildir. Zira bir tehlike az veya çok somut bir olgudur. Asla soyut değil. Soyut tehlike olmadığından bundan bahsetmenin de anlamı yoktur. Özetle yazar internette gerçekleşen soyut tehlike suçlarının tipik bir neticeye vücut veremediklerini savunmaktadır. Buradan da soyut tehlike suçları için Al. CK. § 9/1-3 hükmünün etkisiz olduğu anlaşılmaktadır.

Nihayet Al.CK. § 9/1-3 hükmünün geniş anlaşılmasının önüne geçmek için ortaya konulan bir başka öneri de § 7 hükmünü internet ortamında işlenen suçlar bakımından bir bağlama noktası yapmaktır. Şöyle ki; ülke sınırları dışında internet aracılığıyla icra edilmiş suç niteliğindeki bir eylem Alman hukukunun uygulanabilmesi için tipik neticenin Almanya'da gerçekleşmiş olması ve eylemin bir alman vatandaşına karşı işlenmiş olması, failin eylem anında alman vatandaşı olması veya eylem anından sonra alman vatandaşı olmuş olması şartları aranmaktadır. *Breuer* bu şartların arasına failin eylem anında Almanya'da bulunan bir yabancı olması ve iade edilememiş olması da eklenmesi gerektiğini savunur. Ancak bu görüş de bazı noktalar açısından yetersiz görülmektedir. Örneğin bu kriterin uygulama darlığının internet ortamında işlenecek suçların tamamını kapsamayacağı ve internetin sınır aşan kimliği karşısında yetersiz kalacağı önemli eleştirilerden biridir.⁴⁶⁶

7.3.- Türk Ceza Hukuku Sisteminde İnternet Ortamında İşlenecek Suçlara Uygulanacak Hukukun Tespiti

Türk ceza hukukunda uygulanacak hukukun tespiti ölçütleri alman hukukuyla paralellik göstermektedir. Uygulanacak hukukun tespiti açısından Türk hukukunda geçerli olan ilkeler;

⁴⁶⁵ HILGENDORF, Computer- und Internetstrafrecht sh: 69.

⁴⁶⁶ BREMER, Karsten, Strafbare Internet- Inhalte in internationale Hinsicht, sh: 113, Kaynak: <http://deposit.ddb.de/cgi-bin/dokserv?idn=963762524> (Erişim Tarihi: 08.11.2007, Saat: 00:10),

- a- TCK md. 8-9- Mülklik prensibi
- b- TCK md. 10- 11 – Faile göre şahsılık prensibi
- c- TCK md. 12(1-2 – Koruma ilkesi
- d- TCK md. 12/3 – Evrensellik ilkesi

Bu İlkerler içerisinde mülklik prensibi alman hukukunda olduğu gibi temel prensip olarak dikkati çekmektedir. TCK md. 8'e göre suç teşkil eden bir fiilin kısmen veya tamamen Türkiye'de işlenmesi veya neticenin Türkiye'de gerçekleşmesi durumunda Türk hukukunun geçerli olduğu prensibi kabul edilmektedir. Bu yaklaşımdan hareketle suçun işlendiği yerin tespiti hususunda Türk hukukunun da Alman hukuku gibi karma sistemi benimsediği anlaşılmaktadır. Başka bir ifade ile suçun işlendiği yerin tespiti bakımından ne salt harekete ne de salt neticeye ağırlık verilmekte, hem netice hem de hareket dikkate alındığı için karma bir bakış sergilenmektedir. Ancak yukarıda alman ceza hukukunun uygulanabilirliği konusunda ortaya konan çekincelerin Türk ceza hukuku bakımından da geçerli olduğu görülmektedir.

Karma yaklaşımın doğal sonucu olarak uygulanabilirliğin çok geniş anlaşılması ve CMK'dan kaynaklanan kovuşturma mecburiyetinin varlığı söz konusu durumu özellikle internet ortamında işlenen suçlar konusunda oldukça zorlamaktadır. İnternet ortamında işlenen suçlar bakımından netice ve hareket ilişkisine yukarıda değinilmişti. Bu durumda söz konusu suçluluğa ilişkin kovuşturma makamının dünya üzerinde geçerli bir yargı yetkisinin varlığından bahsetmek, daha önce de ifade edildiği gibi “dünya polisliği” yapmak gibidir ve pratik açıdan verimsizdir. Bu yüzden özellikle internet ortamında işlenen suçların durumuna ilişkin herhangi bir normatif düzenlemenin olmayışı sorunu içinden çıkılmaz bir hale sokacaktır. Bunu engellemenin en kesin yolu da internet ortamında işlenen suçlar için TCK 'ya özel bir hüküm vazetmek ve sorunu o çerçevede çözmektir.

8.- TÜRKİYE'DE İNTERNET ORTAMINDA İŞLENEN İÇERİK VE MÜDAHALE SUÇLARIDA YER BAKIMINDAN YETKİ SORUNU

8.1.- Genel Açıklamalar

İnternet ortamında işlenen suçlara hangi ülke hukukunun uygulanacağına ilişkin değerlendirmelerin ardından Türkiye’de gerçekleşen ve internet ortamında işlenen suçlarda yer yönünden yetki tepsinin yapılması da önem arz etmektedir. Özellikle gerek uygulamada gerekse doktrinde tartışmalı bir hususu teşkil eden bu konuyu ele almak adına daha önce ortaya koyduğumuz ve devamında da kullandığımız içerik suçları ve müdahale suçları ayırımının kullanılabilceği kanaatindeyiz. Bu nedenle internet ortamında işlenen suçlarda yer bakımından yetki ikili ayırımımız temelinden ortaya konulacaktır.

8.1.1.- Müdahale Suçlarında Yer Yönünden Yetkili Mahkemenin Tespiti Sorunu

İnternet ortamında işlenen müdahale suçlarına ilişkin yer yönünden yetki ile ilgili olarak öncelikle göz önünde bulundurulması gereken hüküm hiç şüphe yok ki CMK. md. 12’dir. Anılan maddenin birinci fıkrasına göre davaya bakmak yetkisi suçun işlendiği yer mahkemesine aittir. O halde yer bakımından yetki konusunda en önemli hareket noktası suçun işlendiği yerin tespitidir. Suçun işlendiği yerin tespiti yapılırken suçun karakteri önem arz etmektedir⁴⁶⁷. Öyle ki, örneğin neticesi harekete bitişik suçlarda hareket ile netice birlikte gerçekleşmekte, dolayısıyla hareketin icra edildiği yer aynı zamanda neticenin gerçekleştiği yer olduğundan, suçun işlendiği yer de aynı yer kabul edilir. Benzer bir değerlendirme ani suçlar için de yapılabilir. Ancak hareketle neticenin ayrılabilceği suçlarda durum farklı olmaktadır. Örnek vermek gerekirse mütemadi suçlarda hareketin icrası ile suçun tamamlanması yani neticelenmesi arasında fark vardır⁴⁶⁸. Yine hareket ile neticenin ayrılabilceği suçlara örnek olarak verilebilecek mesafe suçlarında suç teşkil eden hareket bir yerde gerçekleştirilirken netice başka bir yerde gerçekleşmektedir. Dolayısıyla özellikle mesafe suçlarında suçun hareketin gerçekleştiği yerde mi yoksa neticenin gerçekleştiği yerde mi işlendiği konusunda tartışmalar çıkmaktadır. Bu konuda doktrinde farklı değerlendirmeler yapılmaktadır.

Bu değerlendirmeleri en genel manada üç kategori altında ele almak mümkündür. Bunlardan birincisi harekete üstünlük tanıyan görüştür. Bu görüş savunucularına göre suç hareketin yapıldığı yerde işlenmiş sayılmaktadır⁴⁶⁹. Çünkü önemli olan insanın iradesinin ortaya konulmasıdır. Bu da ancak hareketle anlaşılabilir. İkinci görüş savunucuları ise,

⁴⁶⁷ CENTEL, Nur/ ZAFER, Hamide, Ceza Muhakemesi Hukuku, 4. Baskı, İstanbul, 2006, sh: 456.

⁴⁶⁸ DEMİRBAŞ, Timur, Ceza Hukuku Genel Hükümler, 3. Baskı, Ankara, 2005, sh: 217- 218.

⁴⁶⁹ DEMİRBAŞ, Ceza Hukuku, sh: 136.

harekete öncelik tanıyan görüşe karşı neticenin önceliğini savunmaktadırlar⁴⁷⁰. Buna göre, suç hareketin neticesinin ortaya çıktığı yerde gerçekleşmiş sayılmaktadır. Bunun nedeni suçun ancak netice ile belirlenebilir olması ve o suçla korunması amaçlanan hukuksal değerın ancak neticenin doğmasıyla ihlal edildiğinin belirmesi olarak gösterilmektedir. Üçüncü görüş ise her iki görüşü de bir pota içinde eriten karma görüştür⁴⁷¹. Bu görüş savunucuları ise bir ülke içinde gerçekleşen mesafe suçlarında karma teorinin kabul edilebileceğini ve suçun hem hareketin gerçekleştiği hem de neticenin doğduğu yerde işlenmiş kabul edilebileceğini savunmaktadır. Dolayısıyla ortada iki yetkili mahkeme söz konusu olacaktır. Bu durumda önerilen çözüm yolu, yetkili olan mahkemelerin aralarında anlaşarak, suçun kovuşturulması konusunda daha uygun olan mahkemenin belirlenmesidir⁴⁷².

Bu kısa değerlendirmeden sonra şunu ifade etmekte hiçbir sakınca yoktur ki, internet ortamında islenen suçlar mesafe suçlarıdır. Çünkü bu suçlar ister içerik isterse müdahale suçları olsunlar, internet ortamında suç teşkil edecek hareketle ulaşılmak istenen netice farklı yerlerde gerçekleşmektedir. O nedenle CMK. md. 12 çerçevesinde yetkili mahkemenin tespitinde suçun işlendiği yer önem arz ettiği için burada yukarıda belirtilen görüşler dairesinde bir tercih yapmak gerekecektir. Yargıtay aslında doğrudan ifade etmemiş olsa bile internet ortamında gerçekleşen müdahale suçları bakımından netice teorisine öncelik verdiği izlenimi doğmaktadır⁴⁷³. Şöyle ki, 5237 sayılı TCK md. 244/4’de düzenlenen bilişim sistemindeki verileri değiştirmek suretiyle haksız menfaat temin etme suçu, önerdiğimiz ayırım çerçevesinde bir müdahale suçu olarak kabul edilebilir. Davaya kaynaklık eden olayda fail, müşterilere ait hesaplardan internet aracılığıyla kendi hesabına para aktarmıştır. Yargıtay işlenen suçun md. 244’de düzenlenen suça vücut verdiğine ilişkin değerlendirmesinde,

“Bilişim sistemindeki verileri değiştirmek suretiyle haksız menfaat elde edilmesi suçunun sanık tarafından havalenin şikayetçilerin hesaplarından kendi hesabına intikali anında tamamlandığı gözetilmeyerek eylemin teşebbüs aşamasında kaldığından bahisle eksik ceza tayini...”

⁴⁷⁰ DEMİRBAŞ, Ceza Hukuku, sh: 137.

⁴⁷¹ TEZCAN, Durmuş/ ERDEM, Mustafa Ruhan/ ÖNOK, Murat, Uluslar arası Ceza Hukuku, Ankara, 2009, sh: 88.

⁴⁷² CENTEL/ ZAFER, Ceza Muhakemesi Hukuku, sh: 458.

⁴⁷³ Bkz. Yargıtay 11. CD., 18.09.2007, E: 2007/6963 – K: 2007/5533, Kaynak: Kazancı İçtihat Programı – Online, Erişim Tarihi: 22.03.2009, Saat: 10:00)

demek suretiyle aktarma işleminin yapıldığı anı yani hareketin gerçekleştiği anı değil, intikalın gerçekleştiği yani neticenin doğduğu anı suçun tamamlandığı an kabul ettiği için, dolayısıyla suçun gerçekleştiği yeri de neticenin doğduğu yer olarak kabul etmektedir⁴⁷⁴. Bu anlamda Yargıtay'ın bu tercihinin, özel bir düzenleme söz konusu olmadığı durumlarda benzer nitelikte diğer müdahale suçları için de geçerli görmesi gerekmektedir.

Kanaatimizce, bir mesafe suçu olarak internet ortamında işlenen müdahale suçlarında hem hareketin hem de neticenin gerçekleştiği yeri suçun işlendiği yer sayan karma görüşün, bu alanda işlenen suçlarla mücadele bakımından etkili olması muhtemeldir. Çünkü özellikle soruşturma aşamasında delil elde etme ve kovuşturma aşamasında elde edilen delillerin değerlendirilmesinde çok ciddi zorlukların yaşandığı bu alanda suç teşkil eden hareketin yapıldığı yer ve neticenin doğduğu yerin hangisinde ceza muhakemesi şartları daha olgunsa suç kovuşturmasının da orada yapılması uygun olacaktır. Bunun tespiti de hareketin ve neticenin gerçekleştiği yer mahkemeleri arasında kararlaştırılabilir.

8.1.2.- İçerik Suçlarında Yer Yönünden Yetkili Mahkemenin Tespiti Sorunu

İnternet ortamında gerçekleştirilen içerik suçlarında yer bakımından yetkili mahkemenin tespitinde de yukarıda yaptığımız değerlendirmelerin paralelinde karma görüşün benimsenebileceğini söylemek mümkündür. Ancak içerik suçları açıklama ve yayma niteliğinde olduğu için CMK md. 12/5'in de ek olarak incelenmesi ve değerlendirilmesi gerekmektedir. Zira anılan hüküm görsel ve işitsel yayınlarla işlenen suçlara ilişkin bir düzenlemedir. Buna göre suç görsel ve işitsel yayınlar vasıtasıyla işlenecek olursa aynı maddenin suçun basın aracılığıyla işlenmesi halini düzenleyen üçüncü fıkranın uygulanacağını ayrıca söz konusu yayının mağdurun yerleşim yeri veya oturduğu yerde

⁴⁷⁴ Benzer nitelikli başka bir kararında da “2-Dolandırıcılık suçları ile ilgili hükmün temyizine gelince, A)Dolandırıcılık suçundan unsur olan kandırabilecek nitelikteki hilenin, gerçek kişiye yönelmesi ve bu kişinin hataya düşürülüp onun veya bir başkasının zararına, fiili işleyene veya başkasına haksız bir menfaat sağlanması gerekir, Somut olayda; sanığın, mağdurların bankalarda bulunan para hesaplarındaki var olan verileri (bilgileri)sahte kimliklerle açtığı hesaplara internet yoluyla göndererek, yine sahte kimliklerle bu paraları çekmek istemesinden ibaret eylemlerinin; paranın sanığın açtığı hesaplara intikaline kadar gerçek kişilere yöneltmiş hile bulunmayıp eylemlerin tamamen bilişim sistemi içinde gerçekleştirildiğinden, her bir mağdura karşı işlenmiş ayrı ayrı 5237 sayılı TCK. nun 244/4 maddesine uyan suçu oluşturduğu ve paranın açtığı hesaplara transferiyle suçun tamamlanacağı gözetilmeden...(Yargıtay 9. CD. 27.09.2007, E: 2007/ 6709 – K: 2007/6012, Kaynak: Kazancı İçtihat Programı – Online, Erişim Tarihi: 22.03.2009, Saat: 10:00)” demek suretiyle suçun gerçekleşmesi bakımından yine neticeye öncelik verdiği anlaşılmaktadır. Yargıtay burada neticeyi hesaba intikal edilen paraları almak olarak değil paranın hesaba intikali olarak görmektedir.

görmesi veya işitmesi halinde suçun o yerde de işlendiğinin kabul edildiği belirtilmektedir. Atıfta bulunulan üçüncü fıkra hükmünce basın aracılığıyla işlenen suç, ülkede yayınlanan bir basılı eserle işlenmişse yetki, eserin yayım merkezi olan yer mahkemesine aittir. Ancak eser birden çok yerde basılmışsa ve suç teşkil eden içerik başka yerde basılan eserde yer alıyorsa o halde bu suç için o eserin basıldığı yer mahkemesi de yetkilidir.

Bu normatif düzenleme incelemesinden sonra doktrinde konuya ilişkin tartışma örneklerine yer vermek gerekirse, *Özgenç* yayın yoluyla işlenen suçlarda yayının yapıldığı her yerde suçun ilendiğini kabul ederken internet ortamında yapılan yayınlar bakımından da durumun aynı olduğunu ifade etmiştir. Başka bir ifade ile yazar internet ortamında yapılan yayınlarda, söz konusu içeriğe ulaşılabilen her yerde suçun işlendiğini kabul etmektedir. Ancak bu tür suçlar için CMK md. 12'nin sınırlayıcı hükümlerle düzenlemeler yaptığını ve bunun da göz önünde bulundurulması gerektiğini ifade etmiştir⁴⁷⁵. Benzer bir yaklaşımı kabul eden *İçel/ Ünver* ise, özellikle internetin küresel kimliğini ön plana çıkartarak internet ortamında işlenen suçların internete bağlı her ülkede ve bu meyanda Türkiye'de de işlendiğinin kabul edilmesi gerektiğini dile getirmişleridir⁴⁷⁶. Bu tespitten hareketle yazarların Türkiye'de de suç içerikli bir verinin erişilebildiği her noktada suçun işlenmiş olduğunu öngördüklerini söylemek yanlış olmayacaktır. Akis görüş savunan *Tezcan/ Erdem/ Önok'a* göre ise, internet yoluyla işlenen suçlarda internet içeriklerinin dünyanın her yerinden erişilebilir kılınması nedeniyle söz konusu içeriklere ulaşma olanağının bulunduğu her yerde ve bu arada Türkiye'de suçun işlendiğinin kabulü halinde, ortaya çıkacak yetki tartışmalarının üstesinden gelinemeyecektir. Bu nedenle başvurulması gereken yolun, suç teşkil eden içeriğin nerede sunulara yüklendiğinin tespiti olduğu kanaatindedirler. Buna göre, suçun işlendiği yer içeriğin görüldüğü yer değil suç teşkil eden içeriğin sunulara yüklendiği yerdir. Bunun dışındaki hallerde internet yoluyla işlenen suçların Türkiye de işlenmiş sayılması ve dolayısıyla ülkesellik ilkesinin çerçevesinde kovuşturulması imkansızdır⁴⁷⁷.

Kanaatimizce mevcut düzenlemeler bakımından internet ortamında işlenen içerik suçlarının nerede işlendiği konusunda önemli eksiklikler mevcuttur. Her şeyden önce CMK md. 12/3'ün internete uygulanması çok zor hatta imkansızdır. Çünkü ilgili hüküm Basın Kanunu çerçevesinde basılı eserler aracılığıyla işlenen suçlar için geçerli olup, internete

⁴⁷⁵ **ÖZGENÇ**, Ceza Hukuku, sh: 728 (3 nolu dipnot)

⁴⁷⁶ **İÇEL/ ÜNVER**, Kitle Haberleşme Hukuku, sh: 480.

⁴⁷⁷ **TEZCAN/ ERDEM/ ÖNOK**, Uluslar arası Ceza Hukuku, sh: 92-93.

yönlendirilmesi oldukça zordur. Öyle ki, basılı bir eser için basım merkezi veya basıldığı yer tespiti yapmak mümkünken internet için bunun belirlenmesi imkansızdır⁴⁷⁸. Ayrıca aynı maddenin 5. fıkrasında görsel ve işitsel yayınlar için ayrı bir hüküm konulmuştur. Her ne kadar bu hükmün konulmasıyla basılı eserler dışındaki yayın araçları kastedilmiş ise de, 5237 sayılı TCK md. 6'da yapılan basın yayın yolu tanımlamasında görsel, işitsel ve elektronik kitle iletişim araçlarından bahsedilmektedir. Ancak CMK md. 12/5'de sadece görsel ve işitsel yayınlar düzenleme kapsamı dahiline alınmıştır. Dolayısıyla internet yayıncılığı bakımından CMK md. 12/5 uygulanabilir kabul etmek kanunilik açısından sorunlu neticeler ortaya koyabilir. Mevcut halde kanaatimizce tercih edilebilecek yol, içerik suçları bakımından suç teşkil eden hareketin ve neticenin doğduğu yerler ile birlikte suç teşkil eden içeriğin kayıtlı olduğu yer sağlayıcının bulunduğu yerde suçun işlendiği kabul edilmelidir ve buradaki mahkemelerin her birini yetkili kılmak gerekecektir.

Ancak esas kalıcı çözüm *Ünver*⁴⁷⁹ ve *İlkiz'in*⁴⁸⁰, 765 sayılı TCK döneminden itibaren söyledikleri gibi, karakter olarak arklı bir yapıya sahip olan internette işlenen suçlarda suçun işlendiği yerin ayrıca ve açıkça ifade edilmesi gerekmektedir. Aksi takdirde birçok değerlendirme hatasının ortaya çıkması kaçınılmazdır.

⁴⁷⁸ TAŞKIN, Bilişim Hukuku, sh: 175.

⁴⁷⁹ ÜNVER, TCK ve Ceza Kanunu Tasarısının Değerlendirilmesi, sh: 139-140.

⁴⁸⁰ İLKİZ, İnternet Ortamında Yayınlar, sh: 457.

ÜÇÜNCÜ BÖLÜM

TÜRK CEZA KANUNUNDA İNTERNET ORTAMINDA İŞLENEBİLEN SUÇLAR

1.- TÜRK CEZA HUKUKUNDA İNTERNET ORTAMINDA İŞLENEBİLEN BAZI SUÇLARIN DEĞERLENDİRİLMESİ

1.1.- Genel Olarak

Birinci bölümde modern toplum olarak tanımlana bilgi toplumunun temel yapısal özellikleri ve modern ceza hukuku ile olan ilişkisi sorunsallaştırılırken, özellikle bilgi akışındaki hızın ve bilgiyi kullanım alanlarındaki uçsuz bucaksız genişlemenin üzerinde durulmuştur. Bu değerlendirmenin hiç şüphe yok ki temel ekseni internet teknolojisinin gelişimi ve kullanım alanlarındaki etkinliğidir. Bugün dünyada milyarlarca insan siber uzayda hiçbir sınır çatışması yaşamadan dünyanın her bir noktasındaki bilgiye saliseler ile ölçülebilecek hızda ulaşabilmekte, tüm ihtiyaçlarını internet aracılığıyla giderebilir hale gelmiştir. Tabi ki burada kullanıcılar ile hizmeti sunanlar arasındaki arz – talep ilişkisinin önemi büyüktür. Öyle görünüyor ki, hiç de uzak olmayan bir gelecekte bu arz – talep ilişkisi internet lehine gelişecek internet aracılığıyla şuan tasavvur edilemeyen noktalara ulaşılacaktır.

Tabi ki internet sadece hayatın kolaylaşmasına sebebiyet vermemekte, aynı zamanda ortaya çıkardığı problemler dolayısıyla da ciddi bir potansiyel tehlike olarak algılanmaktadır. Çünkü internet aracılığıyla kurulan siber alem halen bir çok boşluklara sahip olup bu boşluklar nedeniyle birçok insanın zarar görmesine neden olmaktadır. Bunun en önemli nedeni de internet teknolojisinin her yaş ve seviye grubuna hitap etmesi, en temel düzeyde ihtiyacı giderebilmesi açısından geniş bir teknik bilgi ve yetenek gerektirmemesidir. Kullanıcıların internet aracılığıyla bilgi aktarım ve paylaşımında birkaç basit komut olarak gördükleri ve bilgi eksikliğinden çok fazla önemsemedikleri bazı tehlikelerin altında yıllarını bu teknolojinin gelişine vermiş, tabiri caizse bu işi meslek edinmiş kimselerin sinsi plan ve “programları” yatmaktadır. Kullanıcıya çok masum gelen bir e-posta veya bir onay penceresinin kendisinin gerçek anlamda siber uzaydan silinmesine neden olabileceği pek düşünülmemektedir. Bu sebeple internetin amacına uygun kullanılması için mutlak suretle bu

tehlikeleri bertaraf edecek hukuksal düzenlemelerin yapılması gerekmektedir. Bu anlamda da en büyük güvence ceza hukukunda gerçekleştirilecek amaca uygun düzenlemelerdir⁴⁸¹.

Özellikle ikinci bölümde de suç genel teorisi çerçevesinde internet ortamında işlenen suçlara ilişkin sorunlu noktalar ve tartışmalar ortaya konulduktan sonra üçüncü bölümde, tarafımızca önerilen sınıflandırmaya sadık kalarak 5237 sayılı TCK'de yer alan ve internet ortamında işlenebilen içerik ve müdahale suçlarından önemli bazı suç tipleri ele alınacaktır. Burada incelemeye esas kabul edilen suç tercihinde dikkat edilen en önemli nokta, suçun işlenişi veya değerlendirilmesi boyutunda internetin bir özellik arz edip etmediğidir. Dolayısıyla burada incelenen suç tipleri dışında da kalan suçlardan internet aracılığıyla işlenen suçların var olduğu özellikle ifade edilmelidir. Daha önceki bölümlerde ifade edildiği üzere internetin bir kitle iletişim aracı olarak kabul edilmesiyle birlikte bir suçun basın yayın yolu ile işlenmesi bakımından geçerli olan genel değerlendirmeler suçun internet aracılığıyla iletilmesi için de geçerli kabul edilebilecektir. Dolayısıyla bu bölümde kanaatimizce özellikli addedilen bazı suç tipleri birinci ve ikinci bölümde ortaya konan teorik yapı üzerinden değerlendirilecektir.

1.2.- TCK'de Düzenlenen Bazı İçerik Suçlarının Değerlendirilmesi

1.2.1.- İntihara Yönlendirme

Hiç şüphe yok ki, internet teknolojisinin getirdiği yenilikler birçok alanda toplumsal hayatı kolaylaştırırken aynı zamanda birçok problemin ortaya çıkmasına da vesile olmuştur. Siber uzayın boşluklarında kendini gizlemeyi başaran veya gizlediğini düşünen kişiler yeni bir yaşam alanı olarak gördükleri interneti hukuksuz bir alan olarak tasarlayıp⁴⁸² her türlü sapkın davranışların ve eğilimlerin mekanı haline de getirmeye çalışmaktadırlar. Bu anlamda birçok suç tipi internet aracılığıyla işlenebilir hale gelmiştir. Bu suçlardan biri de intihara

⁴⁸¹ İnternetin bir kitle haberleşme aracı olarak tasarlanması hakkında ayrıntılı değerlendirme için bkz. **İÇEL/ÜNVER**, Kitle Haberleşme Hukuku, sh: 7 – 9.

⁴⁸² Konu ile ilgili ayrıntılı değerlendirme için bkz. **HILGENDORF**, Eric, Ist das Internet ein rechtsfreier Raum? in: Kriminalität im Internet - Strategien zu ihrer Bekämpfung. Kooperationstagung der dbb akademie und der Deutschen Polizeigewerkschaft im dbb am 12.11. 2001/ München, Bonn 2002, sh: 12 v.d. ; **WENNING**, Rigo, Das Internet – ein rechtsfreier Raum?, Kaynak: <http://www.jurpc.de/aufsatz/19970016.htm> (Erişim Tarihi: 07.02.2008, Saat: 09:27); **JUNKER**, Markus, Anwendbares Recht und internationale Zuständigkeit bei Urheberrechtsverletzungen im Internet, sh: 47, Kaynak: <http://www.upress.uni-kassel.de/online/frei/978-3-933146-78-6.volltext.frei.pdf> (Erişim Tarihi: 12.02.2008, Saat: 11:17)

yönlendirmedir. Günümüzde birçok kişi internette tanıştıkları kişiler vasıtasıyla veya internet sitelerinde yayınlanan intihara yönlendirme kapsamlı içeriklerle kendi yaşamlarını sonlandırmaktadırlar. Bu anlamda internet üzerinde önemle durulması gereken bir hal almaktadır⁴⁸³.

İntihara yönlendirme suçu 5237 sayılı TCK md. 84 düzenlenmektedir⁴⁸⁴. Madde ilk önce “İntihar” olarak düzenlenmiş ancak yapılan eleştirilerden sonra 29.06.2005 tarih ve 5377 sayılı Kanununun 10. maddesi ile “İntihara Yönlendirme” olarak değiştirilmiştir.⁴⁸⁵

⁴⁸³ “Bu hususa ilişkin örnekler vermeye mümkündür. Örneğin, Amerika’da Arizona – Phoenix’de yaşayan 21 yaşındaki Brandon Vedas sayılarının yaklaşık 9000 olduğu tahmin edilen “intihar siteleri”nden birine bağlandıktan sonra kendisini web kamerası ile izleyen yaklaşık 12 kişinin karşısında alkol, hap ve marihuandan oluşan bir karışım içerek intihar etti ve ertesi gün yatağında ölü bulundu. 11 Ocak 2003 günü Brandon “Ripper” nicki ile sık sık bağlandığı bir sohbet odasına girdi ve sanal arkadaşlarıyla buluştu. Aynı zamanda web kameralarıyla da birbirlerini görebiliyorlardı. Bir süre sonra alkol ile birlikte hap lamaya başladı. Sanal arkadaşlarından birinin “ Bir tane daha al, hayır hayır 1000 tane daha al”, diğerinin ise “ bu yetmez daha fazla al. Senin yaşayıp yaşayamayacağını veya karanlığa gömülüp gömülemeyeceğini izlemek istiyorum” dediği öğrenildi.” Bu konuda ülkemizde dahil olmak üzere dünyanın bir çok köşesinden bir çok örneğe rastlamak mümkündür, bu bağlamda konu ile ilgili detaylı bilgi için bkz. **ÖZDİLEK**, Ali Osman, İntihar ve İnternet, <http://www.turk.internet.com/abone/login.php?l=2&location=/haber/yazigoster.php3?yaziid=6532> (Erişim Tarihi: 10.12.2007); “İnternet üzerindeki suçların çoğu 16-22 yaş grubu arasına dağılmış çocuklar ve gençler tarafından işleniyor. Bu suçlar çok geniş yelpazeye yayılmış durumda. Suç işleyen çocuklar ve gençler olduğu gibi, kendisine zarar veren gençler de İnternet kurbanı olarak görülüyor. Konunun en ilginç örneği yakın zamanda Galler’de yaşandı. Sosyal network’lerde yer alan gençler arasında birbiri ardına gelen intihar girişimleri Bridgend kasabasını derinden sarsmaya devam ediyor. 17 yaşındaki Natasha Randall’in arkadaş çevresi oldukça genişti. Çocuk eğitimi üzerine eğitim alan Natasha bir süredir kendini mutsuz hissediyordu. Bir gün odasında kendini asmış şekilde bulundu. Galler’in Bridgend kasabasında meydana gelen bu olay bölgede son zamanlarda meydana gelen yedinci intihar vakası. Aileler ve polis alarma geçti. İnternet’teki sosyal network’ler üzerinden mesaj almış olma şüphesi üzerinde duruluyor. Kasabada bu olayın ardından 15 yaşında iki kız çocuğu da intihar girişiminde bulundu. Bir tanesi bileğini keserken diğeri de kendini asmaya yeltendi. Son anda hayata döndürülen iki kızdan biri hala hastanede tedavi altında. Ailesi bir an olsun başından ayrılmıyor. Polis bileklerini keserek hayatını kaybeden Tasha adındaki kızın arkadaşları ve okulu içinde detaylı araştırma yapıyor. Tasha’nın intihar girişiminin yaklaşık on ay öncesinde Bridgend ve çevre bölgede altı genç erkek çocuk kendini öldürdü. Tasha’nın yakın bir süre önce intihar eden Liam Clarke’nin cenazesine katıldığı kanıtlandı. Yapılan araştırma, ölen tüm gençlerin birbirlerini tanıdıklarını ortaya çıkardı. ‘Bebo’ isimli sosyal network’te bir araya gelen grupların birbirleriyle sürekli iletişim halinde oldukları ortaya çıktı. Liam ölmeden önce de Bebo’daki Liam’in web sayfasında Tasha’da gelen mesaj bulundu. Tasha mesajında şöyle diyor: R.I.P Clark! Seni özleyeceğiz! Her zaman geçirdiğimiz güzel anları hatırla! Seni seviyorum!’ Tasha da öldükten sonra, bilgisayarını polis tarafından inceleme altına alındı. Diğer ölümlerle ilgili de bazı bağlantılar ortaya çıkarıldı”. Kaynak: http://www.haber7.com/haber.php?haber_id=295383/Internet-baglantili-7-esrarli-intihar, (Erişim Tarihi:26.01.2008, Saat: 21:08); Kaynak: <http://arsiv.sabah.com.tr/2008/01/24/haber,7E629FA6E6514F50BEAE1A62882138EE.html> (Erişim Tarihi: 26.01.2008, Saat: 21:10)

⁴⁸⁴ Madde 84 - Başkasını intihara azmettiren, teşvik eden, başkasının intihar kararını kuvvetlendiren ya da başkasının intiharına herhangi bir şekilde yardım eden kişi, iki yıldan beş yıla kadar hapis cezası ile cezalandırılır.

(2) İntiharnın gerçekleşmesi durumunda, kişi dört yıldan on yıla kadar hapis cezası ile cezalandırılır.

(3) Başkasını intihara alenen teşvik eden kişi, üç yıldan sekiz yıla kadar hapis cezası ile cezalandırılır.

(4) İşlediği fiilin anlam ve sonuçlarını algılama yeteneği gelişmemiş olan veya ortadan kaldırılan kişileri intihara sevk edenlerle cebir veya tehdit kullanmak suretiyle kişileri intihara mecbur edenler, kasten öldürme suçundan sorumlu tutulurlar.

⁴⁸⁵ **YILDIZ**, Türk Ceza Kanunu, sh: 183.

“İntihara Yönlendirme” suçunun 765 sayılı TCK’deki karşılığı olan 454. madde ile karşılaştırıldığında 765 sayılı TCK md. 454’de intihara yönlendirme suçunun oluşması bakımından tipe uygun hareket olarak ikna ve yardımın birlikte yapılmasının tercih edildiği görülmektedir. Ayrıca söz konusu suçun gerçekleşmesi için kişinin intihar kararı bakımından ikna ve yardım ile birlikte bu girişimlerin neticesinde kişinin yaşamını yitirmesi aranmaktadır. Buna karşın 5237 sayılı TCK md. 84’de suçun maddi unsuru bakımından seçimlik hareketlerin mevcut olduğu (md. 84/1 – azmettirme, teşvik etme, intihar kararını kuvvetlendirme, yardım etme) ve bu seçimlik hareketlerden herhangi birinin tek başına gerçekleşmesi durumunda dahi bu suçun gerçekleşeceği kabul edilmektedir. Yine 765 sayılı TCK md. 454’ün aksine intihar sonucu ölüm neticesinin doğması suçun gerçekleşmesi için zorunlu bir koşul olmaktan çıkartılmış ve md. 84/2’de belirtildiği üzere ölüm neticesinin doğması intihara yönlendirme suçu bakımından bir ağırlaştırıcı neden olarak düzenlenmiştir.⁴⁸⁶

İntihara yönlendirme suçu internet açısından değerlendirilecek olursa; öncelikle suçun *fail ve mağduru* bakımından 5237 s. TCK md. 84’de yapılan düzenleme dikkate alınmalıdır. Genel anlamda gerek fail gerekse mağdur için özel bir durum yaratılmadığı görülmektedir. Bu bakımdan intihara yönlendirme suçunda herkesin fail veya mağdur olması mümkündür. Tek özellikli durum olarak maddenin son fıkrasında kasten adam öldürme suçuna yapılan gönderme gösterilebilir. Buna göre intihara yönlendirme suçu, işlediği fiilin anlam ve sonuçlarını algılama yeteneği gelişmemiş olan ya da ortadan kaldırılmış bir kişiye karşı işlenecek olursa veya mağdur cebir ya da tehditle intihara mecbur bırakılırsa fail intihara yönlendirmeden değil kasten adam öldürmeden dolayı sorumlu tutulacaktır (md. 84/4). Dolayısıyla failin intihara yönlendirme suçunun değil kasten adam öldürme suçunun faili olarak kabul edilmesi söz konusu olacaktır. Haliyle mağdur da kasten adam öldürme suçunun mağduru olarak kabul görecektir⁴⁸⁷. Bu durum suçun internette işlenebilirliği bakımından oldukça önemlidir. Keza bugün internet her yaş ve seviye grubundan kişi tarafından kullanılmaktadır. Özellikle yaş grubu itibarıyla algılama ve muhakeme yeteneği gelişmeyen çocuklara karşı intiharı özendirerek nitelikte iletiler gönderilmesi, sohbetlerde bulunulması ya da yayınların yapılması neticesinde söz konusu fıkranın uygulanabilirliği gündeme gelecektir. Ancak bu noktada dikkat edilmesi gereken bir husus vardır. Söz konusu fıkroda özellikle anılan gruptaki hedef kişilerin intihara mecbur bırakılmaları arandığı için basit düzeyde

⁴⁸⁶ Ayrıntılı değerlendirme için bkz. **CENDEL/ ZAFER/ ÇAKMUT**, *Kişilere Karşı İşlenen Suçlar*, sh: 78 v.d.

⁴⁸⁷ Bu düzenleme 765 sayılı TCK’da yer almamakla birlikte doktrinde savunulan yaklaşımlardan biri olmuştur. Konu ile ilgili tartışmalar için bkz. **DÖNMEZER**, *Kişilere ve Mala Karşı Cürümler*, sh: 102.

kalmış intihara yönlendirme eylemleri (önceki fıkralarda ortaya konmuş olan) bu kapsama girmeyecektir. Şu haliyle md. 84/4’de düzenlenen özelliikli durumu isabetli bulmaktayız.

Suçun maddi unsuru bakımından intihara yönlendirme suçu yukarıda da ifade edildiği üzere seçimlik hareketli bir suçtur. Başka bir anlatımla md.84/1 hükmünce intihara yönlendirme suçu başkasını intihara azmettirmek, teşvik etmek, başkasının intihar kararının kuvvetlendirmek, başkasının intiharına herhangi bir şekilde yardım etmek suretiyle işlenebilir.⁴⁸⁸ Dikkat edilecek olursa, yapı itibariyle her dört seçimlik hareket de internet aracılığıyla gerçekleştirilebilmektedir. Özellikle ilk üç seçimlik hareketin internet aracılığıyla gerçekleştirilebilmesinde bir problem yoktur. Ancak yardım etmenin internet aracılığıyla nasıl gerçekleşeceği sorusuna yanıt da madde metninde gizlidir. Öyle ki kanun koyucu intihara yönlendirmede yardım konusunda herhangi bir sınırlamaya gitmemiş ve her türlü yardımı bu düzenleme kapsamına soktuğu için, örneğin bir web sitesinde veya forum ya da sohbet odalarında veya e- posta ve benzeri kişisel iletiler aracılığıyla özel bir intihar tarzının nasıl gerçekleştirileceği yönünde ayrıntılı bilgi verilmesi durumunda, söz konusu seçimlik hareket gerçekleşmiş olur. Ancak burada söz konusu bilginin intihara açıkça yönlendirici nitelikte olmasının aranması gerekmektedir⁴⁸⁹. Örneğin internet ortamında (bir web sitesi, forum, sohbet odaları ya da kişisel iletiler aracılığıyla olması fark etmeksizin) bir madde ya da karışımın insan sağlığı için çok tehlikeli neticelere sebebiyet vereceğinin vurgulanması durumunda, her ne kadar bu bilgiye erişen kimse bahsedilen madde veya tarzla intihar etmiş dahi olsa şayet kişilerin bu madde veya tarzın kullanılması suretiyle intiharı özendirilmesi söz konusu değilse, burada intihara yönlendirmede yardımdan bahsedilemez. Dolayısıyla burada “yardım etmek” kavramını dar anlamda değerlendirmek gerekmektedir.

⁴⁸⁸ Bu bağlamda seçimlik olarak düzenlenen hareketlerden neyin kastedildiğine bakılacak olursa; *İntihara azmettirmenin*, bir kişinin bir başkasının intihar düşüncesine gelmesini sağlayarak onu intihara yönlendirmesi, yani intihar etme düşüncesine sahip olmayan bir kişide bu fikrin oluşturulmasıdır. Azmettirmen söz edebilmek için intihar eden veya intihara teşebbüs eden kişi, azmettirenin yönlendirmesi gerçekleşmeseydi eylemi işlemeyecekti denilebilmesi gerekmektedir. *Teşvik etmek*, intihara teşvik mağdurda intihar etme düşüncesini uyandırmak, bu konuda ona destek olmak ve vereceği kararı onaylamaktır. İntihar etmeye teşvik ile azmettirme arasındaki fark şudur. Azmettirmede başkasını intihara ikna etmenin söz konusu olmasına karşılık teşvik etme mağdurda mevcut ama henüz ortaya çıkmamış olan intihar düşüncesini uyandırmak demektir. *Kararı güçlendirme*, bu yönde kararını vermiş olan failin cesaretlendirilmesi, bazı nedenlerle bu kararını uygulayamıyorsa, uygulama eğilimini güçlendirme yolunda faaliyette bulunulmasıdır. *İntihara yardımdan* söz edilebilmesi için mağdurun daha önce intihara karar vermiş olması gerekmektedir. İntihardan önce veya intihar sırasında eylemin icrasını kolaylaştırma yardım etmektir. Konu ile ilgili olarak ayrıntılı değerlendirmeler için bkz. **CENTEL/ ZAFER/ ÇAKMUT**, *Kişilere Karşı Suçlar*, sh: 80 v.d.; **TOROSLU**, *Nevzat, Ceza Hukuku Özel Kısım*, Ankara, 2007, sh: 37 v.d.; **TEZCAN/ ERDEM/ ÖNOK**, *Ceza Hukuku Özel Hükümler*, sh: 135 v.d.

⁴⁸⁹ *Salihpaşaoğlu’na* göre 5187 sayılı Basın Kanunu ile 5680 sayılı Basın Kanununda yasak yayımlar içinde belirtilen intihar olaylarına, cinsel saldırı ve cinayetler de eklenmiştir. Madde metninden de anlaşılacağı üzere cinsel saldırı, cinayet ve intihar olaylarına ilişkin haberlerin sadece veriliş biçimi sınırlandırılmıştır. Dolayısıyla okuyucuyu bu tür fiillere özendirilebilecek nitelikte olmamak şartıyla bu olaylarla ilgili haberlerin verilmesi ve resimlerin yayınlanması bu suçu oluşturmayacaktır. **SALİHPAŞAOĞLU**, *Basın Özgürlüğü*, sh: 165.

Bu deęerlendirmeye paralel olarak *manevi unsuruna* geilecek olursa, gerek Yargıtay uygulamalarında gerekse doktrinde intihara ynlendirme suçunun kasten işlenen bir suç olduęu kabul edilmekte ve kastın türü bakımından da özel bir tercihte bulunulmamakta, manevi unsur olarak genel kast esas alınmaktadır⁴⁹⁰. Bunun yanında doktrinde anılan suçun TCK md. 21/2 çerçevesinde bu suçun kastın bir türü olan olası kastla işlenebilmesi de mümkün olduęu ve failin suçun kanuni tipe uygun neticenin gerekleşebileceğini öngörmesine rağmen maęduru intihara ynlendirmeye yönelik harekette bulunması halinde bu suçun olası kastla işleneceğinin kabulünü savunan görüşlere rastlanmaktadır⁴⁹¹.

Suçun internet aracılığıyla işlenebilirliği bakımından *kusurluluęu* etkileyen herhangi bir durumun söz konusu olup olmadığı ele alınacak olursa; failin 5237 sayılı TCK md. 28 ve 29 hükmünce cebir, şiddet, korkutma ve tehdit altında veya haksız tahrik etkisiyle bu suçun işlenmesi durumu pek mümkün görünmemektedir, ancak özellikle internet teknolojisinin kullanımında sıklıkla hatlara düşülmesi dolayısıyla failin eyleminde TCK md. 30 anlamında bir hatadan bahsedilip bahsedilemeyeceğii üzerinde durulabilir. Özellikle internet üzerinden kurulan iletişimde kullanıcı isimleri, milyonlarca kullanıcı ile karışmaması için “*nick name*” denilen takma isimler, normal isimlerden farklı şekillerde veya sembollerle desteklenerek oluşturulmaktadır. Ayrıca internette iletişim olanağı sunan birçok varlığı da kişileri hata yapmaya sevk etmektedir. Dolayısıyla internet ortamında girişilen hareketlerde hata yapma olasılığı artmaktadır. Bu anlamda internette en çok karşılaşılan hata türü olan şahısta hataya örnek olarak bir kişiye e- posta aracılığıyla hakaret etmek isteyen bir başka kişinin, hedef kişinin e- posta adresinde bir harf veya sembolü yanlış bilmesi veya girmesi neticesinde başka bir kişiye hakaret içerikli e- postayı göndermesi gösterilebilir⁴⁹². **Ancak kanaatimizce uygulamada gözden kaçırılması muhtemel bir hata türünün bu suç açısından gerekleşmesi mümkündür. Daha önce üzerinde durulduęu gibi internette aleniyet sadece herkes için doğrudan erişilebilirliğinin söz konusu olduęu durumlarda deęil, aynı**

⁴⁹⁰ “İntihara ikna suçunun teşekkül edebilmesi için müntehire karşı failin suumuamelede bulunması ve müntehirin de maruz kaldığı suumuameleden bizar olarak intihar ettiğinin sübutu kağı olmayıp fail tarafından bu neticenin kasıt ve istihdaf edildiğinin sübutu da şarttır.” YCGK 29.01.1951, 1950 – 261/17, **CENTEL/ ZAFER/ ÇAKMUT**, Kişilere Karşı Suçlar, sh: 84, dipnot: 20’den naklen.

⁴⁹¹ Bkz. **CENTEL/ ZAFER/ ÇAKMUT**, Kişilere Karşı Suçlar, sh: 84.

⁴⁹² 5237 sayılı TCK md. 30’da şahısta hata ayrıca düzenlenmemiştir. Madde gerekçesinde de ifade edildiğii üzere şahısta hata durumları birinci fıkrada düzenlenen suçun maddi unsurlarında hata ve ikinci fıkrada düzenlenen suçun nitelikli unsurlarında hata çerçevesinde düşünülmüştür. Ayrıca hedefte sapma halinde de bir hatanın söz konusu olmadığı gerekçesiyle md. 30 kapsamında düzenlenmemiştir. Ayrıntılar için bkz. **ÖZGENÇ**, Ceza Hukuku, sh: 402- 403.

zamanda belli koşullar altında dolaylı veya aşamalı erişilebilirliğin söz konusu olduğu durumlarda da geçerlidir. Örnek verilecek olursa, bir web sitesinde yorum sayfasına yorum eklemek için üyeliğin şart koşulmasını, o içeriğin aleniyetini engelleyen bir faktör olarak algılayan bir kişi, söz konusu sayfaya üyelik başvurusu yapan ve bilgileri eksiksiz dolduran herkesin üye olabileceğini, dolayısıyla buradaki üyelik prosedürünün aleniyeti engelleyen bir prosedür olmadığını atlaması sonucu o siteye intiharı teşvik eden bir yorum yazarsa bu durum suçun nitelikli halinde yapılan hata kapsamında (TCK md. 30/2) değerlendirilmelidir. Çünkü md. 84/3 de suçun aleni işlenmesi ağırlaştırıcı bir nedendir.

Suçta etki eden nedenler arasında interneti en yakından ilgilendiren düzenleme maddenin üçüncü fıkrasındaki düzenlemedir. Buna göre, başkalarını intihara alenen teşvik eden kişi üç yıldan sekiz yıla kadar hapis cezası ile cezalandırılacaktır. Maddenin ilk halinde anılan ağırlaştırıcı nedene ek olarak suçun basın yayın yolu ile işlenmesi de yer almıştı⁴⁹³. Ancak 29.06.2007 tarih ve 5377 sayılı kanunla yapılan değişiklikle bu hüküm madde metninden çıkarılmıştır. Bu değişikliğin gerekçesi de aynen şöyle yapılmıştır.

“Suçun basın ve yayın yoluyla işlenmesi hali de, aleniyetin gerçekleşiş şekillerinden birini oluşturmaktadır. İntihara teşvik suçuyla ilgili olarak aleniyet bir nitelikli unsur olarak belirlendiği için, söz konusu suçun basın yayın yoluyla işlenmesi, bu suç açısından ayrı bir nitelikli unsur olarak görülmemiştir.”

Bu değişiklik internet açısından irdelendiğinde, suçun internet aracılığıyla işlenmesi bakımından herhangi bir farklılığa sebebiyet verilmediği görülmektedir. Çünkü gerekçede de aktarıldığı üzere bir suçun işlenmesinde aleniyet unsurunun aranması kaplamsal bir bakış açısını beraberinde getirecektir. Bu yüzden suçun basın yayın yolu ile işlenmesi bu bağlamda ele alınacaktır. O yüzden bir suçun basın yayın yoluyla işlenmesinde kabul edilen tüm hususlar suçun aleni işlenmesinin kabulünde evleviyetle göz önünde bulundurulacaktır. Fakat bu çerçevede aynı muhteviyatı kapsayan iki nitelikli halin birlikte düzenlenmemesi bakımından düzenlemenin isabetli olduğu söylenebilir. Bunun yanında bu değerlendirme yapılırken daha önce yapılan internetin basın - yayın aracı olarak kabulü ve aleniyet ilkesinin

⁴⁹³ YILDIZ, Türk Ceza Kanunu, sh: 183- 184.

kapsamına ilişkin açıklamalar her daim göz önünde bulundurulmalıdır⁴⁹⁴. Bu anlamda söz konusu ağırlaştırıcı neden salt internetin araç olarak kullanılması ile gündeme gelmeyecektir. Burada kastedilen internetin kamusal erişilebilirliği mümkün olan unsurlarında yapılan intihara teşviktir. Şayet aynı unsurları içeren davranış internetin kişiye özel alanında gerçekleşirse (e-posta gibi), yani aleniyetin söz konusu olmadığı ve ancak iletişimin taraflarınca bilinen bir intihara teşvik gerçekleşirse, burada suç internet aracılığıyla gerçekleşmiş olursa olsun aleniyet unsuru söz konusu olmadığından md. 84/3 değil şartlar gerçekleşmişse md. 84/1 hükmü uygulanır⁴⁹⁵.

Kanaatimizce fıkra hükmünün sadece intihara alenen teşviki kapsamı da hatalıdır. Suçun temel halinin düzenlendiği birinci fıkrada intihara yönlendirmenin seçimlik hareketli bir suç olduğu görülmektedir. Ancak üçüncü fıkrada sadece alenen teşvik ele alınmıştır. Şayet böyle bir hükmün düzenlenmesi ihtiyacı hissediliyorsa, bunun sadece teşvikle sınırlandırılmayıp “ *Suçun alenen gerçekleştirilmesi durumunda...*” şeklinde tüm seçimlik hareketleri kapsayacak şekilde yapılması gerekmektedir. Konu internet aracılığıyla işlenen intihara yönlendirme suçu bakımından değerlendirecek olunursa, bir internet sayfasında veya forumlarda intihara yönlendirme içerikli bir yazı veya resmin sadece intiharı teşvik edip etmediğine bakmak ve bu anlamda sınırlayıcı bir yorumda bulunmak sakıncalıdır. Bu içeriğin teknik anlamda azmettirme, daha önce verilmiş bir intihar kararının kuvvetlendirilmesi ve hatta bilgiler vermek suretiyle intihara yardım etme teşkil etmesi mümkündür. Bu anlamda yapılması gereken, ya böyle bir hükmün düzenlememesi ya da bir ihtiyaca binaen bir düzenleme yapılacaksa ihtiyacın doğru tespit edilmesi ve birinci fıkradaki tüm seçimlik hareketleri kapsamasıdır. Ayrıca aynı çelişki üçüncü fıkrada alenen intihara teşvik ile dördüncü fıkrada intihara sevk tercihinde de gözlenmiştir. Yani madde metninde fıkralar arasında bir kavram karmaşası yaşanmaktadır. Bu karmaşa içinde bir de suçun seçimlik hareketle işlenebileceği kabul edildiğinde somut olay değerlendirmesinde önemli problemlerin yaşanması muhtemeldir. Bu sorun suçun internet ile işlenebilirliği de dahil olmak üzere tüm maddeyi bir bütün halinde ilgilendiren bir sorundur.

⁴⁹⁴ Bkz. § 5. – 5237 Sayılı Tck Md. 6/1-G Hükmünce Bir Kitle İletişim Aracı Olarak İnternet Ve § 6.- Suça Etki Eden Neden Olarak Aleniyet Unsurunun İnternet Aracılığıyla İşlenen Suçlar Bakımından Değerlendirilmesi.

⁴⁹⁵ Konuyla ilgili ayrıntılı değerlendirme için bkz. **ÖZEL**, Cevdet, 5237 Sayılı Türk Ceza Kanunu'nun Basın Yayın Yoluyla İlenen/ İşlenmesi Mümkün Olan Suçlar Yönünden İncelenmesi, http://www.turkhukuksitesi.com/makale_713.htm (Erişim Tarihi: 10.12.2007).

Suçun özel görünüş biçimleri bakımından bir değerlendirme yapılacak olursa, intihara yönlendirme suçu sırf hareket suçu olması dolayısıyla kural olarak, suç teşkil eden davranışın gerçekleşmesiyle tamamlanmış olacağından *teşebbüse* elverişli bir suç tipi değildir. Ancak konu internet aracılığıyla işlenen intihara yönlendirme suçu bağlamında ele alındığında pekala söz konusu suç için teşebbüsten bahsetmek mümkündür. Çünkü internet aracılığıyla işlenen intihara yönlendirme suçunda hareketin bölünebilirliği söz konusudur⁴⁹⁶. Örneğin intihara yönlendirme kapsamında kanunda sayılan seçimlik hareketleri barındıran bir içerik e- posta aracılığıyla gönderilmek istenmesi ve fakat e- postanın muhatabına ulaşmaması (alıcı adresinin yanlış yazılması, alıcının e- posta kapasitesinin dolması nedeniyle e- postanın karşı tarafça okunamaması gibi) ya da forum veya sohbet odası denetçileri tarafından söz konusu içerikli mesajın internet sayfasına aktarılmaması veya içerik denetleme programları tarafından iletilmesi yasaklı kelimeleri barındıran metnin görüntülenmesinin engellenmesi gibi. Bu durumlarda suça teşebbüsten bahsedilebilmektedir.

Suçta *iştirak* bakımından suçun internet aracılığıyla işlenmesi bir ayrıcalık getirmez. İştirake ilişkin genel kurallar bu suç tipi için de geçerli olup özellikli bir durum yaratılmamıştır⁴⁹⁷.

İçtima konusunda ise suçun internette işlenmesi bir takım özellikler göstermektedir. Örneğin bir kişi birden fazla kişiye aynı anda tek bir e- posta göndermek suretiyle intihara azmettirmesi, teşvik etmesi, kararını güçlendirmesi, ya da onlara herhangi bir şekilde yardım etmesi durumunda zincirleme suç hükmünün uygulanması mümkün olabilir⁴⁹⁸. Yine aynı suç işleme kararıyla değişik zamanlarda anılan suçun seçimlik hareketlerinden herhangi birinin bir kişiye karşı icra edilmesi durumunda da zincirleme suç hükümleri devreye girecektir. Ancak md. 84/4'deki ağırlaştırıcı nedenin koşulları oluşursa aynı şartlarda burada bir zincirleme suçtan bahsetmek imkansızdır. Çünkü fıkra hükmünce suç, işlediği fiilin anlam ve

⁴⁹⁶ Sırf hareket suçlarına teşebbüsün söz konusu olup olmayacağı ile ilgili bkz. AYDIN, Devrim, Suça Teşebbüs, sh:110, Kaynak: <http://auhf.ankara.edu.tr/dergiler/auhfd-arsiv/AUHF-2006-55-01/AUHF-2006-55-01-Aydin.pdf> (Erişim Tarihi: 07.02.2008, Saat: 10:26)

⁴⁹⁷ İnternet süjelerinin, internet aracılığıyla işlenen suçlara iştirakinin dördüncü bölümde yapılacak açıklamalarla birlikte yapılmasının daha isabetli olacağı düşünüldüğünden söz konusu değerlendirmeye bu bölümde girilmemiştir.

⁴⁹⁸ Özgenç, 5237 sayılı TCK sisteminde suç sayısı belirlenirken neticenin değil fiilin esas alındığını ifade ederek bir fiille aynı suçun birden fazla kişiye karşı işlenmesi durumunda zincirleme suçun değil md. 43/2 hükmünce aynı neviden fikri içtimain söz konusu olduğunu kabul etmektedir. Yazarın görüşlerinin ayrıntıları için bkz. ÖZGENÇ, Ceza Hukuku, sh: 517 v.d. Ayrıca genel anlamda zincirleme suçun 5237 sayılı TCK'de düzenlenişi ile ilgili bkz. SANCAR, Türkan YALÇIN, Teni Türk Ceza Kanununda Zincirleme Suç, in: TBBD., Sayı: 70, Ankara, 2007, sh: 244 v.d.

sonuçlarını algılama yeteneği gelişmemiş veya ortadan kaldırılmış kişilere karşı işlenirse veya cebir şiddet tehdit kullanmak suretiyle işlenirse fail kasten adam öldürme suçundan dolayı sorumlu tutulacaktır. Kasten adam öldürme suçu da TCK md. 43/3 hükmünce zincirleme suçun istisnalarından sayıldığı için bu ağırlaştırıcı neden internet aracılığıyla gerçekleşse ve görünüşte zincirleme suça elverişli olsa dahi zincirleme suç söz konusu olmayacaktır.⁴⁹⁹

İnceleme konusu suçun internet aracılığıyla işlenebilirliği hususunda fikri içtima hükümlerinin de gerçekleşebileceği kabul edilebilir. Örneğin bir örgütün temsilcisinin e-posta ile veya elektronik ortamda yapılan sohbet esnasında bir veya birden fazla örgüt mensubuna, şehrin işlek caddesinde bir intihar eylemi gerçekleştirmeleri yönünde teşvik etmesi eyleminde, tek eylemle hem md. 84 hem de md. 214 kapsamında suç işlemeye tahrik suçu gerçekleştiği için her iki suçun fikri içtima hükümlerine göre değerlendirilebilir.⁵⁰⁰

1.2.2.- Cinsel Taciz

İnternetin son yıllarda en önemli problemlerinden birini cinsel çocuk pornografisi başta olmak üzere internet ortamında kişilerin cinsel dokunulmazlığına karşı işlenen suçlardır. İnternetin yapısı itibariyle kullanıcılar üzerinde hakim olan gizlilik ve anonimlik duygusu çoğu zaman gündelik yaşamda yansıtılmakta çekinilen ifadelerin ve davranışların daha rahat yansıtılmasına neden olmaktadır. Bunların başında da cinsel içerikli ifadeler yahut diğer materyaller gelmektedir. Artık dünyada internet üzerinden cinsel içerikli materyallere ulaşmak çok kolay olmakla birlikte bu konuda ciddi bir sektörün oluştuğu da bilinmektedir. Tabi ki konu sadece cinsel içerikli materyallerin dolaşımı ve bunlara erişimin rahatlığı değildir. Bunun yanında kişiler internet teknolojisinin verdiği imkanlardan faydalanmak suretiyle başka kişileri cinsel bütünlüklerini ihlal eder tarzda taciz etmektedirler. Bu anlamda 5237 sayılı TCK md. 105⁵⁰¹,de düzenlenen cinsel taciz suçunun da internet aracılığıyla

⁴⁹⁹ Aynı yönde değerlendirmeler için bkz. **CENDEL/ ZAFER/ ÇAKMUT**, Kişilere Karşı Suçlar, sh: 88.

⁵⁰⁰ 5237 sayılı TCK md. 44' de düzenlenen fikri içtima düzenlemesinin ayrıntıları için bkz. **İÇEL**, Ceza Hukuku, sh: 287 v.d.; **ÖZBEK**, İzmir Şerhi, sh: 520 v.d.; **ÖZGENÇ**, Ceza Hukuku, sh: 513 v.d.; **HAKERİ**, Ceza Hukuku, sh:231 v.d.; **YILDIZ**, Türk Ceza Hukuku; 126 v.d.; **ÖZTÜRK/ ERDEM**, Uygulamalı Ceza Hukuku, 244 v.d.; **YARSUVAT**, Duygun, Yeni Türk Ceza Kanunu Genel Hükümleri, Genel Değerlendirme, İlkeler ve Genel Kurallar, in: YÜHFD, C. II, S: 2, 2005, sh: 357 v.d.; **BAKICI**, Sedat, Ceza Hukuku Genel Hükümler, Ankara, 2007, sh: 914 v.d.; **ÖZEN**, Mustafa, Ceza Hukukunda Fikri İçtima, in: TBBD, S:73, Ankara, 2007, sh: 132 v.d.

⁵⁰¹ MADDE 105. - (1) Bir kimseyi cinsel amaçlı olarak taciz eden kişi hakkında, mağdurun şikâyeti üzerine, üç aydan iki yıla kadar hapis cezasına veya adli para cezasına hükmolunur.

işlenebileceği kuşkusuzdur⁵⁰². Özellikle e- posta yoluyla veya diğer kişisel iletişim (MSN, ICQ v.b.) kanalları kullanılmak suretiyle cinsel amaçlı rahatsızlık verici ifadeler kullanılabilir. Özellikle internetin, bir multimedya aracı olarak aynı anda hem görsel hem işitsel, hem yazıyla hem resimle bu suçta kullanılması mümkündür.

Suçun fail ve mağduru bakımından kanun koyucu herhangi özel bir belirlenime gitmemiş ve dolayısıyla cinsel taciz suçunun her erkek veya kadın tarafından işlenebileceğini kabul etmiştir. Bu anlamda suçun mağduru herkes olabilir. Kanunda “bir kimseyi cinsel amaçlı olarak taciz eden” denildiğinden, mağdur açısından da herhangi bir sınırlamaya gidilmemiştir. Bununla birlikte mağdur faille farklı cinsten olabileceği gibi aynı cinsten de olması mümkündür⁵⁰³. Özellikle internette kişilerin kimliklerini olabildiğince gizlemeye çalışmaları ve hangi cinsiyetten olduklarının anlaşılammaları karşında kanun koyucunun cinsel taciz suçlarında mağdur ve fail açısından cinsiyet temelli bir ayrıma gitmemesi normal karşılanmalıdır. Bunların yanında *Yargıtay* cinsel taciz suçunun oluşabilmesi için eylemin doğrudan doğruya mağdura karşı işlenmesi gerekliliğini aramaktadır.⁵⁰⁴

Anılan suç tipinin *tipe uygun eylem unsuruna* yönelik internet aracılığıyla işlenebilirliğini de kapsayacak şekilde bir değerlendirme yapmak gerekirse; md. 105/1’e göre cinsel taciz suçunun maddi unsuru bir kişiyi cinsel amaçlı olarak taciz etmektir. *Sevük*

(2) Bu fiiller, hiyerarşi veya hizmet ilişkisinden kaynaklanan nüfuz kötüye kullanılmak suretiyle ya da aynı işyerinde çalışmanın sağladığı kolaylıktan yararlanılarak işlendiği takdirde, yukarıdaki fıkraya göre verilecek ceza yarı oranında artırılır. Bu fiil nedeniyle mağdur; işi bırakmak, okuldan veya ailesinden ayrılmak zorunda kalmış ise verilecek ceza bir yıldan az olamaz.

⁵⁰² “ Söz konusu bu madde (cinsel taciz) 765 sayılı TCK’nin 421. maddesinde düzenlenen söz atma ile sarkıntılık suçlarını kapsar şekilde yeniden düzenlenmiştir. Madde gerekçesinde cinsel tacizin, kişinin vücut dokunulmazlığının ihlali niteliği taşıyan cinsel davranışlarla gerçekleştirilebileceği ve cinsel tacizin, cinsel yönden, ahlak temizliğine aykırı olarak mağdurun rahatsız edilmesi olduğu belirtilmiş ancak hangi tür hareket veya sözlerin bu madde kapsamında olduğu açıklanmamıştır. Ancak bir kişiye karşı şehvet duygusuyla ani ve sözle yapılan saldırılar ile belirli bir kimseye karşı işlenen ve o kişinin edep ve iffetine dokunan ani ve hareketler yönünden kesiklik gösteren edepsizce davranışlar bu kapsamda değerlendirilecektir.” **BAYDEMİR**, Erdal, Cinsel Dokunulmazlığa, Kişi Hürriyetine ve Genel Ahlakla Karşı Suçlar, Ankara, 2007, sh:720.

⁵⁰³ **ARTUK**, Mehmet Emin/ **GÖKCEN**, Ahmet/ **YENİDÜNYA**, Caner, Ceza Hukuku Özel Hükümler, Ankara, 2006, sh: 130.

⁵⁰⁴ 765 sayılı TCK’de, bugünün cinsel taciz suçuna karşılık gelen söz atma ve sarkıntılık suçuna ilişkin Yargıtay vermiş olduğu bir kararında şu ifadeleri kullanılmıştır: “ TCK’nun 421/2 maddesinde düzenlenen suçun oluşması için eylemin doğrudan mağdureye karşı işlenmiş bulunmasının gerekmesine; dosya içeriğinden sanığın mağdure Şerife ile arkadaş olma istediğini Nilgün’ü defalarca arayarak ona bildirdiği, sanığın mağdureye iletilmesini istediği sözlerin sövme ve hakareti de içermediği anlaşılma ile suçun unsurları itibarıyla oluşmadığı gözetilmeden yazılı şekilde mahkumiyetine karar verilmesi kanuna aykırı, sanığın temyiz itirazları bu itibarla yerinde görülmemiş olduğundan hükmün bozulmasına 30.04.2003 tarihinde karar verilmiştir.” Yargıtay 5. CD. 30.04.2003, E: 2003/4788 – K: 2003/2434; **MEYDAN**, Nihat/ **YAPAL**, Fadime, İçtihatlı Türk Ceza Kanunu, II. Cilt, İstanbul, 2004, sh: 1547’den naklen.

kanunun bu ifadesini gerekçesi ve ratio legisini de dikkate alarak biraz daha detaylı bir belirlenimle anılan suçun maddi unsurunu vücut dokunulmazlığı ihlali niteliği taşımayan bir başka deyişle cinsel saldırı boyutuna ulaşmayacak şekilde cinsel amaçlı davranışlarda bulunmak olarak ortaya koymaktadır⁵⁰⁵. Madde metni esas alındığında cinsel taciz bakımından net bir tanıma rastlanmamaktadır. Yine *Seviik* bu durumu şöyle ifade etmektedir⁵⁰⁶.

“TCK md. 105 maddenin gerekçesinde ise cinsel taciz kişinin vücut dokunulmazlığı ihlali niteliği taşımayan cinsel davranışlarla gerçekleştirilen ve cinsel yönden, ahlak temizliğine aykırı olarak mağdurun rahatsız edilmesi şeklinde tanımlandığından gerekçedeki hem “cinsel davranış” hem de “ahlak temizliğine aykırı” kavramları tartışmaya açıktır.”

Doktrinde cinsel tacize kavramına ilişkin çeşitli tanımlar yapılmıştır. Bunlara örnek olarak *Artuk* cinsel tacizi, birey veya bireylerin cinselliklerinde yönelik sözlü veya yazılı vücuda temas içermeyen rahatsız edici nitelikte cinsel amaçlı her türlü hareketler olarak tanımlamaktadır⁵⁰⁷. Temel şekli bakımından cinsel taciz teşkil eden davranışlar sözlü⁵⁰⁸, yazılı⁵⁰⁹, veya el kol işaretleriyle⁵¹⁰ gerçekleştirilebilir. Söz konusu davranışların fiili bir cinsel müdahale boyutuna ulaşmamış olması gerekmektedir⁵¹¹. Cinsel taciz niteliğindeki fiillerin mağdurun vücutuna temas etmek suretiyle gerçekleştirilmesi durumunda ise fail md.

⁵⁰⁵ **SEVÜK**, Handan Y., 5237 Sayılı Türk Ceza kanununda Cinsel Saldırı ve Cinsel Taciz Suçları, in: TBBB, S: 57, Ankara, 2005, sh: 273.

⁵⁰⁶ **SEVÜK**, Cinsel Saldırı ve Cinsel Taciz, sh: 273.

⁵⁰⁷ **ARTUK**, Mehmet Emin, Cinsel Taciz Suçu (TCK M. 105), in: HPD, S: 07, İstanbul, 2006, sh: 73.

⁵⁰⁸ Yargıtay’a göre sanığın mağdureye yönelik olarak “*bayan almaya geldim, istersen seninle de çıkabiliriz*” demesi (5. CD. 27.02.2002, E. 2001/ 2750 – K. 2002/ 100), “*10 milyon vereyim, bir şeyler yaparız niye anlamıyorsun*” demesi (5. CD. 30.01.2002, E. 2001/ 3348 – K. 2002/ 1046), “*gel birlikte ormana gidelim, koluna gireyim bol bol çocuğumuz olsun*” demesi (5. CD. 21.01.2002, E. 2002/ 866 – K. 2002/ 6357) sözlü olarak cinsel taciz kapsamına girmektedir. Emsal gösterilen kararlar için bkz. **BAYDEMİR**, Genel Ahlak Karşı Suçlar, sh: 729- 730

⁵⁰⁹ Yargıtay muhtelif zamanlarda verdiği kararlarda yazılı cinsel taciz eylemlerini sadece mektupla sınırlı tutmamış, örneğin cep telefonu mesajlarını da bu kapsamda değerlendirmiştir (5. CD. 01.03.2004, E. 2003/3400 – K. 2004/ 1294). **BAYDEMİR**, Genel Ahlak Karşı Suçlar, sh: 746.

⁵¹⁰ Yargıtay’ın da bu minvalde verdiği emsal karar örnekleri için bkz. **BAYDEMİR**, Genel Ahlak Karşı Suçlar, sh: 731.

⁵¹¹ **ÜZÜLMEZ**, İlhan, Cinsel Dokunulmazlığa Karşı Suçlar, <http://www.cezabb.adalet.gov.tr/makale/122.doc> (Erişim Tarihi: 10.12.2007, Saat: 16:44)

105'e göre değil cinsel saldırının düzenlendiği 102'e göre veya mağdurun yaşına göre md. 103 çocukların cinsel istismarına göre cezalandırılacaktır⁵¹².

TCK md. 105 anlamında cinsel tacizin yukarıda tanımlanan tipe uygun eylem unsuru çerçevesinde internet aracılığıyla sıklıkla işlenen bir suç tipi olduğu bilinmektedir. Çünkü internetin, isabetli olmamasına rağmen kanunun ifadesiyle “*ahlak temizliği*”nin kirletilmesine müsait bir ortam olduğu bilinmektedir. Özellikle internetin kullanıcılarına sunduğu gizlilik ve anonimlik⁵¹³ güvencesinin tespit edilebilmeyi engelleyen güvenceler olduğu zannıyla, sıklıkla sohbet odalarında, forumlarda veya e-posta ya da kişisel iletişim programları aracılığıyla gönderilen iletilerle cinsel taciz suçunun unsurlarının gerçekleşmesi mümkündür. **Ancak kanaatimizce madde gerekçesinde kullanılan “*ahlak temizliğine aykırı olarak*” ifadesinin özellikle internet aracılığıyla işlenebilen bir suç olması dolayısıyla cinsel taciz suçunda müstakbel genişlemelerin habercisi olduğu, bunun da tehlikeli neticeleri beraberinde getireceği açıktır⁵¹⁴.** Şöyle ki; yukarıda da ifade edildiği gibi internet kanun koyucunun kullandığı ifadeyle “*ahlak temizliğinin*” en rahat kirletilebildiği ortamların başında gelmektedir. Şayet ahlak temizliğine aykırılık gibi muğlak, göreceli bir kriter bir internet içeriğinin değerlendirmesinde kullanılacak olursa internet kullanımı ciddi anlamda engellenir. Çünkü daha önce de dile getirildiği üzere internet küresel bir ağdır ve burada küresel değerlerin hakim olduğu bir düzen yaratılmıştır⁵¹⁵.

⁵¹² Ayrıca *Toroslu*, bir kimsenin cinsel amaçlı olmayan bir biçimde taciz edilmesinin yerine göre 123. maddedeki “*kişileri huzur ve sükununu bozma*” veya 183. maddedeki “*gürültüye neden olma*” suçu oluşabilir. Bu değerlendirmenin detayları için bkz. **TOROSLU**, Ceza Hukuku Özel Hükümler, sh: 68 vd.

⁵¹³ *Anonimlik hakkı* bir kişi veya grubun görüş ve düşüncelerini kimliğini ortaya çıkarmadan açıklaması ve yayması anlamını taşımaktadır. Anonimlik hakkı ifade özgürlüğü ve özel hayatın gizliliği ve korunması hakkı ile çok yakından ilgilidir. Anonimlik hakkı ilk önce basın hukukunda düzenlenmiştir. Bu hakkın basın özgürlüğünün bir gereği olduğu kabul edilmektedir. Anonimlik hakkı basın hukukunda bir yazıyla yazarının imzalamaya mecbur tutulamaması ve bir dönemsel yayında imzasız, rumuzla veya takma adla yayımlanan bir yazının yazarı öğrenilmek üzere hiç kimseye baskı yapılamaması ve böylece bir sırrın muhafazasının bir sorumluluk veya sorumluluğu arttırıcı bir sebep olmaması şeklinde tanımlanmaktadır. İnternet üzerinde anonimlik hakkı ise siber uzay ortamında herhangi bir şekilde faaliyet gösteren kişi veya grupların, bu faaliyetlerini kimliklerini ortaya çıkarmadan anonim kalarak sürdürebilmeleri şeklinde oluşmaktadır. İnternet kullanımının hızlı gelişimi ve artışı, yeni iletişim ve tartışma olanaklarını da beraberinde getirmiştir. Kişiler internet üzerinde anonim kalarak iletişim kurabilme olanağı, yaşadıkları toplumda siyasi, sosyal, ahlaki ve benzer baskılardan kaçarak örgütlenmek isteyenler için önemli bir fırsat alanı yaratmıştır. Konu ile ilgili ayrıntılı bilgi için bkz. **YILDIZ**, Suçta Araç Olarak İnternet, sh: 198- 199.; **SÖZÜER**, Adem, Basın Suçlarında Ceza Sorumluluğu, İstanbul, 1996, sh: 74 v.d.; **SAYAR**, Hande/ **DALKILIÇ**, Mehmet E., İnternet'te Kişisel Bilgi Güvenliği İçin Anonimleştirici Servisler Üzerine Bir İnceleme, Kaynak: <http://ab.org.tr/ab05/tammetin/133.pdf> (Erişim Tarihi: 06.02.2008, Saat: 11:06)

⁵¹⁴ Bu konuya en önemli örnek A.B.D'de İletişim Ahlakı Kanunu'nu ile ilgili Federal Yüksek Mahkeme'nin verdiği iptal kararıdır. Bu konuda bkz. **YILDIZ**, Suçta Araç Olarak İnternet, sh: 115.

⁵¹⁵ Özellikle ceza hukuku boyutu açısından, internetin kültürel değerlerle küresel değerler arasındaki ilişkide sahip olduğu yere ilişkin değerlendirmeler için bkz. **HILGENDORF**, Yeni Medya, sh: 286 v.d.

“*Ahlaki temizlik*” gibi belli bir yaşayış tarzına ve belli bir kültürel alt yapıya dayanan, kültürden kültüre, kişiden kişiye değişiklik gösterecek bir kriterin böylesine küresel değerlerle çevrili bir düzlemde değerlendirme kriteri olarak alınması oldukça hatalıdır ve özgürlüğü gereğinden çok daha fazla sınırlayıcı niteliktedir. Bu anlamda yapılması gerekenin bu kriteri inceleme konusu madde anlam ve uygulama bütünlüğünden çıkartmak olduğunu düşünmekteyiz.

Anılan suçun *maneви unsur* açısından incelenmesinde görülmektedir ki, TCK md. 105 kapsamında cinsel taciz suçu düzenlenişi itibariyle kasten işlenebilen bir suçtur⁵¹⁶. Bunun ötesinde kanun koyucu madde hükmünde cinsel taciz fiilini gerçekleştiren failin, cinsel arzularını tatmin gayesi arandığından bu suçun ancak özel kast ile işlenebileceği kabul edilmektedir⁵¹⁷, yani failin “*cinsel amaçlı*” olarak hareket etmesi gerekir. Bu anlamda söz konusu suçun olası kastla işlenmesi mümkün görünmemektedir. Fail başka bir amaçla hareket etmiş ise, duruma göre hakaret (TCK md. 125)⁵¹⁸ ya da tehdit (TCK md. 106)⁵¹⁹ gibi suçlar oluşabilir. Bu değerlendirme suçun internet aracılığıyla da işlenebilen hali bakımından geçerlidir. Bunun dışında suçun internet ortamında işlenebilirliği bakımından kusurluluğu etkileyen özellikli bir duruma rastlanmamıştır.

Cinsel taciz suçu bakımından *hukuka aykırılık* unsuru üzerinde de durulmalıdır. Suç tipinin kişinin rızası hilafına yapılması gerekmektedir. Başka bir anlatımla kişi kendisine karşı icra edilen cinsel taciz içerikli davranışa karşı rıza göstermemelidir. Şayet rıza söz konusu olursa ortada hukuka aykırılıktan bahsedilemez⁵²⁰. Bu bağlamda bir husus sorun olarak kendini göstermektedir. İnternetteki profil veya paylaşım sitelerine bir takım fotoğraflarını yükleyen bir kişi, bu fotoğrafları dolayısıyla diğer internet kullanıcılarının cinsel taciz kabul

⁵¹⁶ SOYASLAN, Ceza Hukuku Özel Hükümler, sh: 200.

⁵¹⁷ TEZCAN/ ERDEM/ ÖNOK, Ceza Hukuku Özel Hükümler, sh: 256.

⁵¹⁸ “ *Sanığın olay günü kendisiyle birkaç kere karşılaştığı müştekiye “ anasını s.k. ettiğimin karısı ” demekten ibaret eyleminin edep ve iffete saldırı mahiyeti taşıması nedeniyle sarkıntuluk niteliğinde olmayıp müteselsil sövme niteliğinde gözetilmeyerek yazılı şekle cezalandırılması...*” Yargıtay 5. CD. 17. 06. 1996, E. 1996/ 1722 – 1996/ 2178). BAYDEMİR, Genel Ahlaka Karşı Suçlar, sh: 727.

⁵¹⁹ Örneğin failin mağdura karşı sinkaflı küfürler etmek suretiyle kendisinin cinsel bütünlüğü dışında örneğin malvarlığı veya vücut bütünlüğüne karşı zarar vereceğini kastetmesi durumunda her ne kadar ifade ediliş tarzı itibariyle cinsel taciz nitelikli bir eylem gibi görülse de tehdit kastıyla hareket ettiği için burada md. 106 kapsamında tehdidin ve md. 125 kapsamında hakaretin varlığı kabul edilmelidir.

⁵²⁰ TEZCAN/ ERDEM/ ÖNOK, Ceza Hukuku Özel Hükümler, sh:256; ARTUK/ GÖKCEN/ YENİDÜNYA, Ceza Hukuku Özel Hükümler, sh: 182.

edilebilecek davranışlarına maruz kalırsa ve buna rağmen yüklediği bu fotoğrafları ilgili profil veya paylaşım sitesinden çıkartmayacak olursa mağdur kendine uygulanan cinsel tacize rıza göstermiş kabul edilebilir mi? **Kanaatimizce bu durumda mağduru cinsel tacize rıza göstermiş kabul etmek mümkün değildir. Çünkü, her ne kadar kanun koyucu göreceli hale getirirse de, cinsel dokunulmazlık kişisel bütünlüğünün bir parçasıdır. Kişinin yaşam tarzı, ahlaki değer tercihleri ne olursa olsun kişisel bütünlüğüne dair tüm unsurlar mutlak suretle korunmalıdır. Ancak yasa koyucu cinsel tacizi, ahlaki temizliğe aykırı bir davranış olarak kabul ettiği için yukarıda mutlak güvence altına alınması gereken unsurlar göreceli hale gelebilecektir.** Çünkü kim için ve kime göre ahlaki temizliğin tespit edileceği muallâktır. Bir başka anlatımla somut olayda ahlaki temizliğin zedelendiği mülahazasına başvurulurken, uygulamaya temel teşkil eden ahlaki değer tercihinin nasıl somutlaştırılacağı problemlidir. Bu sorunun daha da sıkıntı vermesi muhtemel boyutu, internetin ulusal üstü kimliği dolayısıyla farklı kültürel ve ahlaki değer sisteminde yaşayan kişiler arasında cinsel taciz eylemlerinde kendini göstermektedir.

Bu çerçevede maddenin düzenleniş tarzı bakımından internet perspektifinden bir noktanın vurgulanmasını elzem görmekteyiz. Bu nokta cinsel taciz nitelikli eylemlerin alenen gerçekleştirilmesine yöneliktir. Şayet kanun koyucu madde gerekçesinde ahlaki temizliği koruma kaygısını ifade etmekteyse, mantıksal tutarlılık gereği bir takım ahlaki dengelerin de gözetilmesi gerekmektedir. Örneğin internet haberciliğinin gelişmesiyle birlikte kişiler hakkında verilen haberlere bir link eklenerek, o kişi ile ilgili haberle bağlantısı olsun veya olmasın bir takım resim veya görüntülere erişilebilmek mümkün hale gelmiştir. Bununla birlikte kullanıcılar söz konusu haberi aynı sayfa içinde yorumlayabilmektedirler. Yine bir takım paylaşım sitelerinde⁵²¹ veya forum sayfalarında bazı fotoğraf veya görüntüler aktarılmakta ve bu veriler yorumlanmaktadır. Bu yorumlar kimi zaman o sitenin menşei, yapısı ve işleyişine paralel olarak, olduğu gibi erişime açılmakta ve böylece kullanıcılar tarafından yüklenen içeriği itibarıyla, hakaret, tehdit, cinsel taciz niteliğindeki ifadeler herkes tarafından takip edilebilir hale gelmektedir. Şu halde bir kişiye cinsel taciz niteliğinde kullanılan bir ifadenin herkes tarafından bilinebilir olması daha ağır bir ahlaki temizlik ihlaline neden olmaktadır. Dolayısıyla kanun koyucunun bu konsepti inceleme konusu suçun alenen işlenmesini *nitelikli bir hal* olarak düzenlememesini bir tutarsızlık olarak görmekteyiz.

⁵²¹Günümüzde en popüler paylaşım sitelerinden biri youtube.com'dur.

Suçun özel görünüş şekillerinin internet açısından önem arz eden noktaları incelenecek olursa, suçun bir içerik suçu olması ve diğer içerik suçlarıyla bu anlamda benzerlik göstermesi nedeniyle gerek *teşebbüs*, gerek *iştirak* bakımından örneklendirmede tekrara girmemek için daha önce işlenen suç tiplerinde verilen konuya ilişkin değerlendirme ve örneklere atıf yapmakla yetinilecektir.

İçtima konusunda da zincirleme suç hükümlerinin uygulanabilirliği hususunda önceki açıklamalara atıfta bulunulurken sadece bir hususun altı çizilmelidir. Fail tarafından gerçekleştirilen davranışın bir taciz hükmünde kabul edilebilmesi için mağdur açısından söz konusu davranışın rahatsız edici derecesine varması aranmaktadır. Şu halde kısa aralıklarla aynı kişiye karşı gerçekleştirilen bu neviden eylemler açısından tek suç işleme kararının varlığı kabul edilebilir⁵²². Bunun dışında fikri içtima uygulanabilirliği üzerine birkaç örnek vermekte yarar vardır. Bilindiği gibi TCK md. 44 çerçevesinde bir kişi yapmış olduğu bir eylemle birden çok suçun işlenmesine sebebiyet verebilir. Buna en iyi örneklerden biri de cinsel taciz suçudur. Örneğin bir kişi cinsel taciz içerikli bir iletiyi bir başkasına gönderdiğinde ve bu iletide sarf edilen sözler cinsel taciz suçuna vücut verirken aynı zamanda hakaret veya iftira suçunun unsurlarını gerçekleşmesi durumunda burada fikri içtimadan bahsetmekte yara vardır. Özellikle bu suç tipi bakımından internet fikri içtima sebebiyet verecek durumların ortaya çıkmasında önemli bir araç olma özelliği taşınmaktadır⁵²³.

1.2.3.- Tehdit

⁵²² **BAYDEMİR**, Genel Ahlak Karşı Suçlar, sh: 746.

⁵²³ *Sözür*'in şu açılmasını internet açısından da kabul etmek yerinde olacaktır: “ Aynı yazıda tek bir beyanla kanunun farklı hükümlerinin ihlal edilmesi durumunda fikri içtima kurallarının uygulanması gerekmektedir. Örneğin “ hükümetin manevi şahsiyetini tahkir ve tezyif suçu”nu oluşturan bir yazı, aynı zamanda “ halkı hükümete silahlı ayaklanmaya tahrik suçunu” oluşturabilir. Ya da bir kişiyi tahkir eden beyan aynı zamanda müstehcen bir nitelik gösterebilir. Bu durumlarda, kanunun farklı hükümleriyle çelişen tek ve aynı fiilin bulunması koşulu gerçekleştiğinden, fikri içtima kuralları gereğince, faile en ağır cezayı içeren hükmün cezası verilir.” ; **SÖZÜER**, Basın Suçları, sh: 38.

5237 sayılı TCK md. 106⁵²⁴,da düzenlenen tehdit suçuyla kişinin, korku ve endişe duymadan, huzur içinde, emniyet duygusuyla yaşaması sağlanmak amaçlanmıştır. Suçun oluşması için fiilin, mağdurun güvenlik duygusunu, iç huzurunu etkileyici, onu endişeye, korkuya sevk etmeye elverişli olması yeterlidir. Mağdurun iç huzurunun bozulması, onun serbestçe karar vermesini veya verdiği kararlara göre hareket edebilmesini tehlikeye sokar. Bu bakımdan tehdit; mağdurun karar veya hareket hürriyetini tehlikeye koyan bir fiildir. Tehdit halinde mağdur tehdit konusu tecavüzün ileride gerçekleşeceği beyanıyla korkutularak belli bir davranışta bulunmaya zorlanmaktadır⁵²⁵.

Bu değerlendirmeye tehdit suçunun internet aracılığıyla işlenmesi mümkün ve hatta artık tercih edilebilir olduğu görülmektedir. Çünkü internetin gizlilik ve anonimlik internet kullanımında bir güvence olarak kabul görülürken aynı zamanda da diğer kullanıcılar bakımından ciddi bir tehlike olanağı sunmaktadır. Tehdit suçu açısından da internet ortamında tehdidi gerçekleştiren kişinin tespitindeki zorluk, kişinin daha çok korku yaşamasına ve daha kolay daha sık tehdit edilebilme endişesini taşımasına neden olmaktadır. Bu bakımdan tehdit suçu günümüzün en yaygın iletişim aracı olan internet tarafından kolaylıkla işlenebilir.

TCK md. 106'da düzenlenen tehdit suçunun hangi hukuksal değeri korumayı amaçladığı madde gerekçesinde açıkça aktarılmaktadır. Buna göre kanun koyucu tehdidin mağdura bir kötülükte bulunulacağı beyan edilerek kişinin iç huzuru ortadan kaldırılmaya

⁵²⁴ **MADDE 106.** - (1) Bir başkasını, kendisinin veya yakınının hayatına, vücut veya cinsel dokunulmazlığına yönelik bir saldırı gerçekleştireceğinden bahisle tehdit eden kişi, altı aydan iki yıla kadar hapis cezası ile cezalandırılır. Malvarlığı itibarıyla büyük bir zarara uğratacağından veya sair bir kötülük edeceğinden bahisle tehditte ise, mağdurun şikâyeti üzerine, altı aya kadar hapis veya adli para cezasına hükmolunur.

(2) Tehdidin;

a) Silâhla,

b) Kişinin kendisini tanınmayacak bir hâle koyması suretiyle, imzasız mektupla veya özel işaretlerle,

c) Birden fazla kişi tarafından birlikte,

d) Var olan veya var sayılan suç örgütlerinin oluşturdukları korkutucu güçten yararlanılarak,

İşlenmesi hâlinde, fail hakkında iki yıldan beş yıla kadar hapis cezasına hükmolunur.

(3) Tehdit amacıyla kasten öldürme, kasten yaralama veya malvarlığına zarar verme suçunun işlenmesi hâlinde, ayrıca bu suçlardan dolayı ceza verilir

⁵²⁵ Bu hususa Yargıtay yeni tarihli bir kararında yaklaşımını şöyle ifade etmektedir: “*Tehdit fiili, kişinin ruh dinginliğini bozan, iç huzurunu, bilinç ve irade özgürlüğünü ihlal eden bir olgudur. Fiilin mağdur üzerinde ciddi bir korku yaratabilmesi açısından sonuç almaya objektif olarak elverişli, yeterli ve uygun olması gerekir. Ayrıca tehdidin somut olayda muhatap üzerinde etkili olması şart değildir. Bu nedenle mağdurun korkup korkmadığının araştırılması gerekmez. Tehdit suçunun manevi ögesi genel kasttan ibaret olup suçun yasal tanımındaki unsurlarının bilerek ve istenerek işlenmesini ifade eder. Olayda tasarlamanın varlığı aranmadığı gibi, saikin de önemi yoktur.*” Yargıtay 4. CD., 24.09.2007, E. 2006/3183 – K. 2007/7194 (Kaynak: <http://www.adalet.org/cbckran.php?id=4957>, Erişim Tarihi: 30.01.2008)

yönelik bir suç olmasından dolayı öncelikle kişilerin huzur ve sükunun korumaya alındığını belirtmiştir. Zira *Tezcan / Erdem/ Önok* bu nedenle bu suçla korunmak istenen hukuksal değer bireyin iç huzuru hukuksal güvenlik duygusu olduğunu kabul etmektedirler. Buna paralel olarak gerekçenin devamında bu suçla korunmak istenen hukuksal değer kişinin karar verme ve hareket etme hürriyeti olduğu vurgulanmıştır⁵²⁶. **Şu halde kanun koyucunun korunması amaçlanan hukuksal değer konusunda gereksiz bir ayrıntıya girdiği ve bu suretle de kafa karışıklığına sebebiyet verebileceği görülmektedir. Çünkü aslında kişinin karar verme ve hareket etme özgürlüğünün sağlandığı bir ortamda içsel ve dışsal huzur ve sükuna evleviyetle ulaşmış olması gerekmektedir.** Bu anlamda gerekçede iki ayrı hukuksal değermiş gibi gösterilmesine rağmen her ikisi de birbirlerinin tamamlayıcısı ve hatta parçasıdır.

Suçun faili açısından herhangi bir özellik söz konusu değildir. Herkes bu suçun faili olabilir. Mağdurun belirli veya belirlenebilir bir veya birden fazla kişi olması gerekir. Şayet failin tehdit içerikli ifadeleri belirsiz bir kişi veya kitleye hitaben gerçekleştirilirse farklı bir suç tipinin gündeme gelmesi söz konusu olabilir (örneğin TCK md. 213)⁵²⁷. **Madde gerekçesinde mağdur bakımından sadece “belirlilik” açıkça vurgulanmasına rağmen kanaatimizce özellikle suçun internet aracılığıyla işlenebilirliği göz önünde bulundurularak belirlilik unsurunu kapsar nitelikte “belirlenebilirlik” ölçütünün kullanılması daha yerinde olurdu. Örneğin internet aracılığıyla gerçekleştirilen tehdit suçunda mağdurun ilk etapta kim olduğu bilinemeyebilir. Çünkü özellikle internet iletişiminde kimliği açıkça yansıtılmasından ziyade “nick name” denilen takma isim veya kullanıcı adı kullanılmaktadır.** Ancak teknik imkanlar bu kişinin kim olduğunun belirlenebilmesine olanak sağlamaktadır⁵²⁸. Bu bakımdan biz “belirliliğin” kimliksel belirlilik olarak anlaşılması gerektiğini kabul ediyoruz.

Doktrinde tehdidin yöneldiği kişinin tehdidi algılayabilecek ve anlayabilecek durumda olması da gerektiği ve bu nedenle algılama yeteneği olmayanlara karşı tehdit suçu işlenemeyeceği yönünde kanaatlere rastlanmaktadır. Bu görüş sahiplerine göre fiil, bu

⁵²⁶ **TEZCAN/ ERDEM/ ÖNOK**, Ceza Hukuku Özel Hükümler., sh: 264; aynı yönde **ÇINAR**, Ali Rıza, Tehdit Suçu, Ankara, 2002, sh: 51.

⁵²⁷ **ÇINAR**, Tehdit, sh: 59 v.d.

⁵²⁸ Özellikle ceza yargılaması sürecinde internet de dahil olmak üzere bilişim sistemleri aracılığıyla işlenen suçlarda kullanılan teknolojik yöntemler ile ilgili ayrıntılı bilgi için bkz. **ER**, Biyometrik Yöntemler sh: 28 v.d.; **RYSER**, Dominic, “Computer Forensics”, eine neue Herausforderung für Das Strafprozessrecht, in: Internet – Recht – Strafrecht, sh: 553 v.d.

kimsenin yakınlarını korku ve telaşa düşürmeye ve iç huzurlarını bozmaya elverişli ise onlara karşı tehdit suçu söz konusu olabilir⁵²⁹. Kanaatimizce bu yaklaşım yine madde gerekçesinde belirtilen çerçevede yerinde değildir. Çünkü madde gerekçesinde açıkça “*Objektif olarak ciddî bir mahiyet arz eden tehdidin somut olayda muhatabı üzerinde etkili olması şart değildir. Kişi, fail, objektif olarak ciddî bir mahiyet arz eden söz ve davranışlarla mağduru tehdit etmek istemiş olmasına rağmen; mağdur, bu söz ve davranışları ciddiye almamış olabilir. Bu durumda tehdit yine gerçekleşmiştir. Tehdidin gerçekleşip gerçekleşmemesi, muhatabı üzerinde etkili olup olmamasına bağlı tutulmamalıdır.*” denilmek suretiyle tehdit suçunun mağdurun algılayabilme yeteneğine bağlı olmadığı vurgulanmıştır.

Suçun tipik eylem unsuru internet açısından ele alınacak olursa; tehdit suçunun temel şekli (md. 106/1) bakımından bir kişinin internetin gerek kişisel iletişim araçları (e-posta, MSN, ICQ, ... v.b.) gerekse herkes tarafından kullanılabilen web sayfaları ve forumlar aracılığıyla bir başkasını, kendisinin veya yakınlarının yaşamına, vücut bütünlüğüne veya cinsel dokunulmazlığına yönelik bir saldırı gerçekleştireceğine veya malvarlığı itibariyle büyük bir zarara uğratacağından veya sair bir kötülük edeceğinden bahisle tehdit etmesi mümkündür. Bu çerçeveden de anlaşılacağı üzere tehditte bizzat mağdurun veya yakınlık duyduğu üçüncü kişinin sayılan hukuksal değerlere bir zarar verileceği veya başkaca bir kötülük yapılacağına bildirilmesi söz konusudur. Başka bir anlatımla tehdit gerçekleşmesi failin iradesine bağlı olarak gelecekte bir kötülüğün meydana geleceğini bildirmektir⁵³⁰. Yukarıda belirtilen kapsam içinde ceza hadleri bakımından suçun temel şekli itibariyle ikili bir ayrıma gidildiği dikkati çekmektedir. Birinci grupta yaşama, vücut bütünlüğe veya cinsel dokunulmazlığa yönelik bir saldırılar (altı aydan iki yıla kadar hapis cezası), ikinci grupta da malvarlığına karşı saldırılar ve sair kötülük yapma beyanları (mağdurun şikayetine bağlı olarak altı aya kadar hapis cezası veya adli para cezası) yer almaktadır.

Tehdit suçunda tehdidin ağırlığı konusunda kanun koyucu birinci grup olarak belirttiğimiz yaşama, vücut bütünlüğüne ve cinsel dokunulmazlığa karşı gerçekleştirileceği ifade edilen saldırılar bakımından herhangi bir ağırlık tercihinde bulunmamıştır. Buna göre

⁵²⁹ ÇINAR, Tehdit , sh:60

⁵³⁰ TEZCAN/ ERDEM/ ÖNOK, Ceza Hukuku Özel Hükümler, sh: 270 v.d.

normal şartlarda gerçekleştirilmesi mümkün görünen (Elverişlilik İlkesi)⁵³¹ bir tehdidin bu alan bakımından suça vücut vermek bakımından yeterli olduğu görülmektedir. Buna karşın ikinci grupta sayılan malvarlığı değerlerine karşı gerçekleştirileceği belirtilen saldırı bakımından büyük bir zarara sebebiyet verecek tarzda bir tehdidin söz konusu olması gerekmektedir⁵³². Uğratılacağı bildirilen zararın bir suç teşkil etmesi aranmamaktadır. Bu anlamda kanun koyucu sadece zararı esas almaktadır.

TCK md. 106/2 de tehdit suçunda ağırlaştırıcı nedenler düzenlenmiştir. Buna göre tehdit suçunun silahla, kişinin kendini tanınmayacak bir hale sokması suretiyle, imzasız mektupla veya özel işaretle, birden fazla kişi tarafından birlikte, var olan veya var sayılan suç örgütlerinin oluşturdukları korkutucu güçten yararlanarak işlenmesi durumunda ceza arttırılır. *Artuk/ Gökçen/ Yenidünya* tarafından md. 106/1'in ikinci cümlesinde yer alan ve mal varlığı değerlerine karşı zarar verme içerikli tehdidin birinci cümledeki düzenlemeye göre daha az bir cezaya tabi tutulması bu düzenlemenin bir cezanın azaltılmasını gerektiren bir hal olarak gösterilmektedir⁵³³.

Suçun nitelikli halleri bakımından özellikle md. 106/2-b ve d'nin ağırlıkla internet aracılığıyla gerçekleştirilen tehdit suçunda gerçekleşebileceğini söylemek mümkündür. Bunlar tek tek incelenecek olursa; md. 106/2-b'de tehdit suçunun kişinin kendisini tanınmayacak bir hale koyarak, imzasız mektupla veya özel işaretlerle işlenmesi düzenlemiştir. Tehdit suçu bakımından kişinin kendini tanınmayacak hale koymasıyla ilgili bir çerçeve çizilmemiştir ama Yargıtay kendini tanınmayacak hale koymanın bir görünüm biçimi olarak değerlendirilebilecek kılık değiştirmeyi yağma suçunda faile kolaylık sağlayacak, toplumda

⁵³¹ Yargıtay elverişlilik ilkesinden neyi anladığını kararlarında dile getirmiştir. Örneğin Yargıtay 4. CD, 28.11.1995, E: 1995/ 7288 – K: 1995/ 8054: “ bir tehlike suçu olan tehdidin ciddi olup olmadığı, tehdidi içeren sözlerin gerçekleşmesinin kaçınılmaz olup olmamasına göre değil, olduğu ortama göre ve tarafların bedensel ve ruhsal durumlarına göre tehdit edici sözlerin gerçekleşme olasılığı ve mağdurun iradesini etkileme derecesi ölçütleri içinde, önceden bir bir sayılması olanaksız etkenler gözetilerek ilk mahkemece gözetilecek olgusal bir sorundur”; **TEZCAN/ ERDEM/ ÖNOK**, Ceza Hukuku Özel Hükümler, sh: 268'den naklen. Aynı yönde bir karar için bkz. Yargıtay 2. CD, 09.10.2003, 9703/11923: “ taraflar arasındaki tartışma esnasında tehdit içeren sözlerin, muhatabı üzerinde ciddi bir şekilde korku ve endişe yaratacak uygunluklu elverişlilik ve yeterlilikte olup olmadığı tartışılmadan sırf tartışma sırasında söylendiği şeklindeki, yasal dayanaktan yoksun gerekçeyle ve ceza genel kurulunun da kararını yanlış değerlendirme sonucu beraat hükmü tesisi bozmayı gerektirmiştir.”; **ÜZÜLMEZ**, İlhan, Tehdit, Şantaj ve Cebir Kullanma Suçları, Ankara, 2007, sh: 88'den naklen.

⁵³² Maddenin birinci fıkrasında yapılan tanımda, tehdidin yöneldiği hukukî değere göre bir ayırım yapılmıştır. Buna göre, tehdidin, mağdurun kendisinin veya yakınının hayatına, vücut veya cinsel dokunulmazlığına yönelik bir saldırı gerçekleştireceğinden bahisle yapılması, söz konusu suçun temel şeklini oluşturmaktadır. Buna karşılık, tehdidin, mağduru malvarlığı itibarıyla büyük bir zarara uğratacağından veya sair bir kötülük edeceğinden bahisle yapılması ise, suçun temel şekline göre daha az cezayı gerektirmektedir. Ayrıca, bu suçtan dolayı soruşturma ve kovuşturma yapılması, mağdurun şikâyetine bağlı kılınmıştır. (Gerekçe)

⁵³³ **ARTUK/ GÖKÇEN/ YENİDÜNYA**, Ceza Hukuku Özel Hükümler, sh: 230.

yaygın bir tedirginlik oluşturacak, mağdurda korku yaratacak ve failin kimliğinin bilinmesini engelleyecek şekilde olması kaydıyla nitelikli hal saymıştır⁵³⁴. Bu belirlenim karşısında kişilerin internette “*nick name*” denilen takma isimlerle alınan posta adreslerden gönderilen postalarla, yine aynı şekilde sanal sohbetlerde ve forum sayfalarında kullanılan ve md. 106/1’de belirtilen maddi unsuru gerçekleştiren tehdit içeriklerinin de bu ağırlaştırıcı nedene vücut verdiği kabul edilmelidir. Kişinin kimliğini gizlemesi suretiyle gerçekleştireceği tehdit eylemlerinin internet aracılığıyla gerçekleştirilebilirliği hususunda bir takım teknik imkanlar da mevcuttur. Bu imkanlar en önemli örnek “*spoofing*” adı verilen gizleme ve aldatma yöntemidir⁵³⁵. Bu yöntemin esası sahte e- posta, e- postada bulunan gönderen kısmının veya herhangi başka bir kısmının değiştirilerek başkasından geliyormuş gibi gösterilmesidir. E-posta sisteminin bir zayıflığı olarak alıcı tarafında görüntülenmek üzere, e- postanın kimden geldiği kısmında sahte bir gönderen yazılması sağlanabilir. Bununla birlikte temel internet kimlik unsurlarını oluşturan IP ve e- posta adreslerinin gizlenmesi de mümkündür. IP ve/veya e-posta adreslerinin gizlenmesi suretiyle tehdit içerikli bir iletinin gönderilmesi söz konusu olduğunda, bu tehdidi gerçekleştiren failin kimliğinin tespitinin o an için mümkün olamaması durumunda md. 106/2-b hükmünün gerçekleştiği kabul edilmelidir.

Yine aynı hüküm çerçevesinde tehdidin imzasız mektupla işlenmesi de bir ağırlaştırıcı neden olarak düzenlenmiştir. Bilindiği gibi mektup kavramı ilk anlamında ele alınır ve başka yerde bulunan bir kimseyle haberleşmeyi sağlayan yazılı kâğıt şeklinde anlaşılırsa, fikri içeriğin mutlaka maddiyat kazanması zorunlu hale gelecektir. Buna karşılık mektup “*yazılı hale getirilmiş, yazıya geçirilmiş şey*” olarak ele alınırsa, bu durumda yazının yazıldığı şeye bakılmaksızın maksat ön plana geçecektir. Bu bakımdan bir e- posta ve benzeri elektronik iletiler de mektup kapsamında değerlendirilmelidir⁵³⁶. Ancak bir e- posta veya internet ortamında paylaşılan herhangi bir ileti ile gerçekleştirilen tehdit suçunun bu kapsamda değerlendirilebilmesi için mutlak suretle gönderenin gizlenmesi, muhatap tarafından söz konusu iletinin kimin tarafından gönderildiğini bilememesi gerekmektedir. Bu anlamda

⁵³⁴ Konuyla ilgili ayrıntılı değerlendirme için bkz. ÇINAR, Tehdit, sh: 130.

⁵³⁵ “*Spoofing*” yönteminin teknik ayrıntıları için bkz. CANBEK, Gürol/ SAĞIROĞLU, Şeref, Kötücül ve Casus Yazılımlar: Kapsamlı Bir Araştırma, in: GÜMMFD, Cilt:22/1, Ankara, 2007, sh:132; CANBEK/ SAĞIROĞLU, Bilgisayar Sistemlerine Karşı Yapılan Saldırımlar ve Türleri: Bir İnceleme, in: EÜFBED, Cilt: 23 (1-2), 2007, sh: 5 v.d.; AKGÜN, Fatma/ BULUŞ, Ercan/ ŞEN, Şenol, Bilgisayar Ağları Üzerinde İletilen Verilere Zarar Vermek İçin Kullanılan Önemli Teknikler ve Koruma Yollarının İncelenmesi, Kaynak: <http://ercanbulus.trakya.edu.tr/vavin/11%20ulusal%20kong%2068-BILGISAYAR%20AGLARI%20.pdf>, (Erişim Tarihi: 06.02.2007, Saat: 11:31)

⁵³⁶ ÜZÜLMEZ, İlhan, Yazışmaların İhlali Cürümü ve Bu Bağlamda Elektronik Postalara (e- Postalara) Yönelik Saldırımların Durumu, in: A.Ü.H.F.D., C: 53, 2004/1, sh: 152.

göndericiye ait herhangi bir isim, takma isim, e- posta adresi, IP adresi ve benzeri bir unsurun bulunması halinde söz konusu tehdidin imzasız mektupla işlendiği kabul edilemez. Burada imzasız mektuptan kastedilen, iletinin kime ait olduğunu ortaya koyan herhangi bir unsurun söz konusu olmamasıdır⁵³⁷. Ancak kim olduğu tespit edilememesine rağmen gönderene ait herhangi bir ibare mevcutsa burada artık imzasız mektuptan bahsedilemez ancak bu durumda şartları gerçekleşmişse kişinin kendini tanınamayacak bir hale getirmesi suretiyle tehditten bahsedilebilir⁵³⁸. Aynı yönde *Artuk/ Gökcen/ Yenidünya'a* göre de, uydurma imzalı mektup imzasız mektup sayılır. Nitelikli unsur tatbikinde dikkate alınması gereken husus; mağdurun ulaşan tehdidi havi mektubun içeriğinden failin kim olduğunu anlayamaması yahut onu kesin olarak teşhis etmesinin mümkün olmamasıdır. İmzasız mektubun kim tarafından gönderildiği mağdurla fail arasındaki ilişkiden veya kullanılan ifadelerden anlaşılıyorsa, mektup imzasız dahi olsa bu nitelikli hal uygulanmaz⁵³⁹.

Bunun yanında md. 106/ 2-d'de düzenlendiği üzere tehdidin var olan veya var sayılan suç örgütlerinin oluşturdukları korkutucu güçten yararlanılarak gerçekleştirilmesini içermektedir. Örneğin bir yasa dışı örgütün veya o örgütün liderinin adıyla bir posta adresi alıp, kişiye o örgütün üyesi olarak veya kendini o örgütün üyesiymiş gibi göstererek tehditte bulunduğu takdirde bu ağırlaştırıcı neden gerçekleşmiş olur. Örnekten de anlaşılacağı gibi şayet kişi aldığı e- posta adresiyle veya kullandığı takma isimle hem kendini tanınamayacak hale getirirse hem de bir örgütün korkutucu gücünden faydalanırsa, md. 106 tehdit suçu anlamında her iki ağırlaştırıcı neden de oluşmuş sayılır.

Suçun özel görünüm biçimleri internet açısından ele alınacak olursa; yine bir içerik suçu olması dolayısıyla *teşebbüs* ve *iştirak* konusunda daha önce yapılan tüm açıklamalar tehdit suçu içinde cari olmakla birlikte sadece iştirak konusunda suçun birden fazla kişi tarafından işlenmesinin suçun temel şeklinden daha ağır bir cezayı gerektirdiği vurgulanmalıdır. *İçtima* konusunda ise yine benzerlikler görülmekle birlikte suç tipinin yapısı

⁵³⁷ Yargıtay bir kararında tehdidin yapıldı imzasız mektubu anonim bir mektup olarak kabul etmiştir. Kararın ayrıntıları için bkz. Yargıtay 4. CD., 25.02.1991, E. 1991/425 – K. 1991/1149.

⁵³⁸ “*Müşteki S:A .nın orman kesim işini sanıktan alıp bşkasına vermesi nedeniyle tehdit ve hakaret içeren imzasız mektubun sanık tarafından yazıldığı, bu hususun müşteki tarafından öğrenilip hazırlık tahkikatı sırasında C. Başsavcılığına bildirmesine göre mektubun imzasız sayılmayacağı gözetilmeden...*” Yargıtay 10. CD., 07. 02, 2000, 8793/ 1183, **TARHAN**, Tehdit ve Hakaret Suçları, sh: 56 (dipnot: 42)’den naklen.

⁵³⁹ Görüşün ayrıntıları ve görüş ile ilgili Yargıtay uygulamaları için bkz. **ARTUK/ GÖKCEN/ YENİDÜNYA**, Ceza Hukuku Özel Hükümler, sh: 228.

itibariyle bazı farklılıklara rastlamak mümkündür. İnternet açısından tehdidin en çok karşılaşıacağı suç tipi şantaj olacaktır. Az sonra da üzerinde durulacağı üzere şantaj da bir tehdit içermektedir. Ancak teknik anlamda tehdit suçundan farklı bir kapsam sahiptir. Bu yüzden bir bileşik suçtan söz edilir. Buna karşılık tehdit suçu yanında bileşik suç ilişkisi içine girmeyen bir başka suç da gerçekleşmişse gerçek içtima kuralları uygulanacaktır. Ancak tek fiille birden farklı suçun oluşması durumunda fikri içtima söz konusu olacağı için aynı sözleşme gelimi hem tehdit hem de hakaret suçunun işlenmesi durumunda en ağır cezayı gerektiren suçtan dolayı failin cezalandırılması yoluna gidilir. Buna karşılık tehdit ve hakaret suçu ayrı ayrı sözlerle gerçekleştirilmişse iki ayrı suç söz konusudur⁵⁴⁰.

Öte yandan tehdit suçu zincirleme biçimde de işlenebilir. Mağdurların değişmesi, aynı suç işleme kararının varlığını tek başına ortandan kaldırmaz ise de TCK md. 43'ün açıklığı gereği ancak aynı mağdura yönelik birden çok müteakip tehdit zincirleme suç kapsamında sayılabilecektir. Buna karşılık, aynı iletiyle aynı anda birden fazla kişi tehdit edilmişse, TCK md. 43/2 gereği zincirleme suçtan söz edilir.⁵⁴¹

1.2.4.- Şantaj

5237 sayılı TCK md. 107⁵⁴²,de düzenlenen şantaj suçu son zamanlarda internet ortamında en çok işlenen suçlardan birini teşkil etmektedir. Daha önce de ayrıntısıyla aktarıldığı üzere internet, teknik olarak, TCP/IP protokolü ile desteklenen pek çok servis sunar. Örnek olarak, internet erişimi olan bir kullanıcı, eğer kendisine yetki verilmişse, internete bağlı diğer herhangi bir bilgisayardaki bilgilere erişebilir, onları kendi bilgisayarına alabilir, kendi bilgisayarından da internet erişimi olan başka bir bilgisayara dosya/bilgi

⁵⁴⁰ Yargıtay CGK, 14.06.1971, 2- 181/ 223: “*Direnme kararında, küll halinde aynı anda söylenmiş sözlerde kasıt birliği bulunduğu ve fevren söylenen sözlerde tehdit suçunun unsurları bulunmadığı belirtilerek sanığın dava konusu konuşmasında tek kasıt ve tek suç niteliği görülmüştür. Ancak dosyadaki delillerden açıkça anlaşıldığı üzere dava konusu hakaret ve tehdit aynı sözlerle değil, ayrı ayrı sözlerle işlenmiştir. Sanık belediye parkında rastladığı öğretmen arkadaşına yaklaşarak arada herhangi bir tartışma ve çekişme bulunmadığı halde, hakkındaki sütozu yolsuzluğu ihbarını onun yaptığı kanısı ile namussuz, şerefsiz adam beni şikayet ettin diyerek yüzüne karşı bir hareketle bulduktan sonra, sözlerine devamla sana yapacağımı biliyorum, adım adım takip ediyorum. Sözleriyle adı geçeni tehdit etmiştir. Bu sözlerin aynı zamanda ve arka arkaya söylenmesi, ayrı suç teşkil etmesine engel değildir.*”; ÇINAR, Tehdit, sh: 164'den naklen

⁵⁴¹ ARTUK, , sh: 74-75.

⁵⁴² **MADDE 107.** - (1) Hakkı olan veya yükümlü olduğu bir şeyi yapacağından veya yapmayacağından bahisle, bir kimseyi kanuna aykırı veya yükümlü olmadığı bir şeyi yapmaya veya yapmamaya ya da haksız çıkar sağlamaya zorlayan kişi, bir yıldan üç yıla kadar hapis ve beşbin güne kadar adli para cezası ile cezalandırılır. (2) Kendisine veya başkasına yarar sağlamak maksadıyla bir kişinin şeref ve saygınlığına zarar verecek nitelikteki hususların açıklanacağı veya isnat edileceği tehdidinde bulunulması halinde de birinci fıkraya göre cezaya hükmolunur.

gönderebilir⁵⁴³. Ancak çoğu zaman internetin bu imkanı kişileri mahrem alanlarındaki gizli kalması gereken unsurların elde edilmesi ve daha sonra herhangi bir menfaat temini kullanıma da sebebiyet vermektedir. Günümüzde bu tarz suç teşkil edecek hareketlere en önemli örnek şantajdır. Hürriyet aleyhine işlenen bir suç olarak şantaj suçunda, hakkı olan veya yükümlülüğü olduğu bir şeyi yapacağı veya yapmayacağından bahisle ya da kişinin şeref ve saygınlığına zarar verebilecek bir hususun açıklanacağı veya isnad edileceğinden söz ederek mağdur belli bir yönde hareket etmeye zorlanmaktadır.⁵⁴⁴

Şantaj suçu internet açısından değerlendirilirken korunması amaçlanan hukuksal değer ve fail – mağdur unsurları bakımından özellikli bir duruma rastlanmamıştır. *Suçun tipe uygun eylem unsuru* bakımından ise yapılacak bir değerlendirmede şunları ifade etmek mümkündür ki, teknik anlamda md. 107/1’de düzenlenen şantaj nitelik itibarıyla md. 106’da düzenlenen tehdit suçuyla ve md. 148’de düzenlenen yağma suçuyla oldukça benzer niteliklere sahiptir. Buna göre şantaj, bir kişinin hakkı olan veya yükümlü olduğu bir şeyi yapacağından veya yapmayacağından bahisle, bir kimseyi kanuna aykırı veya yükümlü olmadığı bir şeyi yapmaya veya yapmamaya ya da haksız çıkar sağlamaya zorlamasıdır⁵⁴⁵. Bu anlamda şantaj suçunda da bir tehdidin varlığı görülmektedir. Başka bir ifade ile şantaj suçunda da kişiyi bir şeyi yapmaya veya yapmamaya zorlama söz konusudur⁵⁴⁶. Madde gerekçesinde de açık olarak vurgulandığı üzere bu durumda tehdit suçunda söz konusu olduğu gibi kişinin veya yakınının vücut veya cinsel dokunulmazlığına saldırıda bulunulacağı veya bir mal varlığı değerine büyük zarar verileceğinden bir zorlama söz konusu değildir. Aksine, kişi, hakkı olan veya yükümlü olduğu bir şeyi yapacağından veya yapmayacağından bahisle başkasını zorlamaktadır. Bu zorlamanın karşılığı mağdurun bir şeyi yapıp yapmaması veya

⁵⁴³ TCP/IP protokolü ve uygulamaları hakkında ayrıntılı bilgi için bkz. **ÇÖLKESEN**, Rifat/ **ÖRENCİK**, Bülent, Bilgisayar Haberleşmesi ve Ağ Teknolojileri, İstanbul, 2003, sh:121. v.d.

⁵⁴⁴ Bu konuda bkz. **YILDIZ**, Türk Ceza Kanunu, sh: 232-233; **SOYASLAN**, Ceza Hukuku Özel Hükümler, sh: 215; **ÜZÜLMEZ**, Tehdit, Şantaj ve Cebir Kullanma, sh: 141 v.d.

⁵⁴⁵ Yargıtay bir kararında şantaj ile yağma arasındaki farkı şöyle ifade etmiştir. “Yağma suçunun ögesi olan tehdidin, mağdurun kendisinin veya yakınlarının yaşamına, vücut veya cinsel dokunulmazlığına yönelik bir saldırı gerçekleştirileceğinden ya da malvarlığı yönünden büyük bir zarara uğratılacağından bahisle yapılması gerekir. Somut olayda, sanıkların ticaretle uğraşan katılanı, “vergi kaçırıldığını, maliye ile sorunları olduğunu, kendilerine 50.000.000.000 lira verilmediği takdirde, ellerindeki bazı belgeleri Maliyeye vereceklerini” söyleyerek şantaj yaptıklarının anlaşılması karşısında eylemlerine uyan 765 sayılı TCK’nun 192/1-2, 59/2. maddelerine göre hükümden sonra 1.6.2005 tarihinde yürürlüğe giren 5237 sayılı TCK’nun aynı suçu uyan 107/1-2, 62/1. maddelerinde öngörülen özgürlüğü bağlayıcı cezanın alt ve üst sınırları bakımından, anılan Yasanın 7/2, 5252 sayılı Yasanın 9/3. maddeleri ışığında sanıklar yararına olması ve 5237 sayılı Yasa hükümleri uyarınca yeniden değerlendirme ve uygulama yapılmasında zorunluluk bulunması bozmayı gerektirmiştir.” Yargıtay 6. CD., 13.03.2006, E. 2004/ 1975 – K. 2006/ 2445.

⁵⁴⁶ Şantaj ile tehdit arasındaki ilişki üzerine değerlendirme için bkz. **ARTUK/GÖKCEN/ YENİDÜNYA**, Ceza Hukuku Özel Hükümler, sh: 202- 203.

failin bir haksız kazanç elde etmesidir⁵⁴⁷. Çınar'a göre ise, tehdit ve şantaj suçlarının ortak paydaları tehdit ile işleniyor olmalarıdır. Ancak tehdit ve şantaj suçları tehdidin nedeni ve konusu bakımından farklılık göstermektedir⁵⁴⁸. Bu bağlamda tehdit suçunda “amaç – tehdit” söz konusu iken, şantaj suçlarında ise “araç – tehdit” söz konusudur⁵⁴⁹.

Özellikle internette e- posta, MSN, ICQ gibi kişiler arası iletişimde (teknik açıdan bu iletişimin görüntülü ve sesli yapılması da mümkündür) paylaşılan mahremiyetlerin veya herhangi bir yolla elde edilmiş ve kamusal paylaşımı ilgilisi tarafından kabul edilemeyecek olan görüntü, bilgi ve/veya belgenin ifşa edileceği tehdidiyle haksız çıkar elde etme yani şantaj eylemlerinin artış göstermesiyle kanun koyucu 29.06.2005 tarih ve 5377 sayılı kanunla anılan maddeye ikinci bir fıkra eklemiştir⁵⁵⁰. Bu fıkraya göre kendisine veya başkasına yarar sağlamak amacıyla bir kişinin şeref veya saygınlığına zarar verecek nitelikteki hususların açıklanacağı veya isnat edileceği tehdidinde bulunulması halinde yukarıda açıklanan birinci madde hükmüne göre cezalandırılacaktır⁵⁵¹.

Maddenin ikinci fıkrasında düzenlenen şantaj esasında birinci fıkranın tamamlayıcısı bir görünümü yansıtmaktadır⁵⁵². Suçun oluşumu şeref veya saygınlığa zarar verebilecek bir hususun açıklanacağı veya isnat edileceği tehdidinin varlığını ve bunun mağdurun iradesinin zorlamaya elverişli olmasını gerektirmektedir⁵⁵³. Buna örnek olarak bir kişinin belli bir çıkarın sağlanmaması durumunda muhatap ile ilgili elinde bulunan ve gizli veya rıza ile

⁵⁴⁷ Benzer değerlendirmeler için bkz. ÜZÜLMEZ, Tehdit, Şantaj ve Cebir Kullanma, sh: 145.

⁵⁴⁸ “ Sanığın yakınına” benimle olmazsam önceki ilişkilerini eşine söylerim” demesi biçimindeki eylemin 765 sayılı TCK md. 192 (5237 sayılı TCK md. 107) kapsamında düzenlenen şantaj suçunu oluşturduğu gözetilmeden tehdit suçundan karar verilmesi yasaya aykırıdır.” Yargıtay 4. CD. 06.03.2007, 13082/ 2180. TARHAN, Tehdit ve Hakaret Suçları, sh: 175’den naklen.

⁵⁴⁹ ÇINAR, Tehdit, sh: 175.

⁵⁵⁰ Bu konuda basına da yansıyan bir örnek vermek gerekirse, “Samsun’da, lise öğrencisi 17 yaşındaki D.A.’ya tehdit ve şantajla ilişkiye zorladıkları öne sürülen 2’si üniversite öğrencisi 3 kişi gözaltına alındı. Mahkeye çıkarılan zanlılardan üniversite öğrencileri 2 bin YTL kefaletle serbest bırakılırken, diğeri tutuklanarak cezaevine gönderildi.Lise öğrencisi D.A. ile 28 yaşındaki Bekir K., 1.5 yıl önce internetten tanıştı. İddialara göre bir süre gönül ilişkisi olan gençler, 5 ay önce ayrıldı. Ancak Bekir K., genç kıza, çıplak çekilen fotoğraflarını internete vermekle tehdit edip cinsel ilişkiye girmeye zorladı. İddiaya göre, Bekir K. ve üniversite öğrencisi olan arkadaşları ikisi de 22 yaşındaki U.G. ve F.A., genç kızla zorla ilişkiye girdi. D.A., polise giderek 3 kişinin kendisine şantaj yaparak tecavüz ettiğini belirtip şikayetçi oldu.” (Kaynak: <http://www.milliyet.com.tr/2008/01/07/son/sontur50.asp?prm=152678454>, Erişim Tarihi: 10.01.2008)

⁵⁵¹ YILDIZ, Türk Ceza Kanunu, sh: 233.

⁵⁵² SOYASLAN, Ceza Hukuku Özel Hükümler, sh: 216.

⁵⁵³ ÜZÜLMEZ, Tehdit, Şantaj ve Cebir Kullanma, sh: 148.

çekilmiş, özel kalması amaçlanan bir görüntü veya resimlerin internette paylaşım sitelerine yüklenmesi gösterilebilir. Ayrıca internet üzerinden tanıştıkları kişilere randevu veren, daha sonra buluşma noktasına gelen kişileri zorla alıkoyup cinsel tacizde bulunan bir kişinin, bunu da kamera ile görüntüleyip bunları internette yayınlayacağını söylemesi bu suça verilebilecek örneklerdir⁵⁵⁴.

Özellikle ikinci fıkranın eklenmesi, şantajla tehdit arasındaki çizginin md. 106/1'deki "sair kötülük" nitelemesinin geniş anlamı dolayısıyla ortadan kalkacağı ve söz konusu ihtimalde daha az cezaya karar verilebileceği eleştirisine paralel olarak gerçekleşmiştir. Özellikle de internet ortamında işlenen bu eylemlerin yarattığı etki göz ardı edilemez. Çünkü bilindiği gibi internet diğer kitle iletişim araçlarına nazaran kontrol ve denetleme imkanları daha az ve hatta imkansız bir araçtır. Şu halde diğer kitle iletişim araçlarına oranla her türlü içeriği veya veriyi herkesin dilediği şekilde ifşa etmesi, kamusal erişilebilirliğinin mümkün kılınması daha çabuk ve daha az maliyetlidir. Bu nedenle internet şantaj suç tipi özelinde düşünülecek olursa çok önemli bir suç alanıdır. Yasa koyucular da bu gerçeği her geçen gün daha da net bir biçimde görmekte ve bu gerçeğe uyumlu yasal düzenlemeler yapma ihtiyacı hissetmektedirler. Keza bu yaklaşımın bir görüntüsü de md. 107/2'ye ilişkin madde gerekçesinde şöyle anlam kazanmıştır:

" Kişinin yarar sağlamak maksadıyla başkasının şeref veya saygınlığına zarar verecek nitelikteki hususları açıklayacağı veya isnat edeceği tehdidinde bulunması halinde tehdit suçuna ilişkin "sair kötülük" kapsamında değerlendirilmesinin daha az cezayı gerektireceği eleştirisi karşısında madde metnin söz konusu fıkra eklenmiştir."

Tarafımızca da isabetli bulunan bu düzenlemenin bir takım eksikleri vardır. Kanaatimizce, fıkra oluşturulurken tehdit suçundaki düzenlemeye paralel olarak "Kendisine veya başkasına yarar sağlamak maksadıyla bir kişinin **veya yakınının** şeref ve saygınlığına zarar verecek nitelikteki hususların açıklanacağı veya isnat edileceği tehdidinde bulunulması halinde..." şeklinde bir düzenlemenin daha amaca uygun olacaktır. Çünkü madde metninin hali hazırdaki durumu itibarıyla, " kişinin şeref ve saygınlığı " ifadesi çok geniş bir anlam içeriğine sahip olmakla birlikte bir takım karışıklıklara neden olabilecek bir görünüm

⁵⁵⁴ Yargıtay, sanığın mağdura ait çıplak resimleri ilan edeceğini söyleyerek yarar temin etmesi (Yargıtay 6. CD., 29.01.1993, 416/ 519), oto içinde çıplak olarak sevişenleri gören sanığın anne – babanıza duyururum diyerek menfaat temin etmesi (Yargıtay 6. CD., 11.03.1992, 466/ 2064) eylemlerini şantaj kapsamında değerlendirmiştir. Bkz. SOYASLAN, Ceza Hukuku Özel Hükümler, sh: 217.

kazanmaktadır. Bu karışıklıkların en önemlisi kişinin şeref ve saygınlığının neyi kapsayıp kapsamadığı sorunudur. Örneğin gizli kamerayla kendi görüntüleri alınan bir kişinin, belli bir miktar para vermezse bu görüntülerin internette paylaşılacağı tehdidiyle karşılaşması durumunda fıkra hükmünün devreye gireceğinden şüphe yoktur. Ancak bu görüntüler bizzat o kişi ile ilgili olmamakla birlikte bir yakınının, örneğin çocuğunun, eşinin, kardeşinin, şeref ve saygınlığını zedeleyecek olursa nasıl düşünmek gerekecektir? Bu durumda bizzat şantaj fiiline maruz kalmış kişinin şeref ve saygınlığının bahsi geçen kişilerin şeref ve saygınlığına kapsayacak şekilde geniş düşünülmesi mümkün değildir. Dolayısıyla bu fıkra hükmünü sadece “*kişinin şeref ve saygınlığı*” yerine “*kişinin veya bir yakınının şeref ve saygınlığı*” demek suretiyle daha belirgin hale getirmekte fayda vardır.

Bunun dışında suçun *manevi unsuru ve suçun özel görünüş şekilleri* bakımından tehdit suçuna atıf yapmakla yetinilecektir.

1.2.5.- Hakaret

5237 sayılı TCK md. 125⁵⁵⁵,de düzenlenen hakaret suçu internet aracılığıyla işlenen suçlar arasında en çok rastlanılanların başında gelmektedir. Çünkü internet kullanımında anonimlik düşüncesi, suç takibinin sınırlı ölçülerde yapılabilmesi⁵⁵⁶ ve kontrol – denetleme

⁵⁵⁵ **MADDE 125.** - (1) Bir kimseye onur, şeref ve saygınlığını rencide edebilecek nitelikte somut bir fiil veya olgu isnat eden ya da yakıştırmalarda bulunmak veya sövmek suretiyle bir kimsenin onur, şeref ve saygınlığına saldıran kişi, üç aydan iki yıla kadar hapis veya adli para cezası ile cezalandırılır. Mağdurun gıyabında hakaretin cezalandırılabilmesi için fiilin en az üç kişiyle ihtilâl ederek işlenmesi gerekir.

(2) Fiilin, mağduru muhatap alan sesli, yazılı veya görüntülü bir iletiyle işlenmesi hâlinde, yukarıdaki fıkrada belirtilen cezaya hükmolunur.

(3) Hakaret suçunun;

a) Kamu görevlisine karşı görevinden dolayı,

b) Dinî, siyasi, sosyal, felsefi inanç, düşünce ve kanaatlerini açıklamasından, değiştirmesinden, yaymaya çalışmasından, mensup olduğu dinin emir ve yasaklarına uygun davranmasından dolayı,

c) Kişinin mensup bulunduğu dine göre kutsal sayılan değerlerden bahisle,

İşlenmesi hâlinde, cezanın alt sınırı bir yıldan az olamaz.

(4) Hakaretin alenen işlenmesi hâlinde ceza altıda biri oranında arttırılır.

(5) Kurul hâlinde çalışan kamu görevlilerine görevlerinden dolayı hakaret edilmesi hâlinde suç, kurulu oluşturan üyelere karşı işlenmiş sayılır. Ancak bu durumda zincirleme suçla ilişkin madde hükümleri uygulanır.

⁵⁵⁶ Yargıtay da özellikle internet aracılığıyla işlenen suçların takibi bakımından hayati önem taşıyan IP adreslerinin tespiti ve ilgili bilgisayarın hangi bağlamda kullanıldığı kriterleri üzerinden verdiği kararda bu noktaya dikkat çekmiştir. “*Yerel Mahkemece verilen hüküm temyiz edilmekle, başvurunun nitelik, ceza türü, süresi ve suç tarihine göre dosya görüşüldü: Temyiz isteğinin reddi nedenleri bulunmadığından işin esasına geçildi. Vicdani kanunun oluştuğu duruşma sürecini yansıtan tutanaklar, belgeler ve gerekçe içeriğine göre yapılan incelemede başkaca nedenler yerinde görülmemiştir. Ancak; sanığın kendisine zayıf not veren öğretim görevlisi, mağdur ile birkaç kişiye gönderdiği "e-posta" iletişimiyle mağdura sövmekten ibaret eyleminde; Sözü edilen iletiyi internet servis sağlayıcısından gönderen bilgisayarın (İ.P) numarasının sorulması, bu yolla*

mekanizmalarının yetersizliği nedeniyle insanlar bu sanal ortamda diledikleri gibi hareket etme cesaretini bulmaktadırlar. Özellikle günümüzde oldukça yaygın olan veri paylaşım siteleri, tartışma ve haber grupları ve forumlar incelendiğinde kullanıcıların birbirlerine karşı suç teşkil edecek ifadeleri rahatlıkla kullandıkları sıklıkla görülmektedir.

5237 sayılı TCK md. 125'de düzenlenen hakaret suçu internet açısından değerlendirilecek olursa; Öncelikle birinci fıkra hakaret suçunun maddi unsur üzerinde durmak gerekmektedir. Hakaret suçunun *maddi unsuru* bakımından iki hal öngörülmüştür. Bunlardan birincisi bir kimseye onur, şeref ve saygınlığını rencide edecek şekilde somut bir fiil veya olgu isnat etmektir⁵⁵⁷. İkinci hal ise sövmek suretiyle bir kişinin onur şeref ve saygınlığına saldırmaktır⁵⁵⁸. Her iki halin de internet aracılığıyla gerçekleşmesi mümkündür.

Bu bağlamda hakaret teşkil edecek eylemlerin gerçekleştirilme tarzına göre internet aracılığıyla işlenen hakaret suçunun huzurda hakaret mi yoksa gıyapta hakaret mi sayılacağı konusu da önem arz etmektedir. Bu noktada konuyu ikiye ayırmakta fayda vardır. Birincisi hakaret içeriğinin yönlendirildiği hedefin doğrudan mağdur olduğu durum ikincisi de hakaret içeriğinin doğrudan mağdura değil üçüncü kişilere yönlendirildiği durumdur. Her iki duruma kanun koyucu madde gerekçesinde bir açıklık getirmiştir. Buna göre birinci durumla ilgili olarak madde gerekçesinde “*Maddenin ikinci fıkrasında, hakaretin mağduru muhatap alan sesli, yazılı veya görüntülü bir mesajla yapılması hâlinde, birinci fıkra hükmüne istinaden cezaya hükmedileceği kabul edilmiştir. Buna göre, kişiyi muhatap alan mektup, telgraf, telefon ve benzeri araçlarla yapılan hakaret de, huzurda hakaret olarak cezalandırılmalıdır.*” denmektedir. Bu değerlendirmeden kanun koyucu hakaretin huzurda işlendiği kabulünde araç bakımından sınırlı bir sayım yapmadığı ve mektup, telefon, telgraf ve benzeri araçlar demek

bilgisayarın kime ait olduğunun saptanması sonucuna göre; 1- İnternet kafe gibi umuma açık yerlerde bulunan bir bilgisayardan ileti gönderilmiş ise sanığın beraatine, 2- Sanığın evi ya da işyerinde bulunan kişisel bilgisayarından gönderilmiş ise mahkumiyetine, 3- Olayla ilgisi bulunmayan bir üçüncü kişinin kişisel bilgisayarından gönderilmiş ise, bu şahsın tanık olarak dinlenmesi ve sonucuna göre karar verilmesi gerekirken, eksik soruşturma sonucu yazılı biçimde hüküm kurulması, yasaya aykırı ve O yer C.Savcısının temyiz nedenleri ile tebliğnamedeki düşünce yerinde görüldüğünden HÜKMÜN BOZULMASINA oy birliği ile karar verilmiştir.” Yargıtay 4. CD., 05.12.2005, E. 2004/ 8763 – K. 2005/21445 (Kazancı İçtihat Programı - Offline).

⁵⁵⁷ “ *Sanığın yakınana gönderdiği mektuptaki “ sen Halil’in altına yattın ve Özcan’ın altına yattın, Necip’in altına yattın” ifadelerinin belli bir olay yüklem niteliğinde olduğu gözetilmeden...*” Yargıtay 4. CD. 22.o4.2003, E. 18689 – K. 2769. ÇETİN, Erol, Yeni Türk Ceza Yasasındaki Hakaret Suçları, 2. Baskı, Ankara, 2007, h: 72’den naklen.

⁵⁵⁸ “ *Bir kimseye mahsus bir fiil isnat etmeksizin, onun şeref ve itibarını lekeleyici bir söz söyleyen veya yazı yazan kimse bir hak kullandığını iddia edemez. Çünkü kimsenin böyle bir hakkı bulunamaz. Hatta fail hem mahsus bir madde isnat etmek suretiyle hakaret hem de ayrıca sövme suçunu işlese ve olayda bir hukuka uygunluk sebebi bulursa, bu sebep hakaretin suç teşkil etmesini engellersen de, sövmenin varlığına hâlel vermez ve failin sövmeden dolayı cezalandırılması gerekli olur.*” Yargıtay CGK, 24.02.2998, E. 1997/4- 386 – K. 1997/ 72.

suretiyle interneti de bu kapsamda ele aldığı anlaşılmaktadır⁵⁵⁹. Hatta yukarıda sayılan araçlar dikkate alındığında ilk bakışta internet teknolojisi “benzeri araçlar” kategorisinde ele alınması gerekebileceği düşünülmesine rağmen esasında mektup ile aynı kategorideki e-posta ve benzeri iletiler, telefon ile kastedilen sesli iletişim imkanı sağlayan ve internet ortamında kullanılan kişisel iletişim programları internetin bu araçlar arsında açıkça sayılmasını zorunlu kılmaktadır. Kanun koyucunun bu noktayı atlamayarak interneti de açıkça huzurda hakaretin işlendiği araçlar arsında sayması gerekmektedir.

İkinci durum ile ilgili olarak da şayet hakaret, mağdurun hazır olmadığı bir ortamda veya doğrudan muttali olamayacağı bir surette üç kişiyle ihtilat edilerek işlenmişse bu durumda gıyapta gerçekleşmiş sayılır⁵⁶⁰. Örneğin fail, mağduru hedef aldığı hakaret içerikli bir e-postayı en az üç kişiye gönderirse burada gıyapta hakareten bahsetmek mümkün olacaktır. Burada en kilit nokta doğrudan muttali olamama (vakıf olamama)⁵⁶¹ durumudur. Bu durum internet açısından aleniyetin gerçekleşmemiş olması olarak yorumlanmalıdır. Yani kamusal erişilebilirliğin mümkün olduğu bir internet sayfasına mağdur da dahil olmak üzere herkesin erişebileceği hakaret içerikli bir veri yüklenirse, mağdur henüz görmemiş olsa dahi görebilme imkanının mevcudiyeti dolayısıyla gıyapta değil huzurda hakaretin varlığı kabul edilmelidir. Dikkat edilirse madde gerekçesinde gıyapta hakaret için muttali olmama değil olamama durumundan bahsetmektedir⁵⁶². Buradan anlaşılması gereken şey, gıyapta hakaret için kişinin o an ve koşullarda hakaret içeriğini bilmemesi değil bilebilme olanağının söz konusu olmaması gerekmektedir⁵⁶³. Yani bir bakıma aleniyet için daha önce yapılan açıklamalarla paralel bir durum mevcuttur.

⁵⁵⁹ **TARHAN**, Tehdit ve Hakaret Suçları, sh:288; **ÇETİN**, Hakaret Suçları, sh:25.

⁵⁶⁰ **ARISOY**, Mine, Hakaret, in: T. B. B. D., Sayı: 72, Ankara, 2007, sh: 165- 166.

⁵⁶¹ **CENTEL/ ZAFER/ ÇAKMUT**, Kişilere Karşı Suçlar, sh: 230; **ERMAN**, Sahir, Hakaret ve Sövme Suçları, İstanbul, 1989, sh: 98.

⁵⁶² “Hakaret suçu, kişinin gıyabında da işlenebilir. Kişiye hazır bulunmadığı bir ortamda veya doğrudan muttali olamayacağı bir surette hakaret edilmesi durumunda, gıyapta hakaret söz konusudur. Ancak, gıyapta hakaretin cezalandırılabilmesi için, fiilin mağdurun gıyabında ve fakat en az üç kişiyle ihtilat ederek işlenmesi gerekir. Bu kişilerin toplu veya dağınık olmalarının suçun oluşumu üzerinde bir etkisi yoktur. Bir veya iki kişiyle ihtilat ederek de mağdura hakaret edilebilir. Bu gibi durumlarda da esasında bir haksızlık gerçekleşmektedir. Ancak, izlenen suç siyaseti gereğince, gıyapta hakaretin cezalandırılabilmesi için, mağdurun gıyabında en az üç kişiyle ihtilat edilerek, yani en az üç kişi muhatap alınarak hakaretin yapılması şart olarak aranmıştır.” (Madde Gereğesi’nden naklen)

⁵⁶³ Yargıtay Ceza Genel Kurulu bir kararında, mağdurun rencide edici sözleri işitme duygusunun azlığı nedeniyle duymaması halinde dahi suçun huzurda işlenmiş sayılacağına, aksine yani gıyapta işlendiğinin kabul edilmesinin yasa koyucunun amacıyla bağdaşmayacağı gibi sağır olan veya çeşitli engellerle söylenen sözleri işitmeyen veya anlamayan kişilere karşı huzurda ve alenen hakaret suçlarının işlenmesini olanaksız hale

Maddenin dördüncü fıkrasında hakaret suçunun alenen işlenmesi durumu düzenlediği⁵⁶⁴ ve bununla internetin kamusal erişilebilirliği mümkün kılınmış boyutu esas alındığı için birinci fıkradaki suçun temel halinin internetin kişisel iletişime açık yönüyle işlenebileceği kabul edilmelidir. Örnek vermek gerekirse, bir kişinin 124 maddede üzerinde durulduğu üzere internetteki kişisel haberleşme araçları ile başka bir kimseye onur, şeref ve saygınlığını rencide edebilecek nitelikte somut bir fiil veya olgu isnad edecek ya da sövecek olursa, bu durumda 125. maddenin birinci fıkrasını uygulamak gerekecektir. Çünkü burada hakaret içeriği aleniyet kazanmamış, dolayısıyla internet bu kapsam kitle iletişim aracı olarak kullanılmamıştır. İnternet, kullanılan imkanın niteliği itibariyle hem kitle iletişim aracı hem de özel iletişim aracı olarak değerlendirilebilir. Bu fıkra düzenlemesiyle kitle iletişim aracı olarak değil özel iletişim aracı olarak kullanılmıştır.

Birinci fıkradaki bu düzenlemenin ardından *bir nitelikli hal* düzenlemesi olan dördüncü fıkraya geçilecek olursa, bu fıkrada ise hakaret suçunun alenen işlenmesi bir ağırlaştırıcı neden olarak düzenlenmiştir⁵⁶⁵. Fıkra hükmü kapsamında internette aleniyet kesbeden halleri ele almadan önce fıkranın düzenleniş süreci ile ilgili çok önemli bir durumu göz önünde bulundurmak gerekmektedir. Fıkranın ilk düzenlendiği halinde suçun aleni işlenmesinin yanı sıra yine bir ağırlaştırıcı neden olarak suçun basın yayın yoluyla gerçekleşmesi de düzenlenmekteydi. Ancak 29.06.2005 tarih ve 5377 sayılı Kanun ile suçun basın yayın yolu ile işlenmesi ağırlaştırıcı nedeni kaldırılmış ve kaldırılış gerekçesi de aynen şöyle dile getirilmiştir;

“... suçun basın ve yayın yoluyla işlenmesi hali de, aleniyetin gerçekleştiği şekillerinden birini oluşturmaktadır. Hakaret suçuyla ilgili olarak aleniyet bir nitelikli unsur olarak belirlendiği için, söz konusu suçun basın yayın yoluyla işlenmesi bu suç açısından ayrı bir nitelikli unsur olarak görülmemiştir.”

Bu ifadeden de anlaşılacağı üzere kanun koyucu aleniyetten bahsettiği her noktada esasında ilgili suçun basın yayın yolu ile de işlenebilirliğini kapsayacak şekilde geniş bir

getireceği kabulüne varmıştır. Emsal gösterilen karar ve değerlendirmenin ayrıntıları için bkz. **TARHAN**, a.g.e., sh: 288.

⁵⁶⁴ “Aleniyet” kavramına ilişkin bkz. İkinci Bölüm, § 5.- Suça Etki Eden Neden Olarak Aleniyet Unsurunun İnternet Aracılığıyla İşlenen Suçlar Bakımından Değerlendirilmesi.

⁵⁶⁵ Yargıtay kararlarında ağırlıklı olarak aleniyetin herkese açıklık ile eş değer tutulduğu gözlemlenmektedir. Bu yönde kararlar için bkz. Yargıtay 4. CD, 03.05.2004, 5242/ 5734; Yargıtay 4. CD. 23.06.2004, 5003/ 8012; Yargıtay 4. CD. 28.12.2004, 13822/ 12777, **TARHAN**, Tehdit ve Hakaret Suçları, sh: 459- 460’ dan naklen.

yorumu kabul etmektedir. O halde hiç şüphe yok ki şayet bir suçun aleni olarak işlenmesinden bahsedilecekse burada aynı zamanda basın yayın yolu ile de işlenebilir olduğunu kabul etmek gerekecektir. Bu yaklaşım tarzı tarafımızca yerinde görülmele beraber bir noktanın üzerinde durulması gerektiğini düşünmekteyiz. Böyle bir ön kabul sadece hakaret suçunun karakteristik özelliğinden kaynaklanmamaktadır. Bizatihi aleniyet kavramı ile basın yayın arasındaki ilişkiden kaynaklanmaktadır. Buna rağmen kanun koyucunun bu ve buna benzer birkaç maddede uyguladığı bu düşünceyi tüm Ceza Kanunu sistemine yansıtması gerekmektedir. Ancak ileride ele alınacak suç tiplerinde görüleceği üzere aynı madde kapsamında hem suçun aleni işlenmesi hem de basın yayın yoluyla işlenmesi ayrı ayrı düzenlenmiştir. **Kanaatimizce bu durum sistem içi bir tutarsızlığı ortaya koymaktadır. Bu konuya daha sonra yeniden değinilecektir. Bu konuda son bir not daha aktarılması gerekmektedir. Her ne kadar madde metninden basın yayın yoluyla hakaret suçunun işlenmesi hükmü çıkarılmışsa da madde gerekçesinde halen “ Keza aleniyetin basın yayın yoluyla gerçekleşmesi durumunda arttırma oranı ayrıca düzenlenmektedir.”** demek suretiyle madde metni ile gerekçe arasında bazı maddelerde de olduğu gibi uyumsuzluk yaratılmıştır. **Bu anlamda daha düzenli bir yasama mühendisliği bir gereklilik haline dönüşmüştür.**

Daha önce diğer suç tipleri için yapılan değerlendirmelere paralel olarak internet açısından aleniyet unsurunun gerçekleşmesi, suç teşkil eden içeriğin internetin kamusal erişilebilirliği mümkün kişisel veya kurumsal siteleri, forumlar, haber grupları, gazete ve dergilerin internet siteleri, v.b. unsurlarından edinilebilir olmasına bağlıdır. Bu şart gerçekleştiği takdirde internet ortamında aleniyet gerçekleşmiş olacaktır. Dolayısıyla internet aracılığıyla işlenen hakaret suçunda da aleniyet bu minvalde düşünülmesi gerekmektedir.

Bu değerlendirmelerin yanında maddenin üçüncü fıkrasında düzenlenen içeriğe ilişkin ağırlaştırıcı nedenlerin tümünün internet aracılığıyla da işlenebileceği de vurgulanmalıdır.

İnternet açısından hakaret suçunda en çok karşılaşılabilecek olan *hafifletici neden* hakaretin karşılıklı olarak işlenmesidir(5237 sayılı TCK md. 129/3)⁵⁶⁶. Yukarıda da örnekleriyle açıklandığı üzere kişiler internet ortamında denetim mekanizmalarının zaafı dolayısıyla düşüncelerini hakaretimiz ifadelerle dile getirebilmekte ve buna karşın teknik

⁵⁶⁶ MADDE 129. - (1) Hakaret suçunun haksız bir fiile tepki olarak işlenmesi hâlinde, verilecek ceza üçte birine kadar indirilebileceği gibi, ceza vermektense vazgeçilebilir.

(2) Bu suçun, kasten yaralama suçuna tepki olarak işlenmesi hâlinde, kişiye ceza verilmez.

(3) Hakaret suçunun karşılıklı olarak işlenmesi hâlinde, olayın mahiyetine göre, taraflardan her ikisi veya biri hakkında verilecek ceza üçte birine kadar indirilebileceği gibi, ceza vermektense vazgeçilebilir

bir incelemeye girilmeksizin tespit edilememektedirler. Bu nedenle özellikle değişik konularla ilgili açılmış forum sayfalarında veya sohbet odalarında kişiler karşılıklı olarak birbirlerine hakaret edebilmektedirler. Burada önemli olan husus karşılık anının herhangi bir süreye tabi tutulup tutulmadığıdır. *Soyaslan*, karşılıklı hakaretin niteliği itibariyle ancak kişilerin huzurda olmaları halinde işlenebileceğini savunmaktadır⁵⁶⁷. Ancak yazarın bu ifadesinden huzurda sayılan halleri de bu kapsamda değerlendirip değerlendirmedeği anlaşılmamaktadır. Kanaatimizce huzurda sayılan hallerin de karşılıklı hakaret suçuna imkan vereceği kabul edilmelidir⁵⁶⁸. Böyle bir durumda ilk hakarete maruz kalan tarafın hakaret içerikli ifadeyi öğrendiği zamanın karşılıklı hakaret için aranan zaman olduğu düşüncesi de her zaman istenilen sonucu verecek bir çözüm değildir. Örneğin bir kişinin internette bir forum veya paylaşım sitesinde yada kişisel bir web sayfasında kendisi hakkında kullanılan hakaretimiz ifadeyi ne zaman öğrendiğinin tespiti çok güç ve hatta yerine göre imkansızdır. Dolayısıyla böyle bir durumda zaman kriterinden hareketle değil her iki hakaret arasındaki nedensellik bağı üzerinden bir değerlendirme yapmak daha isabetli olacaktır.

Hukuka aykırılık unsuru internet perspektifinden değerlendirilecek olursa bu noktada iki önemli nokta dikkati çekmektedir. Bunlardan biri haber verme hakkının sınırları ikincisi de eleştiri hakkıdır. Bu hakların kullanılması dahilinde kalmak suretiyle ifade edilen sözcükler görünüş itibariyle bir hakaret suçuna vücut veriyormuş gibi algılansa da 5237 sayılı TCK md. 26 çerçevesinde hakkın kullanımı dolayısıyla hukuka uygun kabul edilmelidir. Her iki hak kullanımının ceza hukukunda algılanış tarzı ve Yargıtay'ın belirlediği temel kriterler ile ilgili birinci bölümde ayrıntılı olarak bilgi verilmiştir. Bu açıdan tekrara girmek için konu ile ilgili birinci bölüme atıf yapmakla yetiniyoruz.

Suçun *özel görünüş şekilleri* ile ilgili olarak da gerek teşebbüs, gerek iştirak gerekse içtima bakımından incelemeye tabi tutulan diğer içerik suçlarından farklı özelliğe rastlanmamıştır. Hakaret suçu kural olarak teşebbüse elverişli değildir. Ancak internet ortamında hakaret içerikli bir iletinin muhatabına teknik veya başkaca sebeplerden ulaştırılamaması durumunda teşebbüsten bahsetmek mümkün olacaktır⁵⁶⁹. Yine hakaret suçunun internette işlenebilen hali bakımından zincirleme suç ve fikri içtima hükümlerinin

⁵⁶⁷ **SOYASLAN**, Ceza Hukuku Özel Hükümler, 258.

⁵⁶⁸ Nitekim *Yargıtay* da 17.05.2002 tarih ve E. 2002/203 – K. 2002/1903 sayılı kararında “*santığın, internet ortamında maktül ile küfürleştiği...*” ifadesini kullanmak suretiyle huzurda sayılan hallerde de bir karşılıklılığın söz konusu olabileceğini kabul ettiği anlaşılmaktadır.

⁵⁶⁹ **CENTEL/ ZAFER/ ÇAKMUT**, Kişilere Karşı Suçlar, sh:253; **ÖNDER**, Ceza Hukuku Özel Hükümler, sh: 274-275.

uygulanabileceğini söylemek mümkündür. Ancak bu noktada bir hususa dikkat çekilmelidir. Failin aynı suç işleme kararıyla gerçekleştirdiği fiillerden biri hakaret diğeri sövmeyi oluşturduğu takdirde, 5237 sayılı TCK’de bu her iki hareket de hakaret suçunun seçimlik hareketleri olarak düzenlendiği için bunlar arasında zincirleme suç hükümlerinin uygulanması gerekmektedir.

1.2.6.- Haberleşmenin Gizliliğini İhlal

Bir haberleşme aracı olarak internet günümüzde sunduğu birçok hizmetle telefon, telgraf, mektup gibi birçok haberleşme aracının “klasik” olarak adlandırılmasına neden olmuştur. Özellikle kişiler arası iletişimin süratle ve küresel bir ağ üzerinden çoklu ortam yani multimedya olanaklarıyla eş zamanlı olarak sesli ve görüntülü olarak kurulabilmesi ve bu iletişimin deniz aşırı ve hatta kıta aşırı ülkeler arasında diğer haberleşme araçlarına oranla daha az maliyetle yapılabilir hale gelmesi internetin çağın en etkin haberleşme aracı haline gelmesini mümkün kılmıştır⁵⁷⁰. Bu yönde yaşanan gelişmeler de internet aracılığıyla kurulan haberleşmenin içeriğinin muhafaza edilmesi hususunda ciddi problemlerin yaşanmasına neden olmaktadır⁵⁷¹. Bu problemlerin önüne geçmek için teknik anlamda bir takım tedbirlere

⁵⁷⁰ İnternetin bu özelliğine bir örnek olarak VoIP (Voice Over IP) tekniği gösterilebilir. Bu teknikle iletimi istenen ses IP ağı üzerinden analog işaretler vasıtasıyla sayısal işaretlere dönüştürülüp sıkıştırılır, paketlere bölünür. Daha sonra IP ağı üzerinden gönderilir ve alıcıda tekrar analog işaretlere dönüştürülür. Nihayet analog sinyaller olarak paket olarak aktarılan verisinin çözülmesini sağlayacak uygun bir encoder ve sesi dışarıya yansıtacak gerekli donanım ile sesli iletişim sağlanmış olur. VoIP teknolojisinin detayları için bkz. http://www.tele.com.tr/blog_comment.asp?bi=918 (Erişim Tarihi: 15.01.2008, Saat:21:45)

⁵⁷¹ Kutlu bu durumu şöyle ifade etmektedir; “NSA, CIA ve FBI; İnternet üzerinden yapılan haberleşmeleri uzun süredir gözliyorlar. Bilgisayar servis sağlayıcılara yerleştirilen bir yazılım sayesinde belirli bir e-posta adresine veya oradan yollanan mesajlar gizli servislerce alınabilmekte, belirli İnternet adresiyle ilgilenen herhangi birisinin tüm İnternet faaliyetleri izlenebilmektedir. NSA'nın geliştirdiği ECHELON sistemi telefonların yanı sıra, teleks, faks ve internette de hedef kelimelerle tarama yapabilmektedir. NSA, milyonlarca mesajın içinden aranan sözcüklerin geçtiği mesajları; o mesajı gönderen bilgisayarı ve hesap sahibini saptayabilmektedir. NSA ve CIA, İnternet üzerinden yapılan tüm haberleşmeyi uzun süredir gözlemektedir. Kısaca internette sörf yapmak özgür ve bakir alanda dolaşmak olmaktan çoktan çıkmıştır. Yalnız sanal dünyada yapılan yolculuklar ve haberleşmeler sistemin egemenleri tarafından gözlenmiyor. Bilgisayar eşleştirme tekniği ile daha önce farklı veri tabanlarında ayrı ayrı duran verilerin birleştirilmesi ve karşılaştırılması sayesinde, insanların tam bir profilini çıkarmak mümkün hale gelmiştir. Bu yolla başka şeyler yanında tüketici profilleri de çıkarılmakta, hedef alınan ve yaratılan tüketici, kendini gözlenir kılmakta, kişi kendi gözetiminin taşıyıcısı haline gelmektedir. Bu tür gözetim, genel olarak hayatının rutinindeki gözetimin yoğunlaşmasına neden olmaktadır. Herhangi bir ücretli siteme girmeden bile e-posta kutunuzda hemen her gün junk- posta niteliğinde mesajlar bulmanız mümkündür. Yasal denetim ise başta İngiltere ve ABD olmak üzere tüm dünyada yaygınlaşmaktadır. Bu durumda İnternet servis sağlayıcıları bilgisayar sistemlerine bir kara kutu koymak zorunda kalmaktadırlar. Türkiye’de ise geçtiğimiz yıl yayınlanan bir yönetmelikle, güvenlik güçlerinin dinleme yetkisi genişletildi. Buna göre chat, e-posta ve internet üzerinden yapılan haberleşme de dinleme ve takip altına alındı. Yani İnternet kullanımıyla özgürleşmek bir yana denetim mekanizmalarının daha da artması söz konusu artık.” Ayrıntılı bilgi

rastlamak mümkündür⁵⁷². Ancak bu tedbirler internet teknolojisinin her geçen gün gelişim göstermesi karşısında internet üzerinden kurulan haberleşmenin gizliliğini korumakta her zaman istenilen neticeyi veremediği gibi haberleşme gizliliği artık daha kolay ihlal edilebilir bir hale gelmiştir. Örneğin casus yazılımlar olarak bilinen bir takım programlar kullanıcının internet ortamında kendine gönderilen sahte bir posta üzerinde işlem yapması veya açılan düzemece bir pencerede yönlendirilen komutları vermesi ile bilgisayara yerleşir, kendini kopyalar ve kullanıcının haberi olmadan tüm verileri toplayarak yetkisiz bir kişiye gönderebilir⁵⁷³. Bu veriler içinde hiç şüphe yok ki iletişim içerikleri de yer almaktadır. Bahsedilen tarzda faaliyetlerin gerçekleştirildiği casus ve kötücül atak tarzlarına örnek olarak, iletişimin tarafı olmayan üçüncü bir kişinin iletişim içeriklerine ulaşmasını mümkün kılan MITM (*Man- in- the- middle attack*)⁵⁷⁴, kişiler arasındaki iletişimin yetkisiz kişiler tarafından dinlenilmesine imkan tanıyan telekulak/ saçak damlası (*Eavesdropping*)⁵⁷⁵ gösterilebilir. Bunlar sadece birkaç örnek olup internet üzerinden kurulabilecek her türlü haberleşmeye ilişkin içeriğin ele geçirilmesine imkan tanıyan bir çok casus ve kötücül yazılım mevcuttur. Bu bakımdan dolayısıyla internet üzerinden gerçekleştirilen haberleşme gizliliğini ihlal eyleminin bir suç olarak ceza kanunlarında düzenlenmesi önem arz etmektedir.

için bkz. **KUTLU**, Işıl, İnternet: Olanaklar ve Hayaller, Kaynak: <http://www.bianet.org/bianet/yazdir/8729> (Erişim Tarihi: 06.02.2008, Saat: 16:10)

⁵⁷² Bu tedbirlerden biri şifreleme tekniğidir. Şifreleme, mesajları kodlama ve kod çözme tekniğidir. Esas olarak, şifreleme sıradan bir düz metni veya haberi şifreli bir metne dönüştürmek demektir. Bu haberi alan taraf bir anahtar kullanarak şifreli metni çözerek düz metne dönüştürür. İki tarafta uygun anahtara sahip olduğu müddetçe şifre çözerek bir mesajı eski orijinal şekline veya düz metne çevirebilirler. Şifreli haberleşmenin bütünlüğünü sağlamada risk, gizli kalması gereken anahtarın başarılı bir şekilde karşı tarafa aktarılmasını güvence altına almadır. Bundan dolayı bir şifreli haberleşme ancak anahtarının emniyet ve gizliliği kadar emin ve gizlidir. Şifreleme tekniği bir çok birey ve özel sektör örgütünce kullanıldığı gibi, İnternet üzerindeki e-posta haberleşmesine yetkisiz girişi önleyen PGP (Pretty Good Privacy) gibi yazılımlar sayesinde e-posta mesajlarının transferinde de kullanılır. PGP bir güçlü şifreleme programı olup orijinal olarak, iletişimin dinlemesine karşı bireysel mahremiyeti korumak amacı ile güçlü şifrelemenin kamu için ulaşılabilir hale getirilmesi hedeflenmiş ve bu yönde çalışmalar yapılmıştır. Bugün şifreleme yazılımlarına internet üzerinde erişilemek ve bunları kullanabilmek mümkündür. Ancak bu tarz şifreleme yazılımlarının devre dışı bırakıldığı kötücül yazılımların varlığı da bilinmektedir. O bakımdan internet üzerinden kurulan iletişimin bu tarz programlarla mutlak anlamda güvence altına almak imkansızdır. Şifreleme tekniği ile ilgili olarak bkz. **ÖCAL**, Fatih/ **BİLGE**, Hasan Şakir, Güvenli İletişim İçin Donanımsal Şifreleme Sistemi, in: Ulusal Elektronik İmza Sempozyumu – Bildiriler Kitabı, Ankara, 2006, sh: 64 v.d.; **ŞAŞIOĞLU**, A. Betül/ **ACAR**, Doğan/ **GÜNEŞ**, İs posta/ **BAHADIR**, Ömer/ **ÇAKMAKKAYA**, Zerrin, Güvenli Kurumsal Mesajlaşma Uygulamaları, in: UEİS., sh: 86 v.d.; **ÜLGEN**, Halil İbrahim/ **SAGIROĞLU**, Şeref/ **YÜNCÜ**, Selma, Güvenli Bir E- Posta Uygulaması: Gü- Posta, in: UEİS, sh: 142 v.d.; **TUĞLULAR**, Tuğkan, Güvenli Elektronik Posta, in: Türkiye Bilişim Ansiklopedisi, sh: 436.

⁵⁷³ **CANBEK/ SAĞIROĞLU**, Kötücül ve Casus Yazılımlar, sh: 125.

⁵⁷⁴ **AKGÜN/ BULUŞ/ ŞEN**, Bilgisayar Ağları, (Erişim Tarihi: 07.02.2008, Saat:15:08).

⁵⁷⁵ **CANBEK/ SAĞIROĞLU**, Bilgisayar Sistemlerine Karşı Saldırımlar, sh: 8.

Haberleşmenin gizliliğini ihlal suçu 5237 sayılı TCK md. 132’de düzenlenmiştir⁵⁷⁶. TCK md. 132’de düzenlenen haberleşmenin gizliliğini ihlal suçunu internet açısından değerlendirirken öncelikle *maddi unsuru* üzerinde durulmalı ve madde fıkra fıkra ele alınmalıdır.

Maddenin birinci fıkrasının birinci cümlesinde haberleşmenin gizliliğinin ihlali bakımından herhangi bir özel tercihte bulunulmamış ve haberleşmenin gizliliğini ihlal edici nitelikte her tür eylemin bu kapsamda değerlendirilebileceği ortaya konulmuştur. Madde gerekçesinde de söz konusu suçun belirli kişiler arasındaki haberleşmenin içeriğinin öğrenilmesiyle işleneceği ifade edilmiştir. Bu noktada *Şen*, gerek madde metninde gerekse madde gerekçesinde “*haberleşme*” kavramından neyin kastedildiğinin açıkça belirtilmemesini kanunilik ilkesi açısından problemlili görmekte ve haberleşme deyiminden anlaşılması gerekenin bireylerin başkalarıyla paylaşmadığı ve doğrudan doğruya olmayıp bir araç vasıtasıyla yapmış oldukları görüşmelerin içeriğinin anlaşılması gerektiğini vurgulamıştır⁵⁷⁷. Bu tespit ile ilgili değerlendirme için haberleşme kavramının içeriği ve kapsamı ile ilgili ikinci bölümde yapılan açıklamalara atıf yapılmakla birlikte⁵⁷⁸ bir noktanın vurgulanması gerektiği kanaatindeyiz.

“*Haberleşme*” kavramı *Şen*’in ifade ettiği üzere bir “*görüşme içeriği*”ni betimlememektedir. Haberleşme kavramı ile esas itibariyle haber niteliği taşıyan bir içeriğin taraflar arsında iletiminin tarz ve yöntemini de kapsayan bir süreç kastedilmektedir⁵⁷⁹. Bu içerik aynı kalmak üzere içeriğin iletimi bakımından tercih edilen aracın niteliğine göre söz konusu etkinlik (haberleşme) özel/ bireysel ya da kitle iletişim olarak görünüm kazanır.

⁵⁷⁶ **MADDE 132.** - (1) Kişiler arasındaki haberleşmenin gizliliğini ihlâl eden kimse, altı aydan iki yıla kadar hapis veya adlî para cezası ile cezalandırılır. Bu gizlilik ihlâli haberleşme içeriklerinin kaydı suretiyle gerçekleşirse, bir yıldan üç yıla kadar hapis cezasına hükmolunur.

(2) Kişiler arasındaki haberleşme içeriklerini hukuka aykırı olarak ifşa eden kimse, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır.

(3) Kendisiyle yapılan haberleşmelerin içeriğini diğer tarafın rızası olmaksızın alenen ifşa eden kişi, altı aydan iki yıla kadar hapis veya adlî para cezası ile cezalandırılır.

(4) Kişiler arasındaki haberleşmelerin içeriğinin basın ve yayın yolu ile yayınlanması hâlinde, ceza yarı oranında artırılır.

⁵⁷⁷ Benzer görüş için bkz. **TEZCAN/ ERDEM/ ÖNOK**, Ceza Hukuku Özel Hükümler, sh: 384.

⁵⁷⁸ Bkz. İkinci Bölüm, § 5.- 5237 Sayılı TCK md. 6/1- G Hükümnce Bir Kitle İletişim Aracı Olarak İnternet.

⁵⁷⁹ Bizim de iştirak ettiğimiz üzere *İçel/ Ünver* “*Haberleşme*”yi şöyle tanımlamaktadırlar: “ haberleşme, bilgi, düşünce ve tutumların ortak semboller sistemi aracılığıyla kişiler ve gruplar arasında değiş tokuş edildiği bir süreçtir.”. **İÇEL/ ÜNVER**, Kitle Haberleşme Hukuku, sh: 4.

Örneğin aynı içerik internette bir e-posta veya bireysel iletişim araçları kullanılmak suretiyle bir kaynaktan bir başka kaynağa iletiliyorsa burada özel bir haberleşmenin varlığından, şayet bu içerik bir web sitesinde herkesin erişimine açılmışsa da burada kitle haberleşmenin varlığından bahsedilebilir. Ayrıca bir etkinlik olarak haberleşmeyi doğrudan doğruya olmayıp mutlak suretle bir araç vasıtasıyla gerçekleşen bir süreç olarak da kabul etmek mümkün değildir. Bu yüzden *Şen'in* suç tipinin temel kaynağı olan “*haberleşme*”ye bakış açısını kabul etmemekteyiz.

Aynı fıkranın ikinci cümlesinde ise gizlilik ihlalinin haberleşme içeriklerinin kayda alınması suretiyle gerçekleştirilmesi, suçun basit şekline oranla daha ağır bir cezai müeyyideye tabi tutulmuştur. Böyle bir düzenleme gizli kalması gereken bir haberleşme içeriğinin, kayıt altına alınmak suretiyle, ifşa edilebilme imkanını daha da geniş tuttuğu için nitelikli bir hal olarak ele alınmıştır. Ancak bu kaygı ile yapılan düzenlemenin, sadece gizlilik ihlalinin bizzat kayda almak suretiyle gerçekleştirilmesi için değil, kayda alınmış özel haberleşme içeriklerinin teminini de kapsar nitelikte olması gerekmektedir. Örneğin internet ortamında bir takım sohbet programları, online sohbet esnasında içerikleri otomatik olarak kayıt altına almaktadır. Bu kayıt altına alma işlemi kullanıcının inisiyatifine bırakılmıştır. Kullanıcı talep ettiği takdirde söz konusu iletişimin kayıt altına alınmasını engelleyebilmektedir. Böyle bir engelleme durumu söz konusu değilse program girilen her veriyi o anda kayıt altına almaktadır. Şayet kullanıcının rızası dışında söz konusu programa yetkisiz erişim sağlanıp, bu program vasıtasıyla kurulan iletişimin kayıt altına alınması komutu verilip, daha sonra kayıt altına alınan veriler temin edilirse burada TCK md. 132/1 – c.2 hükmünün gerçekleşmiş olduğundan şüphe yoktur⁵⁸⁰.

Ancak programa hiçbir müdahalede bulunulmaksızın, otomatik olarak kayıt altına alınmış verileri kopyalayarak temin etmek ve içeriğini öğrenmek suretiyle haberleşme gizliliği ihlal edilecek olursa, suç teşkil eden eylem doğrudan kayda almak suretiyle

⁵⁸⁰ Casus yazılım (spyware), kullanıcılara ait önemli bilgilerin ve kullanıcının yaptığı her türlü işlemi - ki bunlara internet ortamında kurduğu iletişim de dahil olmak üzere - , kullanıcının bilgisi olmadan toplanmasını, kaydedilmesini ve bu bilgilerin söz konusu yazılıma komut veren kişilere gönderilmesini sağlayan yazılım olarak tanımlanır. Bu tarz yazılımlar, benzer nitelikli kötücül yazılımlardan farkı olarak, internet kullanıcıları tarafından sistemlere farkında olmadan bulaştırılmaktadırlar. Yine casus yazılımlar, virüs ve solucanlardan farklı olarak hedef sisteme bir kez bulaştıktan sonra kendi kopyasını oluşturarak daha fazla yayılmaya ihtiyaç duymazlar. Casus yazılımın amacı hedef olarak seçilen sistem üzerinde gizli kalarak istenen her türlü bilgiyi toplayıp kayda alıp üçüncü bir şahsa göndermektir. Şu halde 5237 sayılı TCK md. 132 özelinde bir casus yazılım kullanarak haberleşme gizliliği ihlal ediliyorsa, burada sadece verinin kayda alınması değil kayıt altına alınmış verinin teminin de kapsam dahiline alınması gerekmektedir.

gerçekleşmediği için fıkra hükmü uygulanamayacaktır. Her ne kadar doktrinde *Tezcan/ Erdem/ Önok*,

*“Gizliliği ihlal edilen haberleşmenin içeriğini ses ve/veya görüntü kaydına alınmışsa , 132/1 c2 uygulanır. Bu kayıt konuşmanın ses kayıt cihazı ile tespit biçiminde olabileceği gibi, mektubun bir kopyasının yapılması ve hatta mektup içeriğinin ses ve görüntü kaydına alınması biçiminde de olabilir.”*⁵⁸¹

demekteyseler de kanun metninde veya gerekçesinde bu yönde bir tercihin açıkça vurgulanmamasına ve “*kayda almak*” kavramının anlam açıklığına rağmen kayıt altına alınmış bir verinin kopyasının bu kapsamda değerlendirilemeyeceği kanaatindeyiz. Çünkü süreçsel açıdan öncelikle söz konusu verinin kayıt altına alınması gerekmektedir. Daha sora kayır altına alınmış verinin kopyalanması mümkündür. O halde bu durumu kayda alma kapsamında değerlendirmek mümkün değildir.

Maddenin ikinci fıkrasında haberleşme içeriklerinin hukuka aykırı olarak ifşa edilmesi suçu düzenlenmiştir. Bu suçun faili birinci fıkrada olduğu gibi haberleşmenin tarafları dışındaki biridir. Şayet bu kişi haberleşmenin taraflarından biri olursa o zaman aynı maddenin üçüncü fıkrası söz konusu olacaktır. Anılan fıkrada “*ifşa etmek*” kavramından neyin kastedildiği gerek madde metninde gerekse gerekçede açıkça vurgulanmamıştır. Ancak aşağıda değinileceği üzere üçüncü fıkrada açıkça “*alenen ifşa etmek*” kavramı kullanıldığı için buradaki “*ifşa etmek*” kavramından, gizli kalması gereken haberleşme içeriğinin aleniyet unsuru gerçekleşmeksizin belli veya belirlenebilir sayıda kişiye aktarılmasının anlaşılması gerektiği söylenebilir. Ayrıca gerekçede bu kişilerin yetkisiz kişiler olduğu da belirtilmiştir. Yalnız gerekçenin aynı maddeye ilişkin kısmında maddenin tüm sistemini etkileyecek bir açıklamaya yer verilmiştir.

Şöyle ki; madde gerekçesinde “ *Maddenin ikinci fıkrasında, kişiler arasındaki haberleşme içeriklerinin hukuka aykırı olarak ifşa edilmesi, ayrı bir suç olarak tanımlanmıştır. Haberleşme içerikleri hukuka uygun bir şekilde veya birinci fıkrada tanımlanan suçun işlenmesi suretiyle öğrenilmiş olabilir. İkinci fıkrada tanımlanan suç, haberleşme içeriklerinin ifşasıyla, yayılmasıyla, yani yetkisiz kişilerce öğrenilmesinin sağlanmasıyla oluşur. Fıkra metninde bu ifşanın hukuka aykırı olması açıkça vurgulanmıştır. Bu bakımdan örneğin kişiler arasındaki telefon konuşmalarına ilişkin kayıtların, savcılık veya*

⁵⁸¹ TEZCAN/ ERDEM/ ÖNOK, Ceza Hukuku Özel Hükümler, sh: 383.

mahkemeye verilmesi, duruşmada açık bir şekilde dinlenmesi veya okunması hâlinde, söz konusu suç oluşmayacaktır. Buna karşılık, henüz soruşturma aşamasında iken, kişiler arasındaki konuşma içeriklerinin, hukuka uygun bir şekilde kayda alınmış olsalar bile, örneğin televizyonlarda veya gazetelerde yayınlanması hâlinde, bu suç oluşacaktır.” denilmektedir.

Dikkat edilirse kanun koyucu açıklamanın son cümlesinde gizli kalması gereken haberleşme içeriklerinin şartlar gerçekleştiği takdirde gazete ve radyolarda yayımlanmasını bu fıkra hükmüncü suç olarak değerlendirmektedir. Bu durumda cevap bekleyen birtakım sorular ortaya çıkmaktadır. Şayet aleniyet unsurunu gerçekleştirmeye müsait araçların bu suç için de kullanılmaları mümkünse, niçin aynı maddenin bir sonraki fıkrasında özellikle “*alenen ifşa*” kavramı kullanılmıştır, bir başka ifade ile niçin bu fıkrada sadece “*ifşa*” demekle yetinilmiştir? Şayet “*alenen ifşa*” ile “*ifşa*” arasında bir farklılık yoksa ve aleniyeti gerçekleştirmeye elverişli basın yayın araçlarıyla da bu suç işlenebiliyorsa (gazete, radyo ve hatta internet gibi kitle haberleşme araçları), niçin ayrıca maddenin son fıkrasında suçun basın yayın yoluyla işlenmesi bir ağırlaştırıcı neden olarak düzenlenmiştir? Madde ile gerekçe arasındaki ilişkiden dolayı bu sorulara tutarlı yanıtlar vermek mümkün değildir.

Kanaatimize, bu fıkra hükmü bakımından “ifşa”yı aleniyet unsurunu gerçekleştirmeksizin belli veya belirlenebilen kişilere karşı yapılan açıklama olarak anlamak gerekmektedir. Bu suça internet açısından örnek olarak hukuka aykırı olarak temin edilen haberleşme içeriklerinin başka bir kişiye veya belirlenebilir birden fazla kişiye e- posta veya diğer kişisel iletişim araçlarıyla iletilmesi gösterilebilir.

Maddenin üçüncü fıkrasında kendisiyle yapılan haberleşmelerin içeriğini diğer tarafın rızası olmaksızın alenen ifşa edilmesi düzenlenmiştir. Bu suçun faili ilk iki fıkranın tersine haberleşmenin taraflarından biridir. Suçun internet aracılığıyla işlenebilirliği bakımından, gizli kalması gereken bir haberleşme içeriğinin bir web sayfasında veya forumlarda, yani kamusal erişilebilirliğin mümkün kılındığı internet alanlarında yayınlaması bu fıkranın gerçekleşmesi için birinci şarttır. İkinci şart ise bu içerik yayınlamasının taraflardan birinin rızası hilafına yapılmış olmasıdır. Dolayısıyla bu suç tipi bakımından rıza bir *hukuka uygunluk nedeni* olarak kabul edilmiştir. Bu düzenlemeyle birlikte maddenin dördüncü fıkrası birlikte değerlendirilecek olursa, haberleşme içeriğinin basın yayın yoluyla yayınlanmasını düzenleyen anılan fıkranın bir nitelikli hal olarak düzenlendiği görülmektedir.

Ancak bu düzenleme kanunun bütünü itibariyle dikkati çeken tutarsızlığın bir başka göstergesi olarak ön plana çıkmaktadır. Şöyle ki; 29.06.2005 tarih ve 5377 sayılı kanunla 5237 sayılı TCK’nın birçok maddesinde değişiklik yapılmış, özellikle aynı madde

kapsamında suçun hem alenen işlenmesi hem de basın yayın yoluyla işlenmesi ayrı ayrı düzenlenmişse, aleniyetin basın yayını da kapsayacağından mütevellit suçun basın yayın yoluyla işlenmesi hükmü kaldırılmıştır. Özellikle internet aracılığıyla işlenen suçlardan içerik suçları bakımından bu değerlendirme önceki suçlarda ayrıntısıyla değerlendirilmiştir. Ancak aynı tutum buraya yansıtılmamıştır. Yansıtılmadığı gibi hem “*aleni ifşa*”nın hem de “*basın yayın yoluyla ifşa*”nın birden muhafaza edilmesinin mantığı da dile getirilmemiştir. Hatta yukarıda da açıkça dile getirildiği üzere madde metni ile gerekçe arasında öyle bir karışıklık vardır ki hangi durumda hangi fıkra hükmünün uygulanacağı bile belli olamamaktadır. Dolayısıyla kitle haberleşme olanağı sunan haliyle bir basın yayın aracı olarak kabul edilen internette gizli kalması gereken haberleşme içeriklerinin yayınlanması konusunda bu ikilem ortadan kaldırılmalıdır.

Suçun *manevi unsuru* bakımından kanun koyucu özel bir tercihte bulunmamış ve kasten işlene bir suç olarak düzenlemiştir. Suçun niteliği itibariyle de olası kastla da işlenebilmesi mümkündür. Şöyle ki; bir kullanıcıya internet aracılığıyla gönderilen ve hedef kullanıcı tarafından fark edilmeden kabul edilen bir casus yazılım sahibine kişiye ait özel verileri yazılımı gönderen kullanıcıya gönderirken ilk etapta hedeflenmeden ama ihtimal dahilinde yukarıda örneklendirdiğimiz üzere kayıt altına alınmış iletişim dökümlerini de gönderebilir. Bu suretle kayıt altına alınmış bir veri olması ve bu yazılım vasıtasıyla transferinin mümkün olması dolayısıyla kanaatimizce olası kastla hareket edilebilme imkanı vardır.

Suçun özel görünüş şekillerinin internet perspektifinden değerlendirilmesini de şöyle özetlemek mümkündür; daha önce md. 124 kapsamında haberleşmenin engellenmesi suçunu internet açısından değerlendirirken, müdahale suçlarında içerik suçlarından farklı olarak kural olarak teşebbüse elverişliliğin söz konusunu olduğu vurgulanmıştır. Md. 132’de düzenlenen haberleşme gizliliğinin ihlali suçu da her ne kadar bir içeriğin yetkisiz olarak elde edilmesi ve ifşa edilmesi olsa da sadece bir içerik suçu değil, bu içeriğin yetkisiz bir müdahale ile gizli kalmasının engellenmesi dolayısıyla aynı zamanda bir müdahale suçudur, başka bir anlatım karma nitelikli bir suçtur. Böyle olunca müdahale boyutunu içeren diğer suçlarda olduğu gibi haberleşme gizliliğinin ihlali suçunda da teşebbüsün mümkün olduğu dile getirilebilir. Yine iştirak açısından özellikli bir duruma rastlanmazken içtima bakımından bir ayrıntı gözden kaçırılmamalıdır. Özellikle bir kişinin aynı suç işleme kararıyla internet aracılığıyla birden fazla haberleşme gizliliğinin ihlal edilmesinde aynı suç işleme kararı unsuruna dikkat edilmelidir. Çünkü haberleşme gizliliği taraflar dışından bir kişi tarafından ihlal ediliyorsa,

haberleşmenin yukarıda verildiği üzere karşılıklı bir süreç olması dolayısıyla her iki taraf esas alınarak ve değişen tarafların değişen haberleşme içerikleri göz önünde bulundurularak tespit edilmesi gerekmektedir. Bir tarafı sabit kabul edip değişken diğer tarafı bu bağlamda dikkate almamak zincirleme suç hükümlerinin uygulanmasında aynı suç işleme kararının doğru tespit edilmesini engelleyebilir.

1.2.7- Özel Hayatın Gizliliğini İhlal

Özellik internet teknolojisindeki gelişmeler karşısında özel hayatın küresel bilgi toplumunda büyük ölçüde tehditlerle karşı karşıya olduğu tartışmasızdır. Temel sorun internet üzerinden haberleşme ve veri aktarımının ulusal sınırları aşması, merkezi bir yönetimin, belli bir varlığa verilmiş genel bir sorumluluğun ve yasal mecburiyetleri uygulatacak uluslararası bir gözetim mekanizmasının olmayışdır. Bu nedenle internet kullanıcılarına ait şahsi veriler dünyanın her tarafında farklı sitelerde izlenip erişilebilir durumdadırlar. Her türlü kişisel verinin dijital ortama aktarılabilir olmasına paralel olarak özel hayata ilişkin birçok yeni bilgi uygulamaları gelişmektedir.

Bu açıklamalar ışığında 5237 sayılı TCK md. 134 çerçevesinde özel hayatın gizliliğini ihlal suçu internet açısından irdelenecek olursa, her şeyden önce suçun *maddi konusu* üzerinde durulmalıdır. Anılan suçun maddi konusu özel hayatın mahrem unsurlarıdır. Kanun koyucu gerek madde metninde gerekse madde gerekçesinde özel hayata ilişkin kapsam tercihini ortaya koymamıştır. Bu hususu *Şen*, kanaatimizce de isabetli olarak şöyle eleştirmektedir:

“ Yine kanun koyucu bu maddede, Anayasa hükmünde yer alan genel ve soyut kavramı kullanma yolunu seçmiş “özel hayat” kavramının ne olduğunu ortaya koyabilecek ve “suçta kanunilik” prensibine uygun düşecek tanımlamayı yapmamıştır.”özel hayat” ve “özel hayatın gizliliği” kavramları son derece geniş, soyut, kişiye ve duruma göre değişebilen yeteneklere sahiptirler bu sebeple kişilerin özel hayatının gizliliğini ihlal eden kimse cezalandırılır hükmü yerine kanun koyucu 134 maddenin gerekçesinde de özel hayat ve özel hayatın gizliliği kavramlarının ne olduğu bu kavramların kişiye zamana ve yere göre ne şekilde anlaşılması gerektiğine ve bu kapsamda kamuya mal olmuş kişiler kavramından ne anlaşılması gerektiği hususlarına değinmemiş ve maalesef açıklama gereği duymamıştır. Belki kanun koyucu bu hususların tartışılmasını ve tespitini uygulamaya bırakmıştır. Ancak belirtmeliyiz ki TCK

hükümleri bir anayasa hükümleri değil somut durumlara uygulanması gereken açıklıkları ve somut ölçütleri taşıması gereken uygulama normlarıdır. ”⁵⁸²

Bu çerçevede suçun *maddi unsuru* internet açısından değerlendirilecek olursa, her şeyden önce şunu söylemek mümkündür ki internet teknolojisinin gelmiş olduğu nokta itibariyle bu madde de dahil olmak üzere bu bölümdeki bütün suçlar açısından internet çok önemli bir denek taşı konumundadır. Örneğin md. 134/1,c1'e göre özel yaşamı ihlal eden her türlü eylem bu hüküm çerçevesinde cezalandırılmaktadır. Bu durum yukarıda dile getirilen eleştirilerle birlikte değerlendirildiği zaman dokuzuncu bölümde yani “ *Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar*” bölümünde yer alan diğer suçlarla karışıklığa neden olma durumu söz konusu olabilecektir. Çünkü bu bölümde yer alan bütün suçlar birinci bölümde internet perspektifi ile özel hayatın gizliliğini hakkının değerlendirilmesinden ve örnek olarak belirtilen içtihatlardan da anlaşılacağı üzere özel hayatın gizliliğini korumak amacıyla düzenlenmiştir. Başka bir anlatımla bir kimsenin e-posta yazışma içeriklerinin ifşası veya e- posta kayıtlarına yetkisizi erişim, internet üzerinden eş zamanlı çoklu ortam⁵⁸³ olanaklarından yararlanılarak (MSN programı vasıtasıyla görüntülü ve sesli olarak) kurulan iletişimin kaydedilmesi veya ileride inceleneceği üzere bir bilgisayara internet ortamından gönderilen kötücül veya casus yazılımlar aracılığıyla hedefin kişisel verilerinin kaydedilmesi ve ele geçirilmesi eylemleri TCK md. 132 v.d. maddelerinde ayrı birer suç olarak düzenlemelerine rağmen hepsi özel hayatın gizliliğini ihlal niteliği taşımaktadır.

Ancak TCK md. 134'de “*özel hayat*” ve “*özel hayatın gizliliği*” kavramlarından neyin kastedildiği açıkça vurgulanmadığı ve madde gerekçesinde de “ *maddenin birinci fıkrasında, metninde özel hayatın gizliliğinin ihlali suç olarak tanımlanmaktadır. Böylece, gizli yaşam alanlarına girerek veya başka suretle başkaları tarafından görülmesi mümkün olmayan bir özel yaşam olayının saptanması ve kaydedilmesi cezalandırılmaktadır.*”⁵⁸⁴ gibi muğlak bir

⁵⁸² ŞEN, Hürriyete Karşı Suçlar, sh: 216.

⁵⁸³ İnternette çoklu ortam uygulamalarına ilişkin değerlendirmeler için bkz. ARKUT, Refik C./ ARKUT, İbrahim C. , İnternette Çoklu Ortam: Sorun ve Çözümler, Kaynak: <http://inet-tr.org.tr/inetconf10/bildiri/29.pdf> (Erişim Tarihi: 11.02.2008, Saat: 08:35); GÜRGEN, Fikret, Çokluortam Hizmetleri, in: Türkiye Bilişim Ansiklopedisi, İstanbul, 2006, sh: 300 v.d.

⁵⁸⁴ Gerekçedeki bu ifadelerde geçen “özel yaşam olayı” kullanımı muğlaklığı gidermekten öte olmakla birlikte bilakis sorunu daha da karmaşık hale getirmektedir. Çünkü burada “olay” kelimesinin hangi anlamda kullanıldığı anlaşılabilir değildir. Örneğin saptanan veya kayda alınan şey bir durumu ifade ediyorsa yani “olay” kelimesinin sözlük anlamı bakımından kayda alınan şey süreçsel devamlılık arz eden bir oluş hali değil de salt bir durumu içeriyorsa bu halde özel hayatın gizliliği ihlal edilip edilmediği sorunu kendini gösterecektir. Bu durumda ancak

açıklama yapılması nedeniyle anılan maddenin ayrıca düzenlenmesindeki anlam ve gereklilik ortaya konamamıştır. Böyle bir düzenlemenin amaca uygunluğunu sağlamanın iki yolu vardır. Birincisi yukarıda açıkça vurgulandığı üzere şayet bu bölümde aynı konuları düzenleyen maddelerden farklı bir içeriğe sahip olduğu düşünülüyorsa bu farklılık ve maddenin düzenleme alanının açıkça ortaya konulmasıdır. İkincisi ve tarafımızca da daha yerinde görülen yöntem ise 5237 sayılı TCK md. 257’de düzenlenen “Görevi Kötüye Kullanma” veya md. 244’de düzenlenen “Sistemin Engellenmesi, Bozulması, Verileri Yok Etme Değiştirme” suçlarının model alınmasıdır. Md. 257’de, kanunda açıkça suç olarak tanımlanan haller dışında niteliği itibarıyla görevi kötüye kullanma sayılabilecek eylemlerin cezalandırılması düzenlenmiştir⁵⁸⁵. Yine md. 244/4 göre, ilk üç maddede düzenlenen fiiller aracılığıyla bir menfaat temini söz konusuysa, bu eylem başka bir suça vücut vermediği takdirde anılan madde hükmü çerçevesinde cezalandırılacaktır⁵⁸⁶. Böylece her iki hükmün de tali, tamamlayıcı bir norm olarak düzenlenmenin yanında normatif bir dinamizm de yakalanmıştır⁵⁸⁷. Buna göre, TCK md. 134’e de aynı yaklaşım uygulanarak kanunda açıkça düzenlenmiş özel yaşam ihlalleri dışında uygulama ve doktrinin üzerinde hemfikir olduğu kriterler bazında tespit edilen özel yaşam alanının gizliliğini ihlal eylemlerinin cezalandırılmasına yönelik tali, tamamlayıcı bir düzenlemenin daha isabetli olacağı kanaatindeyiz.

Maddenin ikinci fıkrasında kişilerin özel hayatına ilişkin görüntü ve seslerinin ifşası suçu düzenlenmiştir. TCK md. 132 haberleşmenin gizliliğini ihlal suçunda da ifade edildiği üzere bu fıkra da geçen “ifşa” kavramını da aleniyet boyutuna ulaşamayan belli veya belirlenebilir kişilerin bilgisine sunma olarak kabul etmek gerekmektedir. Örneklendirilecek

kanun koyucunun olay niteliği taşıyan özel hayat verilerinin saptanması ve kaydedilmesini kabul ettiği söylenebilmesine rağmen bu da amacın dışında bir daraltma ve kanun koyucunun açıkça belirtmediği bir hususu var saymak olur ki bu durum ceza hukuku mantığı ile örtüşmez.

⁵⁸⁵ Madde Gereğesinde ilgili kısım şöyle dile getirilmiştir. “ Bir kamu göreviyle görevlendirilen kişi, bu kamu faaliyetinin yürütülmesi sırasında, görevinin gerekli kıldığı yükümlülüklerle uygun hareket etmek zorundadırlar. Öyle ki; kamu faaliyetlerinin gerek eşitlik gerek liyakatlilik açısından adalet ilkelerine uygun yürütüldüğü hususunda toplumda hâkim olan güvenin, inancın sarsılmaması gerekir. Bu yükümlülükle bağdaşmayan davranışlar, belli koşullar altında suç olarak tanımlanmıştır. Görevi kötüye kullanma suçu, bu bakımdan genel, tali ve tamamlayıcı bir suç olarak tanımlanmıştır. ...Görevi kötüye kullanma suçu, genel, tali ve tamamlayıcı bir suç tipidir. Bu nedenle, görevin gereklerine aykırı davranışın başka bir suçu oluşturmadığı hâllerde, kamu görevlisini bu suça istinaden cezalandırmak gerekir.”

⁵⁸⁶ Madde metnindeki açıklamaya karşın 244. maddenin gerekçesinde başka bir suçu oluşturmama kriteri değil daha ağır bir suçu oluşturmama kriterinin esas alınacağı vurgulanmıştır. Madde metni ile gerekçesi arasındaki bu çelişki ilgili maddenin internet açısından değerlendirilmesi esnasında ele alınacaktır.

⁵⁸⁷ **TEZCAN/ ERDEM/ ÖNOK**, Ceza Hukuku Özel Hükümler, sh: 633, **TOROSLU**, Ceza Hukuku Özel Hükümler, sh: 302; **SOYASLAN**, Ceza Hukuku Özel Hükümler sh: 521; **ARTUK/ GÖKCEN/ YENİDÜNYA**, Ceza Hukuku Özel Hükümler, sh:753.

olursa bir kişinin cinsel yaşamına ilişkin bir sırrının görüntülediği bir video dosyasının e-posta aracılığıyla başka kullanıcılara gönderilmesi gibi. Burada söz konusu postanın ve o postanın iliştilirilmiş dosyanın kimlere gönderildiği tespit edilebildiği için madde metninde kullanılan ifşanın gerçekleştiği kabul edilmelidir. Burada gönderilen kişinin gerçek kimliğinin bilinebilir olup olmamasının bir özelliği yoktur. Önemli olan verinin gönderildiği hedefin sınırlı ve belirli olmasıdır. Bu değerlendirme fıkranın devamındaki hüküm dikkate alındığında daha da anlam kazanacaktır.

Suçun manevi unsur genel kasttır. Özel hayatın gizliliğini ihlal suçu genel olarak kapsayıcı bir şekilde düzenlendiği için bu suç için olası kasttan bahsetmenin de mümkün olabileceğini kabul etmek gerekir.

Suçun nitelikli hallerinin internet aracılığıyla işlenebilirliği üzerinde durulacak olursa; birinci fıkranın ikinci cümlesinde, md. 132'de düzenlenen haberleşmenin gizliliğini ihlal suçundakine benzer bir düzenleme getirilmiş ve gizlilik ihlalinin görüntü ve seslerin kayda alınması suretiyle ihlal edilmesi halinde cezanın alt sınırının bir yıldan az olamayacağı belirtilerek bir nitelikli hal düzenlenmiştir. Bu benzerlik dolayısıyla söz konusu ağırlaştırıcı nedenin internet teknolojisinin geldiği nokta da dikkate alınarak sadece kayda alınması değil kayda alınan özel yaşam unsurunun temininin de bu kapsam nitelikte düzenlenmesi gerektiği yönündeki açıklamamıza atıfta bulunuyoruz.

Maddenin ikinci fıkrasının ikinci cümlede fiilin basın yayın yoluyla işlenmesi durumu da ikinci fıkranın birinci cümlesinin nitelikli ağırlaştırılmış hali olarak düzenlenmiştir. Daha önce birçok kez vurgulandığı üzere 29.06.2005 tarih ve 5377 sayılı kanunla, bir çok maddede aynı anda düzenlenen suçun aleni işlenmesi ile basın yayın yoluyla işlenmesi durumuna el atılmış ve basın yayın yoluyla yapılan ifşanın aleniyet unsuru içerdiği kabul edildiğinden suçun basın yayın yoluyla işlenmesi madde metninden çıkarılmıştır. Burada ise suçun basın yayın yoluyla işlenmesi durumu ayrı düzenlendiği için bu cümle hükmünce yapılan ifşanın aleniyeti gerçekleştiren bir ifşa olduğu kabul edilmelidir. Yani yukarıda örnek olarak verilen e-posta aracılığıyla belli kişilere gönderilen içeriğin bir paylaşım sitesine veya bir foruma yüklenmesi ve kamusal erişilebilirliğin mümkün kılınması durumunda md. 134/2- c.2 gerçekleşmiş olur. Bu değerlendirmeden hareketle aynı zamanda ikinci fıkranın birinci ve ikinci cümlelerindeki düzenlemelerin kapsamı belirlenmiştir. Ancak yine de bu suç tipini ihdasla korumak istediği hukuksal değer dikkate alınacak ve özellikle de yukarıda üzerinde durulduğu gibi internet de dahil olmak üzere diğer tüm kitle iletişim araçlarının bu alandaki

etkililiği göz önünde bulundurulacak olursa, kanun koyucunun suç teşkil eden fillerin basın yayın aracılığıyla işlenmesi tercihinin yetersiz kalacağı kanaatindeyiz. Burada özel yaşamı ihlal suçuyla daha etkili ve kapsamlı mücadele için suçun alenen işlenmesinin düzenlenmesi daha isabetli olurdu.

Suçun özel görünüş şekilleri açısından md. 132’de düzenlenen haberleşmenin gizliliğini ihlal suçuna atıf yapmakla yetinilecektir. Çünkü anılan maddede yapılan açıklamalar dışında genel özel hayatın gizliliğini ihlal suçu yönünden ayrıca vurgulanması gereken bir nokta dışında özellikli bir duruma rastlanmamıştır. Bu nokta da 5237 sayılı TCK md. 42 hükmündeki bileşik suç⁵⁸⁸ ilişkindir. Bilindiği üzere biri diğerinin unsuru veya ağırlaştırıcı nedeni sayılan eylemler tek suç kabul edilmektedirler ve bunlar hakkında içtima hükümleri uygulanmamaktadır. Daha önce vurgulandığı ve aynı bölüm çerçevesinde değerlendirilecek suçlar için de geçerli olacağı üzere, ikinci kısım dokuzuncu bölümde yer alan tüm suçlar esasında özel yaşamın gizliliğini ihlal niteliğindeki suçlardır. Örneğin haberleşme gizliliğini ihlal suçu işlenirken zorunlu olarak özel yaşamın gizliliği suçu da işleniş olacaktır. Yine kişisel verilerin kaydedilmesi veya kaydedilen kişisel verilerin ele geçirilmeleri suçları da işlenirken mutlak suretle bir özel yaşam alanının ihlali söz konusu olacaktır. Özellikle maddenin düzenleniş tarzı da özel yaşamın hangi suretle olursa olsun ihlalini kapsadığı için bu yönde düşünmek bir gerekliliktir. Dikkat edilirse bu suçların işlenişinde özel hayatın gizliliğini ihlal bir unsur niteliğindedir. Bu çerçevede gerek işleniş tarzı itibarıyla özel hayatın gizliliğini otomatikman ihlal eden suçlarla md. 134 arasında bileşik suç hükmünün uygulanabilirliği de gözden ırak tutulmamalıdır.

1.3.- TCK’de Düzenlenen Bazı Müdahale Suçlarının Değerlendirilmesi

1.3.1.- Eğitim ve Öğretimin Engellenmesi

Bilgisayar ve internet teknolojilerindeki gelişmeler, gerek eğitimde, gerek eğitimin sınav boyutunda, bilgisayar ve internetin kullanılmasını vazgeçilmez bir duruma

⁵⁸⁸ MADDE 42. - (1) Biri diğerinin unsurunu veya ağırlaştırıcı nedenini oluşturması dolayısıyla tek fiil sayılan suça bileşik suç denir. Bu tür suçlarda içtima hükümleri uygulanmaz.

getirmektedirler. Dolayısıyla eğitim ve öğretimde internet'i kullanan yeni teknolojilere ve araçlara gereksinim duyulması, ve bunların devreye girmesi kaçınılmaz olmaktadır⁵⁸⁹.

Günümüzün gelişen teknolojisi ve değişen ihtiyaçları yaygın olarak kullanılan eğitim ve öğretim metotlarında değişiklikler yapmaktadır. Genelde öğrenci ve öğretmenin aynı zamanda ve aynı mekanda olmasını gerektiren ve öğretmenin hem kaynak hem de idareci rolünü üslendiği öğretim biçimleri artık yetersiz kalmakta, günümüzün başka sorumlulukları ya da kişisel tercihlerinden dolayı belli bir zaman ve mekanda olamayan öğrencilerin öğrenme ihtiyaçlarını karşılamamaktadır. İşlevsel olarak uzaktan eğitim çalışan, meşgul ve ihtiyaç duyduğunu hemen ve gerektiği kadar öğrenmek isteyenler için, istediği zamanda, yerde, miktarda ve hızda öğrenme imkanı sağlamak şeklinde tanımlanabilmektedir.⁵⁹⁰

İnternet, öğrenci ve öğretmeni bilgisayarlar yoluyla birbirine bağlayarak metin, veri, grafik ve metin gibi öğelerin paylaşıldığı elektronik ortamlar oluşturur⁵⁹¹. Pek çok kurum ve organizasyon, bilgisayar ağları ve interneti bir eğitim teknolojisi olarak kullanmaktadır. İnternet ya da intranet üzerinden çalışan belli bir zamandan ve mekandan bağımsız ağ tabanlı öğrenme programları genelde e-öğrenme kapsamı altında değerlendirilmektedir⁵⁹². E-öğrenme programları öğrenme malzemesi, iletişim, öğrenciye destek, dönüt verme ve değerlendirme gibi eğitsel etkinliklerin elektronik yollarla yapıldığı yeni iletişim ve etkileşim kanallarından oluşmaktadır. Tartışma listeleri, ağ sayfaları, ek yazılımlar, e-posta, forum, ağ üzerinden çoklu ortam, sanal sınıf, telekonferans ve video konferans, dijital-analog televizyon, telefon, ağ üzerinden öğrenme faaliyetlerinin gerçekleşmesini sağlayan bazı araçlardır⁵⁹³.

⁵⁸⁹ **ERKUNT**, Hamdi/ **AKPINAR**, Yavuz, İnternet Tabanlı ve İnternet Destekli Eğitim: Kurumsal Bir Eğitim Yönetim Sistemi Örneği, Kaynak: <http://cet.boun.edu.tr/faculty/erkunt/papers/AUUE2002bildiri.pdf> (Erişim Tarihi: 06.02.2008, Saat: 12:42)

⁵⁹⁰ Ayrıntılı değerlendirme için bkz. **GÜNDÜZ**, H. Coşkun/ **SEVİNÇ**, Emre, eMBA: İnternet Tabanlı Yükseköğretimde Başarılı Bir Sistem, Kaynak: <http://cs.bilgi.edu.tr/~cgunduz/emba-baku-makale.pdf> (Erişim Tarihi: 06.02.2008, Saat: 12:48)

⁵⁹¹ **DURU**, Nevcihan, Etkileşimli İnternet, in: Türkiye Bilişim Ansiklopedisi, sh: 381-382.

⁵⁹² **TUNCER**, Murat/ **TAŞPINAR**, Mehmet, Sanal Eğitim – Öğretim ve Geleceği, in: Elektronik Sosyal Bilimler Dergisi, Cilt: 6 – Sayı: 20, 2007, sh: 119 (Kaynak: <http://www.e-sosder.com/dergi/20112-132.pdf>, Erişim Tarihi: 06.02.2008, Saat: 13:00)

⁵⁹³ Türkiye'deki Bazı Uzaktan Eğitim Sistemleri ve Alanları: Bu alandaki çalışmalardan biri, ODTÜ'de 1998 yılında başlayan ve Enformatik Enstitüsü bünyesinde gerçekleştirilmeye çalışılan METU-Online projesidir. Bu proje kapsamında, değişik bölümlere ait lisans ve yüksek lisans dersleri uzaktan eğitim vermek üzere açılmıştır. ODTÜ'de yürütülen bir diğer çalışma ise IDE-AS (İnternete Dayalı Eğitim– Asenkron/Senkron) Öğretim Teknolojileri Sertifika Programı'dır. Bu proje ODTÜSEM (Sürekli Eğitim Merkezi)'nin idari ve ODTÜ Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü'nün akademik sorumluluğunda yürütülmektedir. Projenin amacı, asgari lise/meslek lisesi mezunu gençleri, öğretim teknolojileri konusunda eğitmek ve bu alanda

İnternet destekli veya internete dayalı eğitim – öğretim faaliyetlerinin bu denli geliştiği ve yaygınlaştığı bir durumda hiç şüphe yok ki eğitim ve öğretim özgürlüğünün ihlal edilebilirliği ve bunun engellenmesi için yapılacak düzenlemelerin interneti de içine alan bir düzlemde tartışılması gerekmektedir. Bu anlamda TCK md. 112⁵⁹⁴, de düzenlenen eğitim ve öğretimin engellenmesi önem arz eden bir madde olarak görülmektedir.

Suçun maddi unsurunun internet açısından değerlendirilmesinde, TCK md. 112/1- a hükmünde, devletçe kurulan veya kamu makamlarının verdiği izne dayalı olarak yürütülen her türlü eğitim ve öğretim faaliyetinin engellenmesi cebir, şiddet veya hukuka aykırı bir davranışla gerçekleşebileceği düzenlendiği için⁵⁹⁵ özellikle internet destekli eğitim ve öğretim faaliyetlerinin hukuka aykırı müdahalelerle engellenmesi durumunda anılan suçun internet aracılığıyla da işlenebileceğinden şüphe yoktur. Özellikle modern toplumlarda internet sosyal bir takım süreçlerin daha da kolaylaştırılmasında önemli rol oynamaktadır. Bunlardan biri de eğitim sektörüdür. Uzaktan eğitim ve öğretim ihtiyacına paralel olarak geliştirilen

ülkemizin ihtiyaç duyduğu uzman açığını gidermektir. Yine ODTÜ’de, ODTÜ Sürekli Eğitim Merkezi'nin idari ve ODTÜ Bilgi İşlem Merkezi'nin teknik desteği ile sürdürülen IDE-A(Internete Dayalı Eğitim – Asenkron) programı, bilgi teknolojileri ya da bilgisayar mühendisliği dersi alamamış ancak bu konuya ilgi duyan, kendisini geliştirmek isteyen ve bu alanda çalışmak isteyen kişilere katkıda bulunmayı amaçlamaktadır. IDE-A projesi kapsamında verilmekte olan, Bilgi Teknolojileri Sertifika Programı'ndan bağımsız dersler de vardır. ODTÜ Enformatik Enstitüsü tarafından 2000 yılında, Informatics-Online yüksek lisans programı başlatılmıştır. ODTÜ Yabancı Diller Yüksek Okulu, İngilizce dilini geliştirmeyi arzu eden herkes için "Distance Interactive Learning - diL" programını hazırlamıştır. "diL" internet üzerinden etkileşimli bir İngilizce dil eğitimi programıdır. Dünyada ve Türkiye’de türünün ilk örnekleri arasında olan bu program, ODTÜ/Yabancı Diller Yüksek Okulu ve ODTÜ/Teknopark A.S. ile GANTEK Teknoloji bünyesinde faaliyet gösteren TEMA Bilişim Hizmetleri ve Ticaret A.S. işbirliği sonucu ortaya çıkmıştır. Ülkemizde gerçekleştirilmeye çalışılan bir başka proje ise Sakarya Üniversitesi’ nin IDÖ(Internet Destekli Öğretim) projesidir. 2000 yılında başlamış olan bu proje kapsamında bazı dersler sanal ortamda verilmektedir. Selçuk Üniversitesi de ülkemizde uzaktan eğitim projesi başlatan üniversitelerimizdendir. Üniversite, SUZEP adını verdiği bu proje kapsamında, şimdilik, sadece üç ders (Atatürk İlkeleri ve İnkılap Tarihi, Türk Dili ve İngilizce) sanal ortamda vermektedir. İstanbul Bilgi Üniversitesi'nin gerçekleştirdiği BILGI e-MBA, Türkiye'nin internet üzerinden erişilen ilk Lisansüstü İşletme Yönetimi Programı'dır. e-MBA adlı program, internet üzerinden interaktif ders yapılması esasına dayanmaktadır. 50 kişilik sanal sınıflarda yapılan dersler, zaman ve mekan kısıtlamasını ortadan kaldırmaktadır. 2000-2001 akademik yılı güz döneminde başlayan bu programa katılan bütün öğrencilere, eğitimin aksamaması için, bir standart erişim-öğrenim paketi verilmektedir. Eğitim ücretine dahil olan paketin içinde bilgisayar, yazıcı, e-MBA için gerekli olan tüm ders kitapları, cd, dvd, video kasetler bulunmaktadır. İstanbul Teknik Üniversitesi'nin UNESCO desteği ile başlatıp yapılandırdığı Uzaktan Öğretim Projesi, ülkemizde yeni kurulan üniversitelere destek vermek, Orta Asya Türk Cumhuriyetleri'nde yüksek öğretime katkıda bulunmak ve Doğu Avrupa ülkeleri ile yüksek öğretimde işbirliği yapmak amaçlarını taşımaktadır. Projenin gerçekleştirilmesi için çalışmalar sürdürülmektedir. Kaynak: http://www.ceng.metu.edu.tr/~e1448737/ceit321/proje/week1_reading_2.pdf (Erişim Tarihi: 06.02.2008, Saat: 13:10)

⁵⁹⁴ **MADDE 112.** - (1) Cebir veya tehdit kullanılarak ya da hukuka aykırı başka bir davranışla;

- Devletçe kurulan veya kamu makamlarının verdiği izne dayalı olarak yürütülen her türlü eğitim ve öğretim faaliyetlerine,
- Öğrencilerin toplu olarak oturdukları binalara veya bunların eklentilerine girilmesine veya orada kalınmasına, engel olunması hâlinde, bir yıldan üç yıla kadar hapis cezasına hükmolunur.

⁵⁹⁵ **ARTUK/ GÖKCEN/ YENİDÜNYA**, Ceza Hukuku Özel Hükümler, sh: 206- 207.

teknolojilerle öğrenciler internet aracılığıyla uzaktan eğitim ve öğretimlerini yerine getirmektedirler.

Ülkemizde ve dünyada bu tarz eğitim ve öğretim faaliyetlerinin örneklerine rastlanmaktadır. Örneğin verilen kullanıcı adı ve şifreyle öğrenci internet üzerinden eğitim ve öğretim materyallerinin ve uygulamalarının bulunduğu portala ulaşmakta, burada bireysel eğitim faaliyetleri yürütebileceği gibi görüntülü ve sesli multimedya olanakları ile grup çalışması ve hatta sanal sınıflarında ders dahi yapabilmektedirler⁵⁹⁶. Önümüzdeki yıllarda bu tarz uygulamalar daha sıklıkla karşılaşılan ve tercih edilen uygulamalar olacaktır. Madde metninde devletçe kurulan ve kamu makamlarının verdiği izinle yürütülen her türlü eğitim öğretim faaliyetleri denildiğine göre belirlenen şartları yerine getiren dershaneler, özel eğitim kurumları, sertifika programları ve benzeri her türlü eğitim öğretim faaliyeti yürüten birimler bu düzenlemenin güvencesi altında değerlendirilmelidir.

112. madde kapsamında internet aracılığıyla eğitim ve öğretimin engellenmesinde üzerinde durulması gereken önemli bir problemlilik nokta dikkati çekmektedir. İnternet ortamında gerçekleştirilen eğitim ve öğretim faaliyetlerine dışarıdan yetkisiz ve hukuka aykırı olarak gerçekleştirilen bir müdahale ile (hacking, virüs saldırıları... v.b.) sisteme erişimin tamamen engellenmesi veya sistemin düzenli çalışmamasına neden olunması durumunda bir problem görünmemektedir. Ancak bir eğitim öğretim kurumunca internete oluşturulan portala erişim mümkünken bu portalda yer alan herhangi bir eğitim ve öğretim unsuruna ilişkin linke (online – çevrimiçi - ders notları, uygulamalar, sınavlar veya not görüntüleme, v.b.) dışarıdan yetkisiz herhangi bir müdahale ile erişimin engellenmesi durumunda veya erişim mümkün iken düzenli çalışmasının engellenmesi durumunda kısmi bir engelleme söz konusu olacaktır. Dolayısıyla internet ortamında eğitim ve öğretim faaliyeti sadece bir unsuru dışında sorunsuz devam etmekte olacaktır. Böyle bir durumda eğitim ve öğretim işlerliğinin ne derece engellendiği tartışma konusu olmaktadır. Keza madde gerekçesi de bu konu ile ilgili herhangi açıklamaya yer vermemiştir.

Bu anlamda kanaatimizce madde metninde internet başta olmak üzere modern eğitim destek üniteleri de dikkate alınmak suretiyle md. 243’de yapılan düzenlemeye paralel olarak “eğitim ve öğretim faaliyetinin kısmen veya tamamen engellenmesi”

⁵⁹⁶ ÇAKIR, Hüseyin/ YALÇIN, Nursel, İnternet ve İntanete Dayalı Sanal Dersane Sistemi, Kaynak: <http://www.ksef.gazi.edu.tr/dergi/pdf/Cilt-14-No1-2006Mart/101-112.pdf> (Erişim Tarihi: 06.02.2008, Saat: 13:24).

kavramının kullanılması bu tarz karışıklıkların ortadan kaldırılması bakımından yerinde olacaktır. Çünkü bir bilişim sistemi olarak internet destekli veya internete dayalı eğitim sistemlerine kısmen veya tamamen müdahalelerde bulunulabilmekte, bu nedenle eğitim kısmen veya tamamen engellenebilmektedir. Kanun koyucu tarafından eğitim ve öğretim faaliyetlerinin engellenmesinden neyin kastedildiği açıklığa kavuşturulmadığı için, eğitim ve öğretim faaliyetinin asli veya tali unsurlarına kısmi bir erişim engellemenin bu kapsamda değerlendirilip değerlendirilmeyeceği bir sorun olarak ortaya çıkacaktır. **Bunun önüne geçmenin en önemli yolu da eğitim öğretim faaliyetlerinin kısmen veya tamamen engellenmesinin açıkça dile getirilmesidir. Bu açıdan maddenin internet teknolojisinin gelişim seyri dikkate alınarak gözden geçirilmesi gerektiği kanaatindeyiz.**

Suçun *kusurluluk unsurunun* internet açısından değerlendirilmesinde özellikli bir duruma rastlanmamıştır. Suç kasten işlenen bir suçtur. Suçun yapısı itibariyle özel kastı gerektirecek herhangi bir neden yoktur. Bunun yanında olası kastla hareket edilebilmesinin mümkün olduğu da söylenebilir. Kusurluluğu etkileyen nedenler bakımından ise, suçun internet açısından işlenebilen hali bakımından özellikli bir hususa rastlanmamıştır.

Hukuka aykırılık unsuru bakımından ise özellikle 04.05.2007 tarih ve 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunun yürürlüğe girmesinden itibaren daha da netleşen erişimin engellenmesi eylemlerinin bu çerçevede değerlendirilmesi gerekmektedir. Şayet md. 8/1’de sayılan suçların internet aracılığıyla işlendiği yönünde yeterli şüphe varsa söz konusu yayına erişimin engellenmesine karar verilebilir. Erişimin engellenmesi prosedürü de ikinci ve devamındaki fıkralarda aktarılmıştır. Buna göre erişimin engellenmesi kararı, soruşturma evresinde hâkim, kovuşturma evresinde ise mahkeme tarafından verilir. Soruşturma evresinde, gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısı tarafından da erişimin engellenmesine karar verilebilir. Bu durumda Cumhuriyet savcısı kararını yirmidört saat içinde hâkimin onayına sunar ve hâkim, kararını en geç yirmidört saat içinde verir. Bu süre içinde kararın onaylanmaması halinde tedbir, Cumhuriyet savcısı tarafından derhal kaldırılır. Hâkim, mahkeme veya Cumhuriyet savcısı tarafından verilen erişimin engellenmesi kararının birer örneği, gereği yapılmak üzere Başkanlığa gönderilir. İçeriği birinci fıkrada belirtilen suçları oluşturan yayınların içerik veya yer sağlayıcısının yurt dışında bulunması halinde veya içerik veya yer sağlayıcısı yurt içinde bulursa bile, içeriği birinci fıkranın (a) bendinin (2) ve (5) numaralı alt bentlerinde yazılı suçları oluşturan yayınlara ilişkin olarak erişimin engellenmesi kararı re’sen Başkanlık tarafından verilir. Bu karar, erişim sağlayıcısına bildirilerek gereğinin

yerine getirilmesi istenir. Bu çerçevede şartları oluşturulmuş bir erişimin engellenmesi kararının icrası, TCK md. 112 kapsamında herhangi bir eğitim ve öğretim faaliyetinin engellenmesi kapsamına girse bile hukuka aykırılık teşkil etmeyecektir.

Suçun *özel görünüş şekillerinin* internet açısından değerlendirilmesinde; söz konusu suç, karakteri gereği müdahale suçu olarak kategorize edilebilecek bir suç olduğundan, bu suçlar bakımından genel olarak söylendiği üzere *teşebbüse* elverişlidir. Çünkü internet ortamında gerçekleşen müdahale suçlarında hareketin bölünebilirliği sıklıkla söz konusudur.

İçtima konusunda ise, özellikle bu suç bakımından zincirleme suçla ve fikri içtima ile karşılaşmak mümkündür. Örneğin, aynı suç işleme kararıyla bir eğitim öğretim kurumunun internet üzerinden eğitim amaçlı oluşturduğu portalın faaliyetlerinin defaetle engellenmesi ya da bir defa işlenmesi durumunda dahi tek bir hacking eylemi ile birden fazla öğrencinin söz konusu portaldan yararlanmasının engellenmesi halinde bir zincirleme suçun varlığından bahsetmek mümkündür. Bunun yanında yukarıda aktarıldığı üzere internete dayalı veya internet destekli eğitim sistemlerinde sanal ders ortamı yaratılabilmekte ve öğretmen – öğrenciler eş zamanlı olarak yazıyla veya görüntülü – sesli olarak iletişime geçmek suretiyle ders işleyebilmektedirler. Dışarıdan gerçekleşecek bir müdahale ile bu iletişim imkanı ortadan kaldırılacak olursa tek bir hareketle başta md. 112 olmak üzere, md. 243 çerçevesinde bir bilişim sistemine yetkisiz erişim suçu ve şartları gerçekleştiyse md. 244 çerçevesinde bilişim sistemine zarar verilmesi hatta md. 124 anlamında bireysel ve/veya kitlesel haberleşmenin engellenmesi söz konusu olabilecek, böylece TCK md. 44 çerçevesinde fikri içtima koşulları oluşabilecektir.

1.3.2.- Kişinin Huzur ve Sükununu Bozma

TCK md. 123⁵⁹⁷, de düzenlenen suç tipi de internet aracılığıyla sıklıkla işlenen bir suç tipidir. Maddenin düzenleniş şekline bakılacak olursa; daha önce incelenen tehdit, cinsel taciz, şantaj gibi suç tipleri ile benzerlik göstermekle beraber eylemin sırf rahatsız etmeye yönelik olması, bir başka ifade ile özel bir amaca yönelik olmaması, nedeniyle tamamlayıcı bir norm

⁵⁹⁷ **MADDE 123.** - (1) Sırf huzur ve sükûnunu bozmak maksadıyla bir kimseye ısrarla; telefon edilmesi, gürültü yapılması ya da aynı maksatla hukuka aykırı başka bir davranışta bulunulması hâlinde, mağdurun şikâyeti üzerine faile üç aydan bir yıla kadar hapis cezası verilir.

olarak düzenlendiğini söylemek mümkündür. Bu açıdan maddenin tesisi yerindedir. Ancak maddenin düzenlenişi eleştiriye açıktır. Özellikle de internet açısından madde değerlendirildiğinde bu eleştiriler daha da net bir biçimde dikkati çekmektedir.

Anılan maddenin düzenlendiği yer itibariyle hürriyet aleyhine işlenen bir suç olduğundan şüphe yoktur. Zaten benzer nitelikteki diğer suç tiplerine bakıldığında da onlarında hürriyet aleyhine işlendiği görülmektedir. O bakımından bu düzenlemeyle *korunması amaçlanan hukuksal değer*in kişinin huzur ve sükun içinde yaşama hakkı olduğu söylenebilir⁵⁹⁸. Maddenin tamamlayıcı bir norm hükmünde olması nedeniyle koruma kapsamının da böyle geniş tutulmasında yarar olduğu kanaatindeyiz.

Suçun *maddi unsuru* internet açısından değerlendirilirken eleştiriye açık bir takım noktalar tespit edilmiştir. Bu anlamda önemli bir eleştiri noktası şöyle özetlenebilir; Madde metninde suçun gerçekleşmesi için kişinin huzur ve sükununu bozmak maksadıyla ısrarla telefon edilmesi, gürültü yapılması veya aynı maksatla hukuka aykırı başka bir davranışta bulunulması aranmaktadır. Bu düzenlemeden hareketle, söz konusu suçun maddi unsurunun gerçekleşebilmesi için telefon etmek⁵⁹⁹ ve gürültü yapmak dışında ancak hukuka aykırı bir davranışta bulunulması gerektiği anlaşılmaktadır. Dolayısıyla hukuka aykırılık teşkil etmeyen bir davranışla ısrarla kişinin huzurunu ve gündelik yaşamdaki sükununu bozacak davranış suç teşkil etmeyecektir. Ancak telefon etmek örneğinde de görüldüğü üzere bu suça neden olan tüm davranışlar bizatihi hukuka aykırılık teşkil etmeyebilir. Burada bu hareketlerin ısrarla yapılması ve sırf kişilerin huzurunu ve sükununu bozmaya yönelik olmaları halinde bir hukuka aykırılığın ortaya çıkacağı kabul edilmedir. Bu açıdan kanun koyucunun söz konusu suçun gerçekleşmesi için hukuka aykırı bir davranışı arama kaygısını yerinde bulmamaktayız.

Bu eleştiri internet aracılığıyla gerçekleştirilen huzur ve sükun bozma eylemlerinde daha da belirgin bir biçimde görülmektedir. Örneğin bir kişinin posta adresine kendi isteği dışında sürekli spam posta⁶⁰⁰ gönderilmesi eylemi dikkate alınacak olursa, spam posta

⁵⁹⁸ Konu ile ilgili eleştiriler için bkz. ŞEN, Ersan, Hürriyete Karşı İşlenen Suçlar, in: Yeditepe Üniversitesi Hukuk Fakültesi Dergisi, Cilt:II Sayı:2, 2005, sh: 390.

⁵⁹⁹ Yargıtay telefonla rahatsız etmeye yönelik verdiği aşağıdaki karar örnek olarak gösterilebilir: “ Saniğin, müşterinin ev telefonunu birçok kez arayıp bir şey söylemeden kapatarak rahatsız ettiği, PTT tespit tutanağı, müşteki ve tanık anlatımları ile ispatlanmıştır. Saniğin söz konusu eylemleri itidal ve muvazene dışı harekette bulunma suçunu oluşturur.”, Yargıtay 5. CD. 27.03.2003, E: 2003/450, K: 2003/1533, MEYDAN/ YAPAL, İçtihatlı Türk Ceza Kanunu, sh: 2071’den naklen.

⁶⁰⁰ Memiş, Spamming niteliği taşıyan kitlesel posta gönderilerinin hukuki boyutunu karşılaştırmalı olarak incelerken “Spam” kavramına ilişkin tanımlama çabalarını naklen şöyle ifade etmektedir. “Spam kelimesi,

göndermek eylemini hukuka aykırı kılan bir normatif düzenleme yoktur. Ancak bu postaların posta kullanıcılarına rahatsızlık verecek, bilgisayar ve internet üzerinde işlem yapmasını engelleyecek derecede sürekli ve bol miktarda gönderilebilirliği karşısında, posta kullanıcısının bu spam postalar nedeniyle posta adresinin istediği işlerlikte kullanamaması kullanıcının gerek gündelik gerekse de çalışırken iş huzurunu ve sükununu bozacak nitelikte bir neticeye vücut vermektedir. Bu durumda, görünüşte bu eylem TCK md. 123 anlamında kişilerin huzurunu ve sükununu bozmak suçuna vücut veriyor gibi görünse de suçun telefon açılması veya gürültü yapılması suretiyle işlenmemesi ve bunlar dışında hukuka aykırı bir davranış aranmasına rağmen spam posta gönderilmesini hukuka aykırı kılan bir düzenleme olmadığından bu eylem bakımından TCK md. 123 bir güvence teşkil etmeyecektir. Keza aynı örneği kullanıcıya korkunç, psikolojik açıdan kendisini olumsuz etkileyebilecek ve hatta mobbing⁶⁰¹ etkisi yaratabilecek içerikte e-posta ve benzeri iletiler gönderilmesi, kullanıcı

Amerikan kökenli bir kelime olup, ilk defa Firma Hormel Foods Corporation'un bir kutu içinde baharatlı domuz eti ve jambon için kullandığı bir kısaltmadır. "Spiced pork and ham" kelimelerinin ilk harflerinden oluşmaktadır. Şimdiye kadar da bilgisayarlar için hiç kullanılmamıştır. Sonraları e-posta yolu ile kitlelere reklam yapılmasında kullanılmaya başlanmıştır. Birden fazla kimseye elektronik posta yolu ile gönderilen bu tür reklamlar "spamming" olarak isimlendirilmektedir. Spamming'in değişik tanımlarını yapmak mümkündür. Avusturya İnternet Kullanıcılarının sitesi olan VIBE'de spamming için bir kanun kuralı öngörülmüş ve spam için "e-posta formunda rahatsız edici, sıkıntı verici haberler" tanımı getirilmiştir. Bu tanıda ayrıca içerik tanımı da ayrıntılı bir şekilde verilmiştir. İçerik sansürünün bağımsız bir iletişim aracı olan internette reddedilmesi dolayısıyla, spam da içeriğe göre tanımlanamaz. İçerik, daima bir değer taşımaya karşılık, bu değer daima subjektif ve kültürel olarak değişebilmekte; birine göre iyi olarak değerlendirilebilen şeyler bir başkası tarafından kötü olarak görülebilmektedir. Dolayısıyla içeriğe göre bir spam değerlendirilmesine varılamamaktadır. Spam objektif kriterlere göre tanımlanmalıdır. Fransız Ulusal Enformasyon ve Özgürlük Komisyonu'na göre (Commission Nationale de l'Informatique et des Libertés) spam, hiçbir temas olmaksızın tartışma forumlarından, dağıtılan listelerden ve web sayfalarından elde edilen elektronik adreslere alıcının talebi olmaksızın ara-sıra büyük hacimlerde gönderilen ve ticari amaç taşıyan e-postalardır. Uluslararası Ticaret Örgütü'nün 1996 yılında yayınlamış olduğu "ICC Guidelines on Interactive Marketing Communication" da da spamın tanımına rastlamak mümkündür. Buna göre, spam, bir bülten veya haber grubu üzerinden ticari amaç taşımayanbu forum konularında olmayan ve gönderilmesine açıkça izin verilmeyen reklamlardır." Ayrıntılı değerlendirme için bkz. MEMİŞ, Tekin, Hukuki Açıdan Kitlelere E- Posta Gönderilmesi (Spamming), Kaynak: <http://inet-tr.org.tr/inetconf7/bildiriler/12.doc> (Erişim Tarihi: 06.02.2008, Saat: 14:00). Türk Ceza Hukukunda spam postaların cezalandırılabilirliği tartışmaları için bkz. ÜNVER, TCK ve CK Tasarısı'nın İnternet Açısından Değerlendirilmesi, sh: 110 v.d.

⁶⁰¹ Mobbing, iş yerindeki bir kişinin ya da bir grubun diğer çalışanlar tarafından rahatsız edilmesi, hakarete uğraması ve en sonunda çalışamaz duruma getirilmesi anlamına geliyor. Özellikle hiyerarşik yapılanmış gruplarda ve kontrolün zayıf olduğu örgütlerde, gücü elinde bulunduran kişinin ya da grubun, diğerlerine psikolojik yollardan, uzun süreli sistematik baskı uygulamasıdır. Son dönemde sosyoloji ve hukuk başta olmak üzere çeşitli alanlarda disiplinler arası çalışılan bir konu haline gelmiştir. Mobbing sözcüğü önceleri çocukların birbiriyle olan zorbalık ilişkilerini tanımlamakta kullanılmıştır. İşyerlerinde de 1950-1960'lı yıllarda yapılan araştırmalar, mobbingin sadece çocuklar arasında yaşanmadığını ortaya koymuştur. Mobbing duygusal bir saldırdır. Yaş, ırk, cinsiyet ayrımı gözetmeden, taciz, rahatsız etme ve kötü davranış yoluyla herhangi bir kişiye yönelen saldırganlıktır. Kişiyi iş yaşamından dışlamak amacıyla kasıtlı olarak yapılır. Kişinin saygısız ve zararlı bir davranışın hedefi olmasıyla başlar. İşveren ima ve alayla, karşındakinin toplumsal itibarını düşürmeye yönelik saldırgan bir ortam yaratarak kişiyi işten ayrılmaya zorlar. Bir araştırmaya göre mobbing, kâr amacı gütmeyen kuruluşlarda, okullarda ve sağlık sektöründe daha yaygındır. Mobbing kavramı bununla sınırlı olmayıp Konunun farklı boyutlarıyla birlikte ele alındığı ve konu ile ilgili olarak daha ayrıntılı bilgi için bkz. <http://www.turk.internet.com/abone/login.php?l=2&location=/haber/yazigoster.php3?yaziid=6752> (Erişim Tarihi: 10/12/2007)

tarafından her defasında engellenmesine rağmen farklı kullanıcı adıyla bir kişinin internet aracılığıyla kurduğu iletişime dahil olmaya çalışan kişinin eylemi bakımından da düşünmek mümkündür. **Bu tarz karışıklıkları önlemek ve teknolojik gelişmelerin gerisinde kalan bir yoruma sağlanmamak için madde metnindeki “ hukuka aykırı ” kavramının kaldırılmasını ve bu neticeyi doğurabilecek her türlü davranışı bu kapsamda değerlendirilmesine olanak sağlanmasını önermekteyiz.** Aksi takdirde maddenin muhafazasının bir anlamı kalmayacaktır⁶⁰². Bu yüzden maddenin teknolojisinin gelişim seyri dikkate alınarak yeniden gözden geçirilmesi gerektiği görülmektedir.

Manevi unsur açısından değerlendirilecek olursa, öncelikle suçun özel kastla işleneceği söylenebilir. Bilindiği gibi failin suçu işlerken özellikle belli bir saikle hareket etmesinin arandığı durumlarda özel kasttan bahsedilmektedir⁶⁰³. Bu suç tipinde de kanun koyusu ısrarla edilen telefonların, çıkartılan gürültünün veya hukuka aykırı başka bir davranışın özellikle kişilerin huzur ve sükununu bozmak amacıyla yapılmasını aradığı için bir özel kastın varlığı söz konusudur. Suçun işlenişinde ısrar etmek anlamında bir sürekliliğin aranması ve özel olarak kişinin huzur ve sükununun hedef alınması nedeniyle bu suçun olası kastla işlenemeyeceği söylenebilir.

Suçun özel görünüş şekilleri internet açısından ele alınacak olursa, kişilerin huzur ve sükunlarını bozmak suçu nitelik itibariyle hem içerik hem de müdahale suçu⁶⁰⁴ olarak görünüm kazanabilecek tarzda bir suç tipidir. Ancak suçun *teşebbüse* elverişliliği tartışılırken suçun içerik suçu veya müdahale suçu olup olmamasına bakılmamalıdır. Çünkü her iki suç türünde de kanun koyucu ısrar şeklinde görünen bir süreklilik aradığı için bu sürekliliğin sağlanamaması, daha doğru bir ifade ile yarıda kesilmesi durumunda anılan suça teşebbüsün varlığından bahsedilebilecektir. Ancak bu durumda ısrar olarak aranan süreklilikten neyin kastedildiği ve hangi noktada suçun oluştuğu hangi noktada teşebbüs aşamasında kalacağı hususu muğlak bırakılmıştır. Suçun internet üzerinden işlenebilen şekli bakımından *iştirakin* her şeklinin gerçekleşebileceği söylenebilir.

⁶⁰² Bu değerlendirme de özünde madde tesisindeki iradenin bir devamı olarak yansıtılmaktadır. Şöyle ki; Bu maddenin karşılığı 765 sayılı TCK.nun 546 ve 547 inci maddelerinde kabahat nev'inden bir suç olarak mevcuttur. 5237 sayılı TCK bilindiği gibi cürüm ve kabahat ayrımını ortadan kaldırmış, kural olarak kabahatlerin suç olmaktan çıkarmıştır. Bununla birlikte önem arz eden bazı kabahatlere yeni TCK da yer verilmiştir. İşte bunlardan biri de 5237 sayılı TCK md. 123 üncü maddesindeki suçtur.

⁶⁰³ ÖZBEK, İzmir Şerhi, sh: 283.

⁶⁰⁴ İnternet aracılığıyla işlenen suçlara ilişkin sınıflandırma ile ilgili bkz. İkinci Bölüm, § 1.- İnternet Ortamında İşlenebilen Suçların Sınıflandırılma Sorunu.

İçtima konusunda ise suçun fail tarafından aynı suç işleme kararıyla birden fazla kişiye değişik zamanlarda tek bir fiille (örneğin herkese aynı içerikli e- postaların gönderilmesi, sadece kişinin huzuru kaçırmak için MSN, ICQ gibi kişisel iletişim araçlarının sık sık hacklenmesi ve daha sonra bunların kullanıcılarına iade edilmesi, v.b.) işlenmesi durumunda TCK md. 43 anlamında zincirleme suçtan bahsetmek mümkündür. Bunun yanında kişinin huzuru ve sükununu bozmaya elverişli bir eylem aynı zamanda kanunun başka hükümlerini de ihlal ediyorsa, örneğin hakaret, haberleşmenin gizliliğini ihlal, haberleşmenin engellenmesi, bilişim sistemlerine yetkisiz erişim gibi, burada TCK md. 44 anlamında fikri içtimanın gerçekleşmesi aranmalıdır.

Ancak dikkat edilmesi gereken önemli bir husus suç teşkil eden eylemin farklılaşmadan kanunun diğer hükümlerini ihlal etmesi gereğidir. Örneğin bir kişinin e- posta ve ya MSN adresine yetkisiz erişim sağlandıktan (hacklendikten)⁶⁰⁵ sonra hakaret ve iftira içerikli mesajlar bırakıldığında, bu suretle de kişinin huzur ve sükunu bozulursa burada irdelenmesi gereken kişinin huzur sükununun ne zaman bozulduğudur. **Kanaatimizce bu örnekte, bir kişinin e- posta veya MSN adresine yetkisiz erişim başlı başına kişi huzur ve sükununu bozacak niteliktedir. Bu anlamda aynı bağlamda değerlendirilecek olan TCK md. 243 kapsamında bir bilişim sistemine yetkisiz erişim suçu ile arasında TCK md. 44 anlamında fikri içtimadan bahsedilebilir. Yalnız artık bu noktadan sonra ayrıca hakaret veya sövme suçunu teşkil edecek bir davranışta bulunulması halinde harekette farklılaşma kabul edilmeli ve hareket tür ve adedince suçun işlendiği kabul edilmelidir.**

Bunun dışında günümüzde kişilerin internet üzerinden takip edilmeleri, haklarında tüm bilgilerin toplanması ve herhangi bir özel saike yönelmeden sadece kişinin huzur ve sükununu bozacak şekilde tabiri caizse her komutta karşlarına çıkması durumu “*cyber-stalking*” olarak adlandırılmaktadır ve gün geçtikçe de yaygınlık kazanmaktadır.⁶⁰⁶ “*Cyber – stalking*” kavram olarak temelini “*stalking*”den almaktadır. Türkçede kelime karşılığı gizlenerek avı kollama⁶⁰⁷ olan “*stalking*” esasında hukuksal bir kavram değildir. Ancak son yıllarda iletişim

⁶⁰⁵ Türk Ceza Hukukunda Hacking, Cracking ve Computer Trespass eylemlerinin cezalandırılabilirliği konusundaki görüşleri için bkz. ÜNVER, TCK ve CK Tasarısı'nın İnternet Açısından Değerlendirilmesi, sh: 107,

⁶⁰⁶ “Cyber – Stalking”in ceza hukukundaki görünümü ile ilgili değerlendirmeler için bkz. HILGENDORF/VALERIUS/FRANK, Computer- und Internet Strafrecht, sh: 199.

⁶⁰⁷ ÖZBALKAN, Nuri, Büyük İngilizce – Türkçe Genel Sözlük, Cilt:3, Ankara, 2000, sh: 2885.

olanaklarının artması ile birlikte kişilerin her noktada daha kolay erişilebilir olması, bunun kötüye kullanılmasını da beraberinde getirmiş, bu nedenle “*stalking*” kavramı da hukuksal bir içeriğe bürünmüştür⁶⁰⁸. Özellikle de bilişim teknolojilerindeki hızlı gelişim klasik anlamda telefonla rahatsızlık verme, mektupla tacizde bulunma, geçiş güzergahına kişide endişe, korku, huzursuzluk verecek belirteçlerin konulması veya sürekli izleme gibi fiillerin ikinci planda bırakılarak siber iletişim araçları ve olanakları ile gerçekleştirilen bezer nitelikli fiiller ön plana çıkmıştır⁶⁰⁹. Bunlar da ulusal ve uluslar arası hukuk mevzuatlarına, bilhassa da ceza hukuku mevzuatlarına aktarılmaya başlanmıştır. Bu noktada “*cyber- stalking*” ciddi bir öneme bürünmüştür. Bu kapsamda nitelendirilebilecek eylemler, her ne kadar kelime anlamı olarak “siber izleme” olarak tercüme edilse de bizce ceza hukuku anlamında “siber taciz” kavramı daha isabetli görünmektedir. Doktrinde bu kavramı doğrudan “tehdit” kapsamı altında değerlendiren yazarlara rastlanmaktadır⁶¹⁰. Ancak bu yaklaşıma katılmak güçtür. Çünkü “*stalking*” kavramı ceza hukuku bakımından teknik olarak tehdit fiilini karşılamamaktadır. Eylemin niteliği ve uygulanış tarzı bakımından ileride tehdit kapsamında değerlendirilebilir olması kavramın salt tehdiye indirgenmesini zorunlu kılmaz. Avustralya Kriminoloji Enstitüsü “siber taciz” üç başlık altında incelemenin gerektiğini vurgulamıştır⁶¹¹. Bunlar;

E- posta Aracılığıyla Taciz (E- posta Stalking)

İnternet Aracılığıyla Taciz (Internet Stalking)

Bilgisayar Aracılığıyla Taciz (Computer Stalking)

E- posta aracılığıyla taciz eylemlerinde, fail aynen telefonla gerçekleştirilen taciz eylemlerinde olduğu gibi mağduru aracısız olarak takip ederek tacizde bulunur ancak bir mektupla kurulan iletişimde söz konusu olan etki mesafesi de söz konusudur⁶¹². Günümüzde

⁶⁰⁸ Genel anlamda “*Stalking*” olgusu ile ilgili olarak ülkemizde detaylı ve sistematik bir inceleme yapılmamıştır. Alman hukukunun düşünce sistemi içinde bu kavramın algılanış ve uygulamaya yansıtılış tarzının ayrıntıları için bakımından bkz. **HEINRICH**, Bernd, Einführung eines Straftatbestands für das so genannte Stalking, Kaynak: <http://www.rewi.hu-berlin.de/jura/ls/hnr/lehre/studienarbeiten/stalking.pdf> (Erişim Tarihi: 06.02.2008, Saat: 15:46).

⁶⁰⁹ **HEINRICH**, Einführung, sh: 3; **MEYER**, Frank, Strafbarkeit und Strafwürdigkeit von “Stalking” im deutschen Recht, in: ZStW, 2003, 253- 254.

⁶¹⁰ Bkz. **YILDIZ**, Sevim, Suçta Araç Olarak İnternetin Teknik ve Hukuki Açından İncelenmesi, sh: 617, Kaynak: http://www.sosyalbil.selcuk.edu.tr/sos_mak/makaleler%5CSevil%20YILDIZ%5CYILDIZ,%20SEV%20C4%B0L.pdf (Erişim Tarihi: 06.02.2008, Saat: 15:14).

⁶¹¹ Avustralya Kriminoloji Enstitüsü (*Australian Institute of Criminology*) bünyesinde “Siber Taciz” ile ilgili olarak yapılan çalışmanın ayrıntıları için bkz. **OGILVIE**, Emma, Cyberstalking, Kaynak: <http://www.aic.gov.au/publications/tandi/ti166.pdf> (Erişim Tarihi: 06.02.2008, Saat: 15:31).

en çok kullanılan siber taciz araçlarından olan e- posta taraflar arasında özel iletişim kanalı hüviyeti dolayısıyla tercih edilmektedir. İnternet aracılığıyla taciz eylemleri gerçek dünyada yaşanan takip suretiyle tacizin sanal dünyadaki eşleniğidir. Sadece kullanılan araç bakımından bir sınırlama getirilmiştir. Bu tarz taciz eylemlerinde fail mağdurun internet ortamında işlem yaptığı, eriştiği her noktada (örneğin mağdurun takip ettiği forum sayfalarına, sohbet odalarına, profil veya paylaşım sitelerine yazılı, görüntülü, sesli iletiler, mesajlar bırakarak) adeta takipte bulunarak mağdurun huzur ve güvenini bozmaktadır. Son olarak da bilgisayar aracılığıyla taciz eylemleri vardır. Bu eylemler genellikle failin mağdurun kullandığı bilgisayara sürekli casus veya kötücül yazılımlarla saldırılarda bulunarak, mağdurda bir huzursuzluk yaratmak saikiyle gerçekleştirilmektedir. Bu tarz saldırılarda fail mağdurun bilişim sistemine bütünsel bir zarar vermeyi amaçlamamaktadır hatta mağdurun bilişim sisteminin kullanılmaz hale gelmesi fail tarafından ilk elde talep edilmeyen bir durumdur. Çünkü bu tarz saldırıların gerçek amacı mağdurun sürekli bir tehdit altında olduğu ve her an daha büyük saldırılara ve zararlara maruz kalabileceği hissiyatı içinde tedirginlik yaşamasıdır. **Dünyada son zamanlarda akademik olarak da ele alınan “Cyber Stalking”in ülkemizde de özellikle ceza hukuku alanda irdelenmesi gerektiği kanaatindeyiz⁶¹³.**

1.3.3.- Haberleşmenin Engellenmesi

Özellikle internet teknolojisindeki gelişimin kendini hissettirdiği en önemli yönlerinden biri sunduğu iletişim imkanlarındaki çeşitliliktir. Her geçen gün internet aracılığıyla bireysel veya kitlesel iletişimin daha da kolaylaştığı ve tercih edilir hale geldiği gözlemlenmektedir. Örnek vermek gerekirse, e-posta, sohbet odaları, forumlar, veri paylaşım siteleri, profil siteleri, sohbet programlarıyla görüntülü ve sesli iletişim bu imkanların başında gelmektedir⁶¹⁴. Bilgisayar sahibi olan kullanıcı sayısının artması, internet kafelerin çoğalması gibi nedenler de artık klasik iletişim araçlarının maliyet ve zaman açısından mevcut dezavantajları karşısında internetin sunduğu bu imkanlar herkese cazip gelmektedir. Bu bakımdan artık telefon, mektup gibi klasikleşen iletişim araçlarının yanında ve hatta belki de

⁶¹² STEPHAN, Nadine, Zum Phänomen und Zum Umgang mit Cyberstalking, sh: 4, Kaynak : <http://www.uni-bonn.de/~ujr701/Startseite/Texte/Vonwem/CyberCrime-CyberCrimeKontrolle-SS2003/SammlungCyberCrime/Stephan.pdf> (Erişim Tarihi: 06.02.2008, Saat: 15:35)

⁶¹³ Almanya'dan bir değerlendirme örneği olarak bkz. HILGENDORF, Eric/ HONG, Seung – Hee, Cyberstalking – Eine neue Variante der Internetkriminalität, in: Kommunikation & Recht, 2003, 168 v.d.

⁶¹⁴ DÜLGER, Bilişim Suçları, Ankara, 2004, sh:288.

öncelikle internet aracılığıyla yapılan iletişimin güvenceye alınması modern toplumun ihtiyaçlarına daha da uyumlu olacaktır⁶¹⁵.

İnternet bir çok yeni iletişim metoduna önyak olmuştur; örneğin, e-posta, canlı sohbet ve haber grupları. Fakat, internet aynı zamanda eski iletişim tarzlarının da kullanılmasını mümkün kılar: örneğin internet üzerinden telefon görüşmeleri yapılabilir⁶¹⁶. Bu imkanı sunan programlar vasıtasıyla iletişimin taraflarının sesleri paketlere bölünür. Bu paketler internetin TCP/IP protokolüyle iletilir. İnternet üzerinden telefon görüşmesi yapmanın iki yolu vardır. Birincisinde, bazı özel donanım ve yazılımlar kullanarak PC aracılığı ile telefon konuşmalarını yapılabilir. Genellikle *IP telephony* denilen ikincisinde ise, normal telefon aygıtıyla normal bir şekilde telefon ediyormuş gibi iletişim kurulabilir⁶¹⁷. Fakat burada görüşme normal telefon hattından değil İnternet hattından yapılır. İnternet üzerinden sesli ve görüntülü iletişimin en önemli tercih nedenlerinden biri maliyetinin düşük olmasıdır. Ödeme aynı bir web sitesine bağlanırken ya da e-posta gönderirken olduğu gibi sadece internete bağlanmak için yapılır. Bu anlamda internet üzerinden görüşme yapabilmek için kişinin bir internet erişim adresinin olması yeterlidir. PC'den internet aracılığıyla görüntülü ve sesli iletişime geçmek için değişik yöntem ve yazılım paketleri vardır. İletişimin kurulması için bir mikrofona konuşulmakta ve bir ses kartı ve hoparlör yardımıyla iletişimin diğer tarafının dijital sinyallere dönüştürülmüş sesi dinlenmektedir⁶¹⁸.

Yine internet üzerinde diğer insanlarla iletişim kurmanın en çabuk yollarından biri canlı sohbetlere (chat) katılmaktır. Aslında sohbetten konuşarak ve dinleyerek yapılan iletişim kastedilmemektedir. Bunun yerine, klavye kullanılarak canlı iletişim kurulur, yani bilgisayarınızda yazdığınız kelimeler, karşılıklı olarak, İnternet üzerindeki diğer kişinin bilgisayarında kişiyle aynı anda yapılabilmektedir.

İnternet üzerinde sohbet etmenin birçok yolu vardır. Her gün, dünyanın her köşesinden binlerce insan değişik konularda bu sohbet odaları aracılığıyla iletişim kurmaktadır. Her

⁶¹⁵ ÜZÜLMEZ, Yazışmaların İhlali Cürümü, sh: 155.

⁶¹⁶ Bir ağ üzerinden ses dalgalarının sıkıştırılmış veriler halinde transfer edilmesi işleminin teknik altyapısı ile ilgili bkz. ERZİN, Engin, Konuşma ve Ses Sıkıştırma, in: Türkiye Bilişim Ansiklopedisi (Baş Editörler: Tuncer ÖREN, Tuncer ÜNEY, Rifat ÇÖLKESEN), İstanbul, 2007, sh: 543 v.d.

⁶¹⁷ Ayrıntılı teknik bilgiler için bkz. <http://www.po.metu.edu.tr/links/inf/css25/bolum1.html> (Erişim Tarihi: 10.12.2007, Saat: 08:00).

⁶¹⁸ Ayrıntılı teknik bilgi için bkz. <http://www.po.metu.edu.tr/links/inf/css25/bolum5.html> (Erişim Tarihi: 10.12.2007, Saat: 08:05)

değişik konuya “*kanal*” veya “*oda*” adı verilen sanal ortamlar vardır. Bir sohbet odasına girildiğinde o odada bulunan diğer insanların her yazdığı herkes tarafından görülebilmektedir. Bunun yanında tek bir kişiyle de özel görüşmeler de yapılabilmektedir. Bu işlemler şöyle gerçekleşmektedir: Kullanıcının bilgisayarındaki söz konusu işlemi gerçekleştirmeye elverişli yazılım, internet üzerinden sunucuya bağlantı kurar. Bu yazılımı kullanılarak sunucuya bağlanılır ve istenilen bir sohbet odası seçilir. Bu sunucu küresel bir ağa bağlıdır. Daha sonra gönderilen iletiler ilgili sunucudan diğer sunuculara aktarılır. Böylece ileti o platformda bulunan diğer kullanıcılara ulaşır⁶¹⁹. Görüldüğü üzere internet gerek özel gerekse kitlesel haberleşmenin en kullanışlı ve hızlı aracı olarak kabul edilebilmektedir. Böyle bir durumda haliyle internet üzerinden kurulan haberleşmenin korunmasını da elzem kılmaktadır. Bu bakımdan TCK md. 124⁶²⁰,de düzenlenen haberleşmenin engellenmesi suçunu önem kazanmaktadır.

Haberleşmenin engellenmesi suçunda *fail* açısından herhangi bir özellikli durum yaratılmamıştır. Başka bir ifadeyle söz konusu suç tipi bakımından herkes bu suçun faili olabilecektir. Ancak *mağdur* bakımından her üç fıkrada üç ayrı suç düzenleme yoluna gidildiği için mağdurlar farklı olarak belirtilmiştir. Suçun birinci fıkrasında haberleşmenin tarafı olan herkes, ikinci fıkrasında kamu kurumları ve üçüncü fıkrasında ise basın yayın organları ve muhatapları mağdur olarak belirtilmiştir. Bunun yanında dikkat edilmesi gereken bir başka husus da bu suç tipinin mağduru bakımından, haberleşmenin engellenmesi en az iki taraf arasındaki ilişkinin engellenmesi anlamına geldiği için, ki kanun metninde kişiler arasındaki demek suretiyle bu husus vurgulanmıştır, haberleşme kaç kişi arasında gerçekleşiyorsa o kadar mağduru varlığı kabul edilmelidir. Örneğin madde gerekçesinde verilen örnekten hareket edilecek olursa posta kutusundaki mektupların yırtılması, bir kişiye gönderilen mektupların ilgisine verilmeyip çöp kutusuna atılması, telefon hatlarının kesilmesi, oluşturulan manyetik alanla telefon görüşmelerinin yapılamaz hâle getirilmesi gibi fiillerde sadece mektubu yırtılan veya çöpe atılan kişi değil o kişinin haberleşme kastıyla yöneldiği kişi de mağdur konumunda kabul edilmelidir.

⁶¹⁹ İnternet ortamında gerçekleşen gerçek zamanlı iletişim teknolojisinin alt yapısı için bkz. **ÇÖLKESEN/ÖRENCİK**, Bilgisayar Haberleşmesi, sh: 32.

⁶²⁰ **MADDE 124.** - (1) Kişiler arasındaki haberleşmenin hukuka aykırı olarak engellenmesi hâlinde, altı aydan iki yıla kadar hapis veya adli para cezasına hükmolunur.

(2) Kamu kurumları arasındaki haberleşmeyi hukuka aykırı olarak engelleyen kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır.

(3) Her türlü basın ve yayın organının yayınının hukuka aykırı bir şekilde engellenmesi hâlinde, ikinci fıkra hükmüne göre cezaya hükmolunur.

Haberleşmenin engellenmesi suçunun *maddi unsurunun* internet açısından değerlendirilirken ise şu noktalara dikkat edilmelidir; Haberleşmenin engellenmesinden neyin kastedildiği hususunda madde metninde genel bir tabir kullanmıştır. Buna göre haberleşme hangi suretle olursa olsun engellendiği takdirde suçun maddi unsuru gerçekleşmiş kabul edilir. Bu anlamda haberleşmenin hangi araçla yapıldığı veya haberleşmenin hangi araç vasıtasıyla ya da nasıl engellendiği suçun maddi unsuru bakımından bir önem arz etmemektedir. Önemli olan suçun haberleşmeyi mümkün kılan bir araca karşı gerçekleştirilmesi ve gerçekleştirilen eylemin iletişim olanaklarını ortadan kaldırmaya elverişli olması gerekmektedir. Örneğin eylemin yöneldiği iletişim aracı zaten bir haberleşmenin sağlanmasına elverişli değilse burada bir haberleşmenin engellenmesi suçundan bahsedilemez.

Maddenin birinci fıkrasında kişiler arasındaki haberleşmenin engellenmesi suçu düzenlenmiştir. Madde gerekçesinde bu suç tipi bakımından kastedilen haberleşmenin belirli kişiler arasındaki haberleşme olduğu özellikle vurgulanmıştır. Böyle bir vurgunun amacı kitle haberleşme araçlarıyla gerçekleştirilen haberleşmenin engellenmesi eylemini bu kapsam dışında tutma iradesidir. Yani bir kişinin posta adresinin, kullanıcı adı veya şifresinin yetkisiz bir müdahale ile değiştirilmesi veya herhangi bir şekilde, kullanımının engellenmesi, posta kutusundaki e- postaların kullanıcının iradesi dışında silinmesi, adres defterinde kayıtlı kullanıcıların irade dışı engellenmesi veya silinmesi, kişinin posta adresine çok sayıda spam posta göndermek suretiyle kapasitesinin dolmasına sebebiyet vermesi, yine diğer kişisel iletişim araçlarına karşı girişilen hacking eylemleri ile bunların kısmen veya tamamen kullanılamaz hale getirilmesi ve buna benzer hallerde kişiler arasındaki haberleşmenin engellenmesi söz konusu olacaktır.

Maddenin ikinci fıkrasında kamu kurumları arasındaki haberleşmenin hukuka aykırı olarak engellenmesi durumu düzenleme kapsamına alınmıştır. Bilindiği üzere son yıllarda kamu kurumları arasındaki işleyişte kırtasiyeciliğin önüne geçilmesi ve zaman ekonomisinin sağlanması amacıyla birçok işlem internet ortamında gerçekleşmektedir. Özellikle veri transferine dayalı internet üzerinden haberleşme olanakları sıklıkla kullanılmaktadır. Bu anlamda belli kurumlar arasında internet aracılığıyla gerçekleşen haberleşmenin engellenmesi durumunda anılan fıkra hükmü uygulanacaktır. Bu fıkranın uygulama örnekleri ile birinci fıkrada kişiler arasındaki haberleşmenin engellenmesi suçunda verilen örnekler hemen hemen aynıdır.

Maddenin üçüncü fıkrası yukarıda değinildiği üzere birinci fıkrada düzenlenen kişiler arası haberleşmenin engellenmesi suçu kapsamı dışında tutulan ve kitle haberleşme araçları vasıtasıyla gerçekleşen haberleşmenin engellenmesi suçu düzenlenmiştir. Fıkra hükmünde her türlü basın yayın organının yayını demek suretiyle TCK md. 6/1-g hükmünde tanımlanan tüm basın yayın organları kapsam dahiline alınmıştır⁶²¹. Buna göre gazete, radyo, televizyon, internet, v.b. kitle haberleşme araçlarının yayınlarının hukuka aykırı bir biçimde engellenmesi durumunda fıkra hükmünün uygulanabilirliği söz konusu olur⁶²². Konu internet açısından irdelenecek olursa, bir internet sayfasına - ki burada sohbet odaları, haber grupları, forumlar da dahil olmak üzere internette işlerliği bulunan tüm sayfalar kastedilmektedir- erişimin dışarıdan yapılan bir müdahale ile engellenmesi ya da kamusal erişilebilirliği mevcut bir verinin yetkisiz müdahale ile yok edilmesi bu kapsamda verilebilecek örnekler arasında sayılabilir. Maddenin birinci fıkrasında belirli kişiler arasında gerçekleşen haberleşmenin engellenmesi suçunun düzenlediği görülmektedir. Dolayısıyla bu fıkra anlamında aranması gereken en önemli husus tarafların belirlenebilirliğidir. Şayet engellenen haberleşme, belirsiz sayıda kişiyle yapılıyorsa veya yapılması amaçlanıyorsa üçüncü fıkra hükmü uygulanacaktır. Bu değerlendirme yapılırken ikinci bölümde internetin hangi bağlamda bir basın yayın aracı olduğuna ilişkin yapılan açıklamalar göz ardı edilmemelidir⁶²³.

Haberleşmenin engellenmesi suçunun *manevi unsuru* genel kasttır. Haberleşmenin hukuka aykırı olarak engellenmesinde bilme ve isteme unsurunun birlikte gerçekleşmesinin aranması gerekmektedir.

Suçun özel görünüş şekilleri internet açısından irdelenecek olursa, suç yapı itibarıyla içerik suçlarından farklı olarak bir müdahale suçudur. Dolayısıyla suç tipi teşebbüse müsaittir. Çünkü müdahale suçları olarak kabul edilen suçlarda hareket unsurlarına bölünebilmektedir. Örneğin internet üzerinden gerçekleştirilen haberleşmeyi engellemek için sisteme müdahale ederken, sistemin güvenlik bariyerlerine takılma söz konusu olursa veya sistem müdahaleyi tespit edip müdahalenin sonlandırılmasını sağlarsa haberleşmeyi engelleme suçunda teşebbüsten bahsetmek mümkün olacaktır. İnceleme konusu suça *iştirakin* her türü ile katılmak mümkündür. *İçtima* konusunda da haberleşmenin engellenmesi suçu için özellikli

⁶²¹ Bkz. İkinci Bölüm, § 5.- 5237 Sayılı TCK md. 6/1-G Hükmünce Bir Kitle İletişim Aracı Olarak İnternet.

⁶²² Ayrıntılı bilgi için bkz. ÖZKAN, Turgut, Türk Ceza kanununun Basın ve Yayınla ilgili Maddeleri, Gerekeçeleri ve Yorumları, http://www.medya-turk.net/yeni_tck_turgutozkan_1.php (Erişim Tarihi: 10.12.2007)

⁶²³ Bkz. İkinci Bölüm, § 5.- 5237 Sayılı TCK md. 6/1-G Hükmünce Bir Kitle İletişim Aracı Olarak İnternet.

bir durumun söz konusu olmadığı, suçun zincirleme suç ve fikri içtima uygulamalarına elverişlidir. Örneğin haberleşmenin engellenmesi suretiyle aynı anda md. 243 anlamında bilişim sistemine yetkisiz erişim, md. 244 anlamında bir bilişim sistemine veya veriye müdahale hatta somut olayın koşullarına bağlı olarak md. 123 anlamında kişinin huzur ve sükununu bozma suçu da gerçekleşebilir. Böyle olduğu takdirde tek bir hareketle kanunun farklı düzenlemeleri ihlal edildiği için bu suçlar arasında fikri içtima hükümleri uygulanmalıdır.

1.3.4.- Kişisel Verilerin Kaydedilmesi

5237 sayılı TCK sistemi içinde internetin doğrudan bir araç olarak kullanıldığı önemli suçlardan biri de md. 135⁶²⁴’de düzenlenen kişisel verilerin kaydedilmesi suçudur. Ceza hukukunun tarihsel gelişim sürecine bakılacak olursa kişisel verilerin koruma altına alınması düşüncesi özellikle 70’li yılların ikinci yarısından itibaren bilişim teknolojisinin hızlı bir gelişime girmesiyle her türlü bilginin sayısal kodlara dönüştürülmesi suretiyle teknik anlamda veri konumuna getirilmesi, ceza hukuku terminolojisine girmiş ifadesi ile “bilgilerin otomatik işleme tabi tutulmasıyla” kendini göstermiştir. Birinci bölümde internetin temel hak kullanımları içindeki yerinin ceza hukukundaki görünümüne ve ikinci bölümde kişisel verilerin korunmasına yönelik ulusal ve uluslar arası düzenlemelere ilişkin detaylı açıklamalarda bu net bir biçimde ortaya konulmuştur süreç ortaya konulmuştur. Dolayısıyla bu bölümde atıfta bulunulan açıklamaların referansıla doğrudan 5237 sayılı TCK md. 135’de düzenlenen kişisel verilerin kaydedilmesi suçu değerlendirilecektir. Ancak değerlendirmeden önce özellikle internet teknolojisinin gelişmesine paralel olarak sayıları her geçen gün artan ve hukuka aykırı veri kaydı ve transferi imkanı⁶²⁵ veren uygulamalardan kısaca bahsetmek gerekmektedir. Bu uygulamaların en çok tercih edilen tarzları casus ve kötücül yazılımlarla gerçekleştirilen şekilleridir. Çünkü bu şekilde internetin sunmuş olduğu imkanlar kullanılmak suretiyle sistemin açıklarından yararlanılmakta ve hedef kullanıcı fark etmeden tüm kişisel

⁶²⁴ MADDE 135. - (1) Hukuka aykırı olarak kişisel verileri kaydeden kimseye altı aydan üç yıla kadar hapis cezası verilir.

(2) Kişilerin siyasî, felsefî veya dinî görüşlerine, ırkî kökenlerine; hukuka aykırı olarak ahlâkî eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgileri kişisel veri olarak kaydeden kimse, yukarıdaki fıkra hükmüne göre cezalandırılır.

⁶²⁵ Bu başlık altında açıklanan uygulamaların md. 136 kapsamında düzenlenen kişisel verilerin transferine ilişkin açıklamalarda da geçerli olduğu ifade edilmelidir.

verileri kayıt altına alınmakta ve bir başka kişiye ulaştırılmaktadır. Bu imkanları tüketici bir sayımla ortaya koymak imkansızdır ancak bunlara birkaç örnek vermek gerekirse;

Klavye Dinleme Sistemleri (Keyloggers) olarak tanımlanan yazılım türü, kullanıcının klavye kullanarak girdiği bilgileri yakalayıp, tutan ve bunları bir başka kişiye (ki bu kişi yazılımın sahibi de olabilir, yazılım sahibinin komutuyla üçüncü bir kişi de olabilir) gönderen casus yazılımlardır⁶²⁶. Klavye dinleme sistemlerinin son derece tehlikeli sonuçlar doğurması muhtemel olan bu atağın 80'li yıllardan itibaren kullanıldığı bilinmektedir.

Tarayıcı Yardımcı Nesnesi (Browser Helper Object, BHO), İnternet Gezini (*Internet Explorer*) her açıldığında otomatik olarak çalışan küçük programlar olarak üretilmekte ve genel olarak tarayıcıya diğer yazılımlar tarafından yerleştirilmektedir. Kötücül amaçlarla yazılmış bir BHO, internet tarayıcısına kurularak o kullanıcıya ait internet'te erişilen her bilgiyi toplayabilir ve kullanım verilerini gizlice izleyebilir⁶²⁷.

Şifre Yakalayıcılar ve Şifre Soyguncular (Password Capture and Password Hijacker), Sistemde girilen şifreleri yakalayıp kaydetmeye yönelik çalışan casus programlardır⁶²⁸. Bu tür programlar geniş bir alanda etkinlik gösterebilmektedirler. Özellikle ağ üzerindeki paketler içinde hesap ve şifre bilgilerini saptayıp, kayıt altına alabilme özellikleri bakımından internette şifre üzerinden işlem yapan kullanıcılar açısından büyük bir tehlike arz etmektedir.

E- posta Hasatçısı (E-posta Harvester), çeşitli yöntemlerle bilgisayarlarda sabit disklerde bulunan e-posta adreslerini veya adres listelerini kullanıcıdan habersiz, bir sunucuya iletirler. Mi posta virüsü bu amaçla kötücül yazılımlara bir örnektir⁶²⁹.

Son olarak *Port Tarayıcı'lardan (Port Scanner)* kısaca bahsedilebilir⁶³⁰. Bunlar herhangi birinin bir port'u dinleyip dinlemediğini görmek amacı ile bir makine üzerinde

⁶²⁶ CANBEK/ SAĞIROĞLU, Kötücül ve Casus Yazılımlar, sh: 126.

⁶²⁷ CANBEK/ SAĞIROĞLU, Kötücül ve Casus Yazılımlar, sh: 128.

⁶²⁸ CANBEK/ SAĞIROĞLU, Kötücül ve Casus Yazılımlar, sh: 129.

⁶²⁹ DAŞKIRAN, Levent, Sanal Tehdit: Bilgisayar Virüsleri, in: Bilim ve Teknik/ Ek – Mayıs, Ankara, 2005, sh: 8.

⁶³⁰ Port tarayıcı ile ilgili ABD uygulaması ile ilgili bkz. KURT, Bilişim Suçları, sh: 155. Bu noktada bir husus vurgulanmalıdır. Port tarayıcılar sadece kötücül amaçla kullanılmamaktadır. Kullanım amacına göre anlam kazanan bir sistemdir. Bu araçların port tarayıcılarının Truva Atı saldırılarına karşı güvence olma fonksiyonu bakımından bkz. DAŞKIRAN, Sanal Tehdit, sh: 9.

tanımlı olan 65 536 adet port'un hepsini otomatik olarak sınyan araçlardır. Bu araçlar, önlem almayan sistemlere sızmak veya sistemden bilgi kaçırmak için kullanılabilir⁶³¹.

Yukarıda da görüldüğü gibi internet aracılığıyla sistemin açıklarından yaralanıp kişisel verilerin kaydedilmesi ve kötücül amaçlarla kullanılmaları oldukça mümkündür. Bu minvalde 5237 sayılı TCK md. 135'de düzenlenen "Kişisel Verilerin Kaydedilmesi" suçun incelerken öncelikle inceleme konusu *suçun maddi konusunun* internet açısından ele alınması gerekmektedir. Birinci fıkrada bir kimsenin hukuka aykırı olarak kişisel verileri kaydetmesi suç olarak düzenlenmektedir. Buradan da anlaşılacağı üzere suçun maddi konusu kişisel veridir. Bilindiği üzere kişisel veri gerek ülkelerin ulusal düzenlemelerinde gerekse uluslar arası sözleşmelerde farklı kapsamlarda düzenlenmektedir. Bu açıdan kanun koyucunun ya tanımları düzenlediği 6. maddede ya da inceleme konusu maddenin metninde veya gerekçesinde kişisel veriden neyin kastedildiğini açık bir biçimde ortaya koyması gerekmektedir. Ancak ne Tanımlar başlıklı 6. maddede ne de kişisel verilerin kaydedilmesinin düzenlendiği 135. maddenin metninde bu yönde bir tanımlama yapılmamıştır. Md. 135'in gerekçesinde ise kişisel veriden ne anlaşılması gerektiği ifade edilmiştir. Buna göre, gerçek kişiyle ilgili her türlü bilgi kişisel veriyi oluşturmaktadır.

Bu noktada madde gerekçesinde kendisine atıfta bulunulan Kişisel Nitelikteki Verilerin Otomatik İşleme Tâbi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşme'nin ikinci maddesinde kişisel verinin nasıl belirlendiğine bakmak faydalı olacaktır. Sözleşmenin 2/(a) maddesinde ise kişisel veri, "*kim olduğu belirli olan ya kim olduğu tespit edilebilen gerçek kişilerle ilgili enformasyon*" olarak tanımlanmaktadır⁶³². Buna paralel olarak 1995 yılında Avrupa Birliği ve Parlamentosunda kabul edilen "Kişisel Verilerin İşlenmesinde Gerçek Kişilerin Korunması ve Bu Tür Verilerin Serbest Dolaşımı Yönergesi"nin 2/(a) maddesine ise kişisel veri, "*kim olduğu belirli olan ya da kim olduğu tespit edilebilen gerçek kişilerle ilgili enformasyon*" şeklinde tanımlanmıştır. Maddenin devamında kim olduğu tespit edilebilen kişi, "*özellikle bir id numarasına referans yapılmak suretiyle veya belirli fiziksel, psikolojik, ruhsal (zihinsel) ekonomik, kültürel ya da sosyal kimliği ile ilgili bir ya da birden fazla*

⁶³¹ CANBEK/ SAĞIROĞLU, Kötücül ve Casus Yazılımlar, sh: 131.

⁶³² Sözleşmenin resmi çevirisi için bkz. <http://www.uhdigm.adalet.gov.tr/kisiverkorun.htm> (Erişim Tarihi: 23.05.2007)

faktörlere bağlı olarak doğrudan ya da dolaylı olarak tespit edilen veya edilebilen kişi şeklinde tanımlanmıştır⁶³³.

Kanaatimizce md. 135 gerekçesinde ifade edildiği tarzıyla gerçek kişiyle ilişkilendirilen her bilginin bu madde bağlamında kişisel veri sayılması isabetli değildir. Şen de kişisel veri kapsamının bu denli geniş tutulmasının “belirlilik” ilkesine aykırı görmektedir⁶³⁴. Burada koruma altına alınmak istenen kişisel veriler, kişinin anonimleşmemiş yada alenileşmemiş ve bir özel hayat unsuru teşkil eden verilerdir. Bu husus mutlak suretle vurgulanmalıdır. Konu farklı bir açıdan değerlendirilecek olursa, kişiyi ilgilendiren bir bilginin doğrudan veya dolaylı olarak kamuya paylaşılması ve gerek bu paylaşımın gerçekleştiği anda gerekse sonraki süreçte o bilginin sahibi olan kişinin rızası söz konusu ise alenileşmiş bir bilginin kaydedilmesi bu suç kapsamında değerlendirilmez. Çünkü her şeyden önce suçun düzenlendiği yer itibarıyla kayıt altına alınan bir kişisel veri hayatın gizli kalması gereken alanına ait bir veri olmak durumundadır. Ancak yukarıda da örneklediği gibi bir kişiyi ilgilendiren ancak alenileşmiş birçok veri söz konusudur ve internet ortamında kayıt altına alınıp diğer kullanıcıların bu verilere erişimim mümkün kılınmaktadır. Netice itibarıyla madde metninde ve en azından madde gerekçesinde, korunması amaçlanan hukuksal değerle örtüşen bir kişisel veri tercihinin yapılması doğması muhtemel karışıklıkların önüne geçmek anlamında faydalı olacaktır.

Suçun *maddi konusu* ile ilgili başka bir sorun da md. 132’de düzenlendiği haliyle gizli kalması gereken haberleşme içeriğinin, md. 133’de düzenlendiği haliyle aleni olmayan konuşma içeriklerinin ve md. 134’de düzenlendiği haliyle bir özel yaşam olayının kişisel veri olarak kabul edilip edilemeyeceğidir. İnceleme konusu maddenin gerekçesinde bir gerçek kişiyi ilgilendiren tüm bilgiler kişisel veri kapsamında değerlendirildiği ve bu verilerin de doğrudan bir gerçek kişiyi ilgilendirdiği düşünülecek olursa, kişisel veri olarak kabul edilmeleri gerekmektedir. Bu noktada başka bir sorun gündeme gelmektedir. Şayet bu verileri kişisel veri olarak kabul etmek mümkünse ve ilgili maddelerde ayrıca bu verilerin kayıt altına alınmasının cezalandırıldığı düşünülürse, kişisel verilerin kaydedilmesini münhasıran düzenleyen md.135 karşısında bu hükümler nasıl değerlendirilmelidir?

⁶³³ ŞİMŞEK, Anayasa Hukukunda Kişisel Verilerin Korunması, sh: 41.

⁶³⁴ ŞEN, Hürriyete Karşı Suçlar, sh: 218.

Kanaatimizce bu değerlendirmeyi yapmadan öne “kişisel veri” kavramının md. 135’de nasıl düzenlendiği bir kez daha dikkate alınmalıdır. Kişisel verilerin bir gerçek kişiyi ilgilendiren tüm bilgiler şeklinde düzenlenmesiyle kanun koyucu kişisel veri özelinde aynen özel hayatın gizliliğini ihlal suçunda olduğu gibi tali/ tamamlayıcı bir norm oluşturmak istemiştir. Bu hükmü başka bir şekilde anlamak TCK sistematığına ters düşmek anlamına gelecektir. Bu bağlamda yukarıda tek tek anılan maddelerde kayıt altına alınması cezalandırılan kişisel verilerin de özel olarak düzenlendiği kabul edilmelidir. Bir örnekle açıklamak gerekirse, md. 132’de düzenlenen haberleşme gizliliğinin ihlali suçunda, tarafları arasında gizli kalması gereken bir haberleşme içeriği kayda alınmak suretiyle ihlal ediliyorsa md.132/1- c.2 hükmünce cezalandırılmaktadır. Burada gizlilik ihlali kayda alındığı anda gerçekleşmiş olacaktır. Çünkü gizli kalması bir haberleşme içeriği üzerinde herhangi bir tasarruf hakkı sadece taraflara aittir. Yetkisiz kişilerin bu tasarruflardan birini kullanmasıyla gizlilik ihlal olmuş olur. Kaydetme de bu haberleşme içeriği üzerinde bir tasarruftur. Bu nedenle haberleşme gizliliğini ihlal ile kişisel verinin kaydedilmesi ayrı edilemeyeceği için bu kişisel verinin kaydını haberleşmenin gizliliğini ihlal içinde değerlendirmek gerekir. Bu anlamda md. 132, md.135’e göre özel bir düzenleme olarak konumlanmaktadır. Bu örneğin mantığını md. 133 ve md. 134’e de yansıtmak mümkündür. Netice itibarıyla md. 135 düzenlemesinin, kanunda özel olarak belirtilmemiş olan hukuka aykırı kişisel veri kaydedilmesi eylemleri için düşünmek isabetli olacaktır.

Suçun maddi unsuru internet açısından değerlendirilecek olursa, maddenin birinci fıkrasında hukuka aykırı olarak bir kişisel verinin kaydedilmesi düzenlenmektedir. İnternet açısından bu hükmün iki boyutlu düşünülmesi gerektiği düşüncesindeyiz. Birinci boyutu bir kişisel verinin hukuka aykırı olarak internet ortamına aktarılması anlamında kişisel verilerin kaydedilmesi, ikincisi de internet aracılığıyla başka bir bilişim sisteminde bulunan kişisel verinin kaydedilmesidir. Birinci boyutla ifade edilen kişisel verilerin kaydedilmesi durumlarıyla günümüzde sıklıkla karşılaşılmaktadır⁶³⁵. Ancak burada dikkat edilmesi gereken husus hukuka aykırılık unsur ile ilgili noktadır. Bir kamu veya özel kuruluşun verdiği hizmet

⁶³⁵ Bu husus madde gerekçesinde şöyle ifade edilmektedir: “Çağımızda kişilerle ilgili kayıtların bilgisayar ortamlarına geçirilip muhafaza edilmesi uygulamasına bazı kurum ve kuruluşlar tarafından başvurulmaktadır; hastanelerde hastalara, sigorta şirketlerinde sigortalılara, bankaların ve kredili alışveriş yapılan mağazaların müşterilerine ilişkin kayıtlar, böylece tutulmaktadır. Bu bilgilerin amaçları dışında kullanılmasından veya herhangi bir şekilde üçüncü şahısların eline geçerek hukuka aykırı olarak yararlanılmasından dolayı hakkında bilgi toplanan kişiler büyük zararlara uğrayabilmektedirler. Bu bakımdan, kişilerle ilgili bilgilerin hukuka aykırı olarak kayda alınması suç olarak tanımlanmıştır.”

dolayısıyla hukukun kendilerine verdiği hak ve yetkiyi kullanmak suretiyle kişisel verileri kayıt altına alınmaktaysa, bu noktada bir hukuka aykırılık söz konusu olmayacağından dolayı suç teşkil edebilecek bir kişisel veri kaydı söz konusu olmayacaktır. İnternetin bu anlamda kişisel veri kaydına müsait olup olmadığı konusunda bir açıklama yapmak gerekirse, internet sadece sanal bir ortam değil her şeyden önce bir iletişim ağıdır. Dolayısıyla interneti sadece web siteleriyle oluşmuş bir siber uzay alanı olarak algılamamak ve bu iletişim ağını oluşturan bütün unsurlarıyla birlikte düşünmek gerekmektedir. Bu unsurların başında da internet sükeleri gelmektedir. İnternet ortamında erişilebilen tüm veriler mutlak suretle internet sükelerinin marifetiyle kullanılabilir hale gelmektedir. Örneğin bir web sitesinde bir kişi ile ilgili erişilen kişisel veri niteliğindeki veri mutlak suretle o veriyi internet ortamına aktaran içerik sağlayıcısında veya istenildiği zaman erişilebilmesi için depolandığı yer sağlayıcısında kayıt altına alınmıştır. Bu yönüyle sanal ortamda erişilen tüm veriler aslında kayıt altına alınmış verilerin gösteriminden, paylaşımından ibarettir. Bu yüzden internetin kişisel verilerin kaydedilmesine elverişli olduğundan şüphe yoktur.

İkinci boyutu ise daha önce birçok suç tipinde örnek olarak verildiği üzere, internet aracılığıyla gerek online gerekse offline konumdayken kişilerin kendileriyle ilgili özel verilerinin kaydedilmesi durumudur. Bu konuyla ilgili verilebilecek en basit örnekler internet aracılığıyla kişilere gönderilen casus veya kötücül yazılımlarla internete bağlı olan herhangi bir bilgisayarla yapılan tüm işlemlerin kayıt altına alınabilmesi gösterilebilir. Burada aslında fail internet aracılığıyla bir casus veya kötücül yazılım göndermek suretiyle doğrudan bir veri kaydı gerçekleştirmemektedir. Bu yazılımlar kendilerini hedef bilgisayar içinde uygun boşluklarda muhafaza eder, gerektiğinde kendini çoğaltır ve hedef bilgisayar kullanıcısının yaptığı tüm işlemleri kaydedip kendisine komut veren faile gönderebilir. Bu durumda da bir kişisel veri kaydı durumu söz konusudur.

İnceleme konusu maddenin maddi unsuru dikkatle incelenecek olursa, sadece hukuka aykırı olarak gerçekleştirilen kişisel veri kaydı düzenlenmiştir. Ancak Ketizmen'in de isabetle ifade ettiği üzere, maddenin hali hazırdaki konumu itibariyle hukuka uygun olarak kaydedilmiş bir kişisel verinin, daha sonra kaydetme amacı dışında bir şekilde kullanılması karşısında kanun koyucu bir güvence öngörmemiştir. Şu halde md. 135 hukuka uygun kaydedilen bir kişisel verinin amacı dışında kullanılmasına engel teşkil etmemektedir. Ancak madde gerekçesinde,

“Çağımızda kişilerle ilgili kayıtların bilgisayar ortamlarına geçirilip muhafaza edilmesi uygulamasına bazı kurum ve kuruluşlar tarafından başvurulmaktadır; hastanelerde hastalara, sigorta şirketlerinde sigortalılara, bankaların ve kredili alış veriş yapılan

mağazaların müşterilerine ilişkin kayıtlar, böylece tutulmaktadır. Bu bilgilerin amaçları dışında kullanılmasından veya herhangi bir şekilde üçüncü şahısların eline geçerek hukuka aykırı olarak yararlanılmasından dolayı hakkında bilgi toplanan kişiler büyük zararlara uğrayabilmektedirler. Bu bakımdan, kişilerle ilgili bilgilerin hukuka aykırı olarak kayda alınması suç olarak tanımlanmıştır.”

denilmek suretiyle aslında sadece kişisel hukuka aykırı olarak kaydedilmesinin değil aynı zamanda her ne suretle olursa olsun kaydedilmiş verilerden amacı dışında veya hukuka aykırı olarak yararlanılması durumunun da madde kapsamında düşünüldüğü anlaşılmaktadır. Ancak ceza hukuku kanun koyucunun saikini var sayıp kanunda açıkça yazılmamış bir hususu bir maddi unsur olarak değerlendiremez. Bu nedenle madde gerekçesi ile madde metin arasındaki bu dilemma karşısında madde gerekçesini ikinci plana atarak madde metnin eksik koruma alanı çerçevesinde hareket etmek gerekmektedir.

İnceleme konusu maddenin ikinci fıkrasına göre ise kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgileri kişisel veri olarak kaydeden kimse birinci fıkra hükmüne göre cezalandırılır. Kanaatimizce böyle bir fıkranın düzenlenmesine hiç gerek olmadığı gibi çok önemli bazı karışıklıklara da neden olabilecek tehlikelilikte bir hükümdür. Öncelikle söz konusu fıkra hükmünde sayılan bilgi kategorileri dikkatle incelenecek olursa, zaten doğrudan bir kişiyi belirleyen bilgi kategorileri olmaları anlamında birinci fıkra hükmüne tabidirler, yani bu bilgiler zaten doğrudan kişisel veridir. Çünkü bir kişinin siyasi, felsefi, dini, ahlaki, cinsel yönelimine veya ırki kökenine ilişkin bilgiler, madde gerekçesinde de açıkça ifade edildiği üzere bir kişiyi doğrudan ilgilendiren bilgilerdir.

Dolayısıyla bu bilgilerin ayrıca ifade edilmesinde farklı bir amaç söz konusu olmalıdır. Örneğin bu bilgilerin kayıt altına alınması bir ağırlaştırıcı neden olarak düzenlenmesi durumunda tartışmalı olmakla beraber anlaşılır bir tercih olarak kabul edilebilir çerçevede olduğu düşünülebilir. Ancak cezai müeyyide olarak da birinci fıkraya atıfta bulunması bu bilgilerin esasında kişisel veri olmadığını ancak kişisel veri olarak kaydedildiği durumlarda madde metnince değerlendirilebileceği yönünde bir izlenim ortaya koymaktadır. Keza fıkra hükmünde de açıkça bu bilgilerin kişisel veri olarak kaydedilmesi durumunda demek suretiyle bunların aslında kişisel veri olmadığı ancak kişisel veri olarak kaydedildiği durumlarda

cezalandırılabilceđi belirtilmiřtir. O halde bu verilerin kiřisel veri olarak kaydedilmediđi ynnde bir kanaat hasıl olursa verinin ieriđi yani bizatihi kendisi deđil kaydediliř tarzi itibariyle madde kapsamı dıřında tutulacaktır. Byle bir durum kanaatimizce aık bir eksiklik gstergesidir. Hangi amala dzenlendiđi anlařılamayan ve yasal bir amala da bađdařtırılamayan bu fıkra hkmnn derhal yeniden gzden geirilip uygun bir řekle dnřtrlmesi gerekmektedir.

Son olarak bir kiřisel verinin internet ortamına aktarılmasının ardından bir kullanıcı tarafından eriřilerek kayıt altına alınması durumunda internet kullanıcısının cezai sorumluluđunun dođup dođmayacađı noktasında bir aıklama yapmak gerekmektedir. rneđin bir kiřinin cinsel veya ahlaki tercihleri ile ilgili kiřisel bir veriyi ierik sađlayıcısı olarak internet ortamına herkesi eriřebileceđi bir web sitesine yklemesinin ardından bařka bir kullanıcı o siteyi ziyareti esnasında bu bilgiyi grmř ve herhangi bir amala kendi bilgisayarına kaydetmiřtir. Bu durumda ncelikle kiřisel bir veri konumundaki bilgiyi internet ortamına yklemek suretiyle kayıt altına alan ierik sađlayıcısının cezai sorumluluđu řphesizdir. Burada zerinde dřnlmesi gereken internet kullanıcısının durumudur. Yukarıda ifade edildiđi zere anonimleřen/ aleni hale gelen bir bilginin kayıt altına alınması, veri kiřisel veri konumunda olsa bile su teřkil etmeyecektir. Kullanıcı bu rnekte sz konusu bilgisi kamusal eriřilebilirliđin mmkn kılındıđı bir web sitesinde grmř ise artık sz konusu veri aleni hale getirildiđi iin kullanıcının bu bilgiyi hangi amala olursa olsun kayıt altına alması kiřisel verilerin kaydedilmesi olarak dřnlmemelidir. Keza teknik aıdan bakıldıđında da aslında kullanıcının web sitesinden bir bilgiyi kaydetmesi teknik anlamda bir kayıt sayılmaz. Teknik anlamda kayıt ierik sađlayıcısının gerekleřtirdiđi iřlemdir. Kullanıcının iřlemi ise kayıt altına alınmıř bir ieriđi kopyalamaktır. Kopyalana bir verinin bilgisayara veya herhangi bir araca kaydedilmesi ile ierik sađlayıcının gerekleřtirdiđi kaydetme iřlemi birbirinden ayrılmalıdır.

Suun internet aracılıđıyla iřlenebilirliđi aısından **manevi unsur** deđerlendirilecek olursa, suun manevi unsuru bakımından herhangi bir zellikli durum yaratılmamıřtır. Suun iřlenebilmesi iin genel kastın varlıđı yeterlidir. Ayrıca suun olası kastla da iřlenebilmesi mmkndr. rneđin kiřisel veri niteliđindeki bir bilginin internet ortamına aktarılmasında kiřinin rızasının sz konusu olup olmadıđı ynnde řpheli olmasına rađmen dođabilecek her sonucu gze alarak bu veriyi bir web sayfasına kaydeden ierik sađlayıcının olası kastla hareket ettiđi kabul edilebilir. Kusurluluđu etkileyen nedenlerin varlıđı zerinde de

düşünülecek olursa özellikle suçun internet aracılığıyla işlenebilirliği konusunda en çok rastlanan kusurluluğu etkileyen neden hatadır. Çünkü bilişim teknolojilerinin gelişmesiyle birlikte herkesin, her kurumun gerek kullanıcı herkeşe içerik sağlayıcı olarak kullanması nedeniyle bir takım problemlerin yaşanması kuvvetle muhtemel hale gelmiştir. Örneğin bir verinin kişisel veri olup olmamasında, o verinin kaynağı olan kişinin verinin kayıt altına alınmasına rıza gösterip göstermediğinde veya bizzat verinin kaynağı olan kişinin kimliğinde hataya düşülmesi söz konusu olabilmektedir. Burada suçun olası kastla işlenmesi ile suçun işlenmesinde hataya düşülmesi arasındaki ince çizginin, bilhassa da kasıt unsurunun dikkatli tespit edilmesi gerekmektedir.

Suçun özel görünüş şekilleri bakımından da şunları söylemek mümkündür; bu suçun internet aracılığıyla işlenebilen halleri bakımından *teşebbüsten* bahsetmek mümkündür. Çünkü kayıt işlemi teknik bir işlem olduğu için bu işlemin yarıda kesilmesi veya tüm hareketlerin gerçekleştirilmesine rağmen teknik bir nedenle kayıt işleminin tamamlanamaması mümkündür. Ayrıca yukarıda verdiğimiz örnekten istifade ederek, bir casus yazılım kullanmak suretiyle kişisel verilerin kaydedilmesinde farklı bir alternatifle karşılaşmak da mümkündür. Şöyle ki; yerleştirilen casus yazılıma verilen komut gereğince hedef bilgisayardaki tüm kişisel verilerin bir hafta suretiyle kaydedilmesi ve sonra komut sahibi kişiye gönderilmesi mümkündür ve bu durumla sıkça karşılaşılır. Böyle bir durumda veri kaydına devam eden casus yazılım, yüklenmesinin ardından 6. günde fark edilip etkisiz hale getirilirse burada tek suç işleme kararıyla süreklilik arz eden bir kişisel veri kaydı durumu söz konusu olduğundan, o ana kadar kayıt altına aldığı kişisel veriler dikkate alınmadan suçun tamamlanamadığından bahisle örnek konusu yapılan eylemin teşebbüs aşamasında kaldığı kabul edilmelidir.

İçtima konusunda da aynı suç işleme kararıyla birden çok kez suçun işlenmesi durumunda zincirleme suç hükümlerinin uygulanması mümkündür. Aynı şekilde suçun internetle işlenebilen şekilleri bakımından fikri içtima hükümlerinin uygulanabileceği durumlarda söz konusudur. Örneğin yukarıda verilen örnek çerçevesinde bir kişinin bilişim sistemine yetkisiz erişim sağlanıp orada kalınmaya devam edilmesi (md. 243) suretiyle kişisel verilerin kaydedilmesi mümkün olabilmektedir.

1.3.5.- Verilerin Hukuka Aykırı Bir Biçimde Verilmesi veya Ele Geçirilmesi

Kişisel verilerin korunması prensibinin bir diğer görünümü olarak 5237 sayılı TCK'ye alınmış bir madde olan 136. madde kişisel verilerin hukuka aykırı olarak verilmesi veya ele geçirilmesi eylemlerini suç olarak düzenlemiştir. Bu suç da bir önceki madde olan kişisel verileri kaydedilmesi suçuyla aynı çizgide düşünüldüğü için sadece suç tipinin internet aracılığıyla işlenmesinin mümkün olduğu ifade edilerek genel açıklamalar bakımından md. 135'in değerlendirildiği bölüme atf yapmakla yetinilmektedir.

Suçun maddi konusu hususunda madde metni ile yan başlık arasında bir farklılık göze çarpmaktadır. Çünkü madde yan başlığı verilerin hukuka aykırı olarak ele geçirilmesi ve verilmesi olarak ifade edilmişken madde metni bu açıkça suçun konusunu kişisel veriler olarak belirlemiştir. Bu ikilemin özellikle suçun internet acılığıyla işlenmesi açısından önemli bir riski bulunmaktadır. Şöyle ki; bilindiği üzere bir bilişim sistemi olan internet dahilindeki tüm sanal, dijital unsurlar veri hükmündedir. Keza md. 243'ün gerekçesine bakılacak olursa da bir bilişim sistemi açısından sistem içindeki tüm soyut unsurlar veri hükmündedir. Dolayısıyla veri bilişim teknolojisi bakımından kaplamsal bir kavramdır. Hiç şüphe yok ki uygun formatlara dönüştürülmüş her bilgi, niteliği ne olursa olsun teknik açıdan bir veridir. O halde sadece madde yan başlığına bakıldığında bir bilişim sistemi dahilinde veri olarak kabul edilen tüm soyut unsurların verilmesi ve ele geçirilmesi bu madde hükmünde düzenlenmiş gibi bir izlenim doğmaktadır. Ancak madde metnine bakılacak olursa da burada kastedilenlerin sadece kişisel veri olduğu anlaşılmaktadır. 135. madde yan başlığında açıkça kişisel verilerin kaydedilmesi yazılırken niçin bu maddenin yan başlığında sadece verilerin hukuka aykırı olarak verilmesi ve ele geçirilmesi yazılmıştır anlamak güçtür. Bunun bilinçli bir tercih doğrultusunda gerçekleştiğinin kabul edilmesi durumunda ise madde metni ile başlık arasında yukarıda bahsedilen ikilemin yansıtılmamış olması gerektydi. Kanaatimizce bu husus bir eksiklik olarak ortaya konulabilir ve düzeltilmesi durumunda tehlikeli sonuçlara sebebiyet verebilir.

Suçun *tipe uygun eylem unsuruna* bakılacak olursa öncelikle yine madde yan başlığı ile madde metni arasında bir uyumsuzluk gözlemlenmektedir. Çünkü madde yan başlığında sadece, madde metnindeki ifade esas alındığında, kişisel verilerin hukuka ayır olarak verilmesi veya ele geçirilmesi yazılmışken madde metnine bakıldığında bunlara ek olarak

yayma fiilinin de düzenlendiği görülmektedir. Yasa yapma tekniği açısından elbette ki madde metninde düzenlenen tüm hareketlerin madde başlığına yazılması gerekmemektedir. Ancak madde başlığının madde metninde düzenlenen tüm hareketleri kapsar nitelikte formüle edilmesi bir zorunluluktur. Bu bağlamda madde metni ile yan başlık karşılaştırıldıkları zaman madde metnindeki “yayma” seçimlik hareketini yan başlıkta kapsayan bir ifadeye rastlanmamaktadır. Bu nedenle madde metni ile yan başlığı arasındaki uyumun sağlanmasında fayda görmekteyiz.

İnceleme konusu maddede üç adet seçimlik hareket düzenlenmiştir. Bunlar “vermek”, “yaymak” ve “ele geçirmek” olarak belirlenmiştir. Her üç seçimlik hareket internet açısından değerlendirilecek olursa, bir kişisel verinin hukuk aykırı olarak başka bir kimseye verilmesinde hangi noktadan hareket edilmesi gerektiği çok önemlidir. Kanaatimizce burada iletim tarzında bir hukuka aykırılık durumunun söz konusu olması oldukça zordur. Dolayısıyla kişisel verinin hangi yolla verildiğinden ziyade veren kişinin bu eyleminde ehliyetli olup olmadığına bakmak daha isabetli olacaktır. Bir kişisel veriyi başka bir kimseye ulaştıran kişinin veri üzerinde işlem yapmaya yetkili olmayan veya kendine verilen bir yetkiyi aşmak suretiyle eylemi gerçekleştiren bir kişi olması gerekir. Bu anlamda yetkisiz veya yetkisini aşmış bir kimsenin bu veriyi başkasına nasıl iletildiği önemli değildir. Örneğin bir sigorta şirketinde temizlikçi olarak görev yapan birinin, görevli şahıs verinde yokken sigortalıların kişisel verilerinin depo edildiği bir bilgisayardan edindiği kişisel verileri üçüncü başka bir kişiye vermesi yine aynı şekilde sadece sisteme veri girişi ile görevlendirilen bir personelin kendisine verilen yetkinin sınırların aşarak sisteme sızması ve oradan edindiği bilgiyi başka birine vermesi durumunda söz konusu seçimlik hareket gerçekleşmiş sayılmalıdır. Veriliş tarzının hukuka aykırılık bakımından bir etkisinin olmadığı vurgulanmakla beraber söz konusu veri iletiminin internet üzerinden gerçekleşmesi durumunda bir noktanın altı çizilmelidir. Burada kastedilen verme ile, sadece belli veya belirlenebilir bir taraftan yine belli veya belirlenebilir bir tarafa yapılan iletim işlemi kastedilmektedir. Örneğin bir e- posta veya MSN gibi sohbet programları vasıtasıyla aleniyet unsuru gerçekleşmeksizin yapılan iletim işlemi gibi. Şayet kullanılan araç itibarıyla verinin iletimi aleni bir hal alırsa burada artık belirsiz sayıda kişiler muhatap alınmış olmasından mütevellit “yayma” hareketi gerçekleşmiş olacaktır.

Bu açıklamayı tamamlar nitelikte “yayma” seçimlik hareketi üzerinde durulacak olursa, yukarıda da izah edildiği gibi kanaatimizce “verme” ile “yayma” arasında internet

perspektifinden hareketin gerçekleştiriliş tarzı ve buna bağlı olarak hareketin gerçekleştirildiği araç önem arz etmektedir. Örneğin bir kişisel veri, kaynak kişinin rızası olmaksızın kamusal erişilebilirliği haiz bir web sitesine yüklenecek olursa, burada bu içeriğin herkes tarafından edilebilir kılınması dolayısıyla bir aleniyetin söz konusu olduğu kabul edilebilir. Buna bağlı olarak da belli sayıda kişiye yapılan iletimi kapsayan “verme” burada söz konusu olmayacaktır. Burada artık belirsiz sayıda kişiye sunulması anlamında “yaymanın” gerçekleştiği kabul edilmelidir.

Üçüncü seçimlik hareket olarak belirlenen “ele geçirme” ise yine yetkisiz veya yetkisini aşan bir kişi tarafında bir kişisel verinin, kaynak kişisi ve/veya veriyi yasal anlamda depo eden kişi ya da kuruluşun rızası hilafına temin edilmesi şeklinde kendini göstermektedir. Örneğin internet aracılığıyla güvenlik bariyerleri devre dışı bırakılan bir bilişim sistemindeki verilerin temin edilmesi durumu buna bir örnektir. Daha önce kişisel verilerin kaydedilmesi suçu ile ilgili yapılan açıklamalarda verilen örnek biraz daha geliştirilecek olursa suç tipinin boyutları daha net anlaşılacaktır.

Bir kişi paravan bir web sitesi oluşturmuştur. Hatta bu site hedef kullanıcının sıklıkla kullandığı bir sitenin kopyası şeklinde düzenlenmiştir. Kişi bu siteye bir casus yazılım yerleştirmiştir. Bu siteyi ziyaret eden daha doğrusu aslını ziyaret ettiğini düşünüp kopyasını ziyaret eden ve bunu fark edemeyen bir kullanıcı öğrenmek istediği bir bilgiye ulaşmak için kendisinin yönlendirildiği bir linki tıklamaktadır. Ardından küçük bir pencere açılmakta ve kullanılan bilgisayarda bu linki görüntüleyecek gerekli ActiveX programının yüklü olmadığını, sayfayı görüntülemek için bu programın yüklenmesi gerektiği, bu programı yüklemek için de “Evet” şikkının tıklanması gerektiği söylenmektedir. Durumun hala farkına varmayan kullanıcı güvenilir bulduğu bu sitenin komutunu yerine getirir ve bilgisayarına ActiveX programını yüklediğini düşünürken bilgisayarına paravan site kurucusunun yönlendirdiği casus yazılım yüklenmektedir. Ardından kullanıcının haberi olmadan, yazılım oluşturulurken verilen komutlara bağlı olarak casus yazılım belli periyotlarla kişisel veriler de dahil olmak üzere her türlü veriyi depo etmekte ve internet üzerinden bu kişiye göndermektedir. Dikkat edilecek olursa burada özellikle hedef alınmış bir kullanıcı yoktur. Yani fail doğrudan bir casus yazılım göndermemektedir. Mağdur kendi girdiği siteden kendi eylemleriyle failin hazırladığı yazılımı kendi bilgisayarına kaydetmiştir. İşte böyle bir durumda da fail böyle bir eylemi gerçekleştirmek suretiyle her türlü olasılığı göze alarak söz konusu verilerin kaydedilmesi ve ele geçirilmesi suçunu işlemiş kabul edilecektir.

Bu örneğe paralel olarak internet perspektifinden suçun *kusurluluk* unsuruna bakılacak olursa, öncelikle suçun genel kastla işlenebilir olduğu kabul edilmelidir. Bu noktada bir problem yoktur. Ancak fail doğrudan mağdurun kişisel verilerini ele geçirmeyi amaçlamamasına rağmen, örnekte olduğu gibi diğer verilerle birlikte kişisel veriler de ele geçirilirse ne tür bir kastın varlığının söz konusu olacağı noktasında karışıklık doğabilir. Burada düşünülebilecek ilk olasılık söz konusu durumda bir olası kastın mümkün olacağı ihtimalidir. Çünkü md. 21/2'ye göre kanuni tanımındaki unsurların gerçekleşeceği öngörülmesine rağmen, fail tarafından fiilin işlenmesi halinde olası kast söz konusudur. Ancak örnekte mağdur kullanıcıya yönlendirilen casus yazılım, belli bir periyot içinde nitelik ayırt etmeksizin tüm bilgilerin kaydını ve faile göndermesi üzerine programlandığı için, kayıt adlına alınacak ve gönderilecek veriler arasında zorunlu olarak kişisel nitelikli verilerin de olabileceği öngörülmüşse artık burada olası kasttan değil ikinci derecede doğrudan kasttan bahsetmek yerinde olacaktır⁶³⁶. *Kusurluluğa etki eden nedenler* bakımından da en sık karşılaşılabilecek durum suçun maddi unsurlarında hata durumudur. Çünkü kanun koyucu kişisel veri olarak net bir çerçeve çizmediği için elde edilecek veya yayılacak bir verinin normal bir veri mi yoksa kişisel bir verimi olduğu hususunda hataya düşülmesi mümkündür. Yine aynı şekilde internet aracılığıyla işlenen birçok suçta olduğu gibi, internet ortamında yanlışlıkla başka birinin kişisel verilere erişime ve onları ele geçirilebilir.

1.3.6.- Bilişim Sistemine Girme

İnternet ortamında işlenen suçlar bakımından 5237 sayılı TCK'nin en önemli maddeleri üçüncü kısım onuncu bölümde yer alan "Bilişim Alanındaki Suçlar"dır. Bu bölümdeki suçlar *Yazıcıoğlu* tarafından doğrudan veya gerçek bilişim suçları olarak kabul edilmektedir⁶³⁷. Ancak tez konusunun kapsamı gereği bu bölümde incelenecek suçlar bilişim sisteminin kaplamsal anlam bütünlüğü içerisinde değil sadece bir bilişim sistemi unsuru olarak interneti ilgilendiren kısmı bakımından değerlendirilmeye çalışılacaktır. Çünkü bu bölümde yer alan tüm maddeler bir bütün olarak bilişim sistemi esas alınarak hazırlanmıştır.

⁶³⁶ İÇEL, Suç Teorisi, sh: 189.

⁶³⁷ YAZICIOĞLU, Yeni Türk Ceza Kanunundaki Bilişim Suçları, sh: 397.

Anılan bölümde yer alan ilk düzenleme m. 243⁶³⁸ yer alan bilişim sistemine girme suçudur. Doktrinde bu hükmün, Avrupa Konseyi Siber Suç Sözleşmesi md. 2⁶³⁹, de yer alan, taraf devletlerin iç hukuklarına uygun olarak bir bilişim sisteminin tamamına veya bir kısmına kasten ve haksız olarak erişimi suç haline getirecek yasal tedbirleri alması direktifinin bir sonucu olduğu düşünülmektedir⁶⁴⁰. Ancak buna karşı olarak aşağıda da değinilecek yasal değişiklik süreçleri dahilinde bu amaçtan sapıldığı ve Siber Suç Sözleşmesi'yle arzu edilen paralelliğin sağlanamadığı görüşünü savunan yazarlar da vardır⁶⁴¹. Kanaatimizce her şeyden önce madde içeriği ile maddenin yan başlığı arasındaki uyumun Siber Suç Sözleşmesi'nin 2. maddesiyle paralel olması gerekmektedir. Teknik açıdan, internet de dahil olmak üzere, bir bilişim sisteminin söz konusu olduğu durumda “girmek” kavramı yerine “erişmek” kavramının kullanılması yerinde olacaktır⁶⁴². Keza gerek atıf yapılan sözleşme maddesinde gerekse doktrinde söz konusu suçtan bahsedilirken “yetkisiz erişim” veya “hukuka aykırı erişim” kavramları kullanılmaktadır.

Anılan suçun internet açısından değerlendirmesinde, her unsuruyla doğrudan interneti de kapsamı bakımından suçun unsurları tek tek ele alınmak durumundadır. Bu bakımdan öncelikle *korunması amaçlanan hukuksal değere* bakılacak olursa, bu konuda farklı yaklaşımları görmek mümkündür. *Dülger'e* göre bu suçla sadece bir hukuksal değer korunmaya çalışılmamaktadır. Yazar, yetkisiz erişimin önüne geçilmesiyle, erişilmesi amaçlanan sistemin sahibi veya kullanıcılarının çıkarları, verilerin gizliliği, özel hayatlarının dokunulmazlığı ya da ihtiyaç duydukları güvenlik duygusunun korunması gibi bir çok hukuksal değerlerin korunmasının amaçlandığını savunmaktadır. *Dülger* tüm bu hukuksal değerleri kapsayan bir hukuksal değer tasarımına giderek “*bilişim sisteminin güvenliği*”

⁶³⁸ **MADDE 243.** - (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 hâlinde, 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.

⁶³⁹ **MADDE 2.-** Taraflardan her biri, bir bilgisayar sisteminin tamamına veya bir kısmına haksız bir şekilde erişim fiilinin, kasıtlı olarak yapıldığında kendi ulusal mevzuatı kapsamında cezai bir suç tanımlaması için gerekli olabilecek yasama işlemlerini ve diğer işlemleri yapacaktır. Taraflar söz konusu suçu, bilgisayar verilerinin elde edilmesi amacıyla veya sahtekarlığa yönelik başka bir amaçla güvenlik sistemlerinin ihlal edilmesi şeklinde, veya, başka bir bilgisayar sistemini esas alarak tanımlayabilirler.

⁶⁴⁰ **KARAGÜLMEZ**, Bilişim Suçları, sh: 169.

⁶⁴¹ **DÜLGER**, Bilişim Suçları, sh: 212; **YAZICIOĞLU**, Yılmaz, Bilişim Suçları Konusunda 2001 Türk Ceza Kanunu Tasarısının Değerlendirilmesi, in: Hukuk ve Adalet- Eleştirel Hukuk Dergisi, Yıl:1 – Sayı:1, İstanbul, 2004, sh: 177.

⁶⁴² Bilişim suçları bakımından “girmek” ve “erişmek” kavramları arasındaki ilişkinin ayrıntılı değerlendirmesi için bkz. **KARAGÜLMEZ**, Bilişim Suçları, sh: 169.

hukuksal değeri bünyesinde yukarıda sayılan tüm hukuksal değerlerin korunacağını dile getirmiştir⁶⁴³.

Kurt ise bilişim sistemine yetkisiz erişim suçu ile sistem sahibinin kişisel alanına girildiğini ifade etmiştir. Dolayısıyla yazar bilişim sistemine girme ve orada kalmaya devam etme suçunda korunan hukuksal değer olarak, özel hayatın gizliliği ve sırların masuniyeti olarak belirlenebileceğini ifade etmektedir⁶⁴⁴.

Konuyu farklı bir perspektiften ele alan *Karagülmez* maddenin düzenleniş biçimini esas alarak anılan suçun hukuki konusunun bilişim sisteminin güvenliği olduğu görüşünün tartışmalı hale geldiğini ifade etmektedir. Yazar, 243. maddede yer alan suçun maddi unsurunun sadece sisteme yetkisiz erişim olmadığı, bunun yanında sistemde kalmaya devam etme unsurunun da arandığından yola çıkarak, suçun unsurunun bu şekilde düzenlenişinin suçun hukuki konusunun belirlenmesinde de etkili olduğunu vurgulamaktadır. Bu açıdan bilişim sisteminin güvenliğinin korunmasına yönelik bir düzenlemede “*kalmaya devam etme*” şeklinde bir unsura yer verilmeyeceğini; aynı şekilde 2. fıkrada yer alan düzenlemenin de hukuki konunun bilişim sisteminin güvenliği olduğu düşüncesini zayıflattığını ifade etmektedir. Yazar bu görüşten yola çıkarak ve yine 243. maddede düzenlenen suçta “*kalmaya devam etme*” nin suçun unsuru olmasını esas alarak bu suçun hukuki konusunun bilişim sistemini kullananların belirli bir süreden sonra rahatsız edilmemesi ve devamında suçun hedefi durumundaki sistem kullanıcılarının (sahiplerinin) çıkarlarının zedelenmemesinin de hukuki konu kapsamında olduğu sonucuna varmaktadır⁶⁴⁵.

⁶⁴³ **DÜLGER**, Bilişim Suçları, sh: 214. Aksi yönde görüş için bkz. **KETİZMEN**, Bilişim Suçları, sh: 90.

⁶⁴⁴ “*Bilişim sistemi ve içinde bulunan veriler, programlar sistem sahibinin özel alanı da bulunmaktadır. Bu suç ile bu alana girilmesi suretiyle güvenlik ve sükun duygusunun sarsılması önlenmeye çalışılmıştır. Bilişim sistemi sahibinin kişisel alanına girilmektedir. Hak sahibi izin vermedikçe bu alana girilmesi mümkün değildir. Anayasanın 20. maddesindeki 'özel hayatın gizliliği'ne ilişkin maddesine paralel bir hüküm olarak karşınıza çıkmaktadır*” **KURT**, Bilişim Suçları, sh: 148. Ancak yazar aynı madde ile ilgili yaptığı açıklamanın devamında “*Genel olarak suçun konusu ile suç vasıtasıyla korunan hukuki değer her zaman aynı olmayabilir. Bu suçla da suçun konusu bilişim sistemi olmasına rağmen korunan hukuki değer kişisel verilerin korunmasıdır.*” demektedir. **KURT**, Bilişim Suçları, sh: 150.

⁶⁴⁵ **KARAGÜLMEZ**, Bilişim Suçları, sh: 167.

Son olarak *Ketizmen* ise, karşılaştırmalı hukuktan⁶⁴⁶ da örnek vererek md. 243'ün malvarlığının korunmasına ilişkin bir düzenleme olduğunu dile getirmektedir. Yazara göre, Türk Ceza Kanununda bilişim alanında işlenen suçlar içerisinde 243. maddede düzenlenen yetkisiz erişim suçunda bir zarar tehlikesinin esas alındığı görülmektedir. Bu haliyle de yetkisiz erişim suçunun hukuki konusu, 243. maddede düzenlendiği şekliyle, malvarlığının korunması kapsamında mala zarar verme suçunun özel şekli olarak düzenlenen 244. maddenin hukuki konusu ile paralellik arz etmektedir. Bu açıdan 243. maddede düzenlenen yetkisiz erişim suçunun hukuki konusu, sisteme ve veriye yönelik zarar verici fiillerin engellenmesi anlamında bir tehlike suçu olarak, genel bir ifade ile mülkiyetin korunmasıdır⁶⁴⁷.

Kanaatimizce bu suçla korunması amaçlanan hukuksal değer konusunda karma bir bakış açısının kabul edilmesi isabetli olacaktır. Buna göre her şeyden önce suç teşkil eden erişim yetkisiz olduğuna göre, burada söz konusu bilişim sistemine girmek için yapılan yetkilendirme bir mülkiyet kurumunun tesisini gündeme getirebilir. Yine yetkisiz erişimle aynı zamanda mülkiyetten bağımsız olarak bilişim sisteminin güvenliği de zarara uğratılmaktadır⁶⁴⁸. Dolayısıyla belirtilen her iki hukuksal değer de aynı anda korunmasının amaçlandığını kabul etmek daha isabetli olacaktır.

Suçun konusu, kanunun ifadesiyle, bilişim sistemidir. Bilişim sistemi kavramı madde gerekçesinde şöyle tanımlanmaktadır.

“ Bilişim sisteminden maksat, verileri toplayıp yerleştirdikten sonra bunları otomatik işlemlere tâbi tutma olanağını veren manyetik sistemlerdir.”

⁶⁴⁶ Yazar 243. maddenin esinlendiği Fransız Ceza Kanununda yetkisiz erişim suçuna ilişkin 323-1. maddesinin malvarlığına karşı suçlar arasında düzenlendiğini ifade etmiştir. Ayrıntılı bilgi için bkz. **KETİZMEN**, Bilişim Suçları, sh: 95 v.d.

⁶⁴⁷ **KETİZMEN**, Bilişim Suçları, sh: 99.

⁶⁴⁸ Yetkisiz erişim ile ilgili yeni bir hak kategorisi olarak bilişim sistemlerinin gizliliği ve bütünlüğünün korunmasını bekleme hakkı için bkz. 1.8.- nternet Bakımından Modern Ceza Hukuku Anlayışının Normatif Alana Yansımasına Örnek Olarak Federal Alman Anayasa Mahkemesinin 27.02.2008 Tarihli “Online-Araştırma” Kararı, sh: 77 .v.d.

Bu tanım, özellikle konu internet açısından değerlendirildiğinde, amaca uygun olmaktan uzak ve çok tehlikeli bir tanımdır. Her şeyden önce tanımda bilişim sisteminin en karakteristik özelliği olarak manyetikliği dikkat çekmektedir. Dolayısıyla manyetik olmayan bir unsurun bilişim sistemi kavramı dahilinde düşünülmesi imkansızlaştırılmıştır. Ancak şu ana kadar elde edilebilen tanım örneklerinin hiç birinde internetin manyetikliği üzerine bir özelliğe rastlanmamıştır. *Yazıcıoğlu*'nun da isabetle ifade ettiği gibi⁶⁴⁹, yasa koyucunun tercih ettiği tanım her ne kadar bilgisayar üzerinden bir bilişim sistemini ortaya koymaya çalışsa da bilgisayar bakımından bile yetersiz ve bilişim sisteminin özelliğini ortaya koymaktan uzaktır. İnternetin bu bahiste böyle bir tanım üzerinden bir bilişim sistemi olarak kabulü çok zordur. Dolayısıyla tüm bilişim alanında işlenen suçlara sirayet eden bu tanım üzerinden internetin araç olarak kullanıldığı bilişim suçlarının bu kapsamda değerlendirilmemesi gibi çok büyük bir tehlike kendini göstermektedir. Ancak bunun mümkün olmadığı bilinmektedir ve bundan sonraki tüm açıklamalar da internetin bir bilişim sistemi unsuru olarak kabul edildiği gerçeği üzerinden yapılacaktır.

Suçun *maddi unsuru* internet açısından incelenecek olursa, md. 243/ 1'e göre bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak girmek ve orada kalmaya devam etmek suçun maddi unsuru olarak belirlenmiştir. Madde yan başlığı, madde metni ve maddenin gerekçesi karşılaştırıldığında özellikle maddi unsur ile ilgili bir takım çelişkilerin varlığı dikkati çekmektedir. Öncelikle madde yan başlığı "bilişim sistemine girme" iken birinci fıkrada maddi unsur bilişim sistemine girmek ve orada kalmak olarak düzenlenmiştir. Bunun dışında, tasarıda bahse konu suçunun düzenlendiği maddede "*bir bilişim sistemine giren veya orada kalmaya devam eden*" hükmü mevcut iken TBMM Genel Kurul görüşmeleri sırasında bu maddeye ilişkin değişiklik önergesi verilmiş ve bu hüküm "*bir bilişim sistemine giren ve orada kalan*" olarak kabul edilmiştir⁶⁵⁰. Bu değişikliğe rağmen, madde gerekçesi tasarıdaki hükme göre yapıldığı için ve yapılan değişikliğe rağmen değişiklik madde gerekçesine yansıtılmadığından hali hazırda madde gerekçesine göre suçun maddi unsuru bir bilişim sisteminin tamamına veya bir kısmına hukuka aykırı olarak girmek veya orada

⁶⁴⁹ YAZICIOĞLU, Yeni Türk Ceza Kanunundaki Bilişim Suçları, sh: 404.

⁶⁵⁰ Bu önerge ve değişikliğe ilişkin görüşmelerde, değişiklik gerekçesi şöyle dile getirilmiştir: "*Biliyorsunuz bir de bilgisayar sistemin bozan hackerlar var, onlar size bir şey gönderdi, üzerine tıkladınız ve bir sisteme girdiniz. Hemen bunu suç haline getirirsek, çok geniş bir kapsama almış oluruz, suç kapsamını genişletmiş oluruz: Burada da – hazırladığımız taslakta- girme ve orada kalma şartını koyduk; çünkü bu bir kasıttır. Kazara girersiniz çıkarırsınız, bu başka bir şey; ama, girdiniz, kaldınız, değiştirdiniz, bozdunuz, bu farklı bir şey. İşte tasarıda, buraya açıklık getirdik...*" denmiştir.

kalmaktır. Anılan deęişiklikten sonra sadece madde metni ile gerekçe arasında deęil maddenin fıkraları arasında da çelişkilere rastlanmaktadır. Maddenin birinci fıkrasında “veya” bağlacı “ve” olarak deęiştirildięi için, tasarıdaki seçimlik hareketler tek bir harekete dönüştürülmüştür. Ancak hemen ikinci fıkrada “yukarıda tanımlanan fiiller...” demek suretiyle birinci fıkrada birden çok fiilin varlığı öngörülmektedir⁶⁵¹. Tüm bu çelişkilere maddenin düzenlenişindeki kararsızlık ve itinasızlığı ortaya koymaktadır.

Bir bilişim sistemine kısmen veya tamamen hukuka aykırı olarak girme ve orada kalmaya devam etme fiili unsurları bakımından ikiye ayırmak mümkündür. Birinci unsur girme unsuru ikinci unsur ise orada kalmaya devam etme unsurudur. Bir bilişim sistemi olarak internette⁶⁵² yaygın kullanılan tabirle yetkisiz erişim, kanunun ifadesiyle hukuka aykırı girme sıklıkla karşılaşılan bir ihlal modelidir. Burada internetteki herhangi erişimde hukuka aykırılık durumu, erişimde yetkili olmayla ilgili olup bu konu hukuka aykırılık unsurunu tartışılırken ele alınacaktır. Maddenin kapsamı anlamında “girmek” kavramı, Türkçeye erişim olarak çevrilen “access” teriminin karşılığı olarak kullanılmıştır⁶⁵³. Ancak doktrinde, bizim de katıldığımız üzere, bu terimin fiziksel bir alana erişilmesini ya da girilmesini çağrıştırdığı, fakat bilişim sistemine girişin bu açıdan imkânsız olduğunu belirtilmiştir⁶⁵⁴. İnternet ortamında gerçekleşen yetkisiz erişim fiillerine ilişkin en önemli örnekler, kullanımı sadece üyelerine özgülenmiş internet sitelerine veya internet üzerinden verilen hizmetlere usulüne aykırı olarak erişmek, belli fonksiyonları(okuma, kopyalama, nakletme, v.b.) engellenmiş veya koruma altına alınmış verilerin bu fonksiyonlarını getirilen engelleri aşarak aktif hale getirmektir. Bu örnekleri çoğaltmak mümkündür. **Kanaatimizce teknik anlamda internet aracılığıyla gerçekleşen yetkisiz erişimden bahsedebilmek için şu aşamaların gerçekleşmiş olması gerekmektedir.**

i.- Her şeyden önce internet ortamında konusu veya nitelięi ne olursa olsun verilen hizmetin kamusal erişilebilirliğinin söz konusu olmaması gerekmektedir. Başka bir deęişle,

⁶⁵¹ Madde metni ile madde gerekçesi arasındaki çelişki ile ilgili ayrıntılı bilgi için bkz. **KARAGÜLMEZ**, Bilişim Suçları, sh: 169; **KURT**, Bilişim Suçları, sh:151.

⁶⁵² *Ketizmen* interneti bir bilişim sistemi olarak kabul etmektedir. Ayrıntılı bilgi için **KETİZMEN**, Bilişim Suçları, sh: 19 v.d.

⁶⁵³ **ÇÖLKESEN**, Rıfat/ **ÖRENCİK**, Bülent, Bilgisayar Haberleşme ve Ağ Teknolojileri, İstanbul, 2003, sh: 390.

⁶⁵⁴ **KARAGÜLMEZ**, Bilişim Suçları, sh: 170.

md. 243 anlamında bir yetkisiz erişimden bahsetmek için ilk önce erişimi sınırlandırılmış bir internet ortamından bahsetmek gerekmektedir. Örneğin herkesin o an erişebileceği bir internet sitesinin veya internet üzerinden hizmetin yetkisiz erişim suçuna konu olamayacağı kesindir. Çoğu zaman internet üzerinden alışveriş imkanı sunan firmalar veya değişik konularda bilgi kaynağı içeren portallar sadece kullanıcılarını kayıt altına almak için, özel bir prosedürel ya da teknik işlem söz konusu olmadan, bir takım bilgileri almak suretiyle üyelik işlemi gerçekleştirmektedirler. Bunun dışında daha özel yetkilendirme süreçlerine de rastlanılmaktadır. Örneğin sorumlusu olduğu derslere ilişkin not girişlerini internet ortamında gerçekleştiren bir öğretim üyesinin, bu girişi gerçekleştirebilmek için ilgili portala erişimini sağlayacak kullanıcı adı veya şifresi gibi. Bu tür durumlarda bahsi geçen servise bağlanmak veya hizmeti almak sadece bu yönde yetki almış kullanıcılara özgülenmiştir. Bir bakıma erişim sınırlandırılmıştır.

Konunun daha net anlaşılması için aynı örnek üzerinden iki durumu yansıtmakta fayda vardır. Bir gazetenin internet sitesinden o günün gazete bilgilerine rahatlıkla ve herkes tarafından erişim mümkün iken gazetenin arşiv bölümüne veya özel bir ekine erişim sadece üye kaydı olan kullanıcılara özgülenebilir.

ii. Erişimi mümkün kılacak yetkinin usulüne uygun olarak alınmış olması gerekmektedir. Bu noktada gerekli yetkinin alınmasında hangi usuli prosedürlere riayet edileceği sınırlandırmayı gerçekleştiren yönetici birim tarafından belirlenmektedir. Belirlenen prosedür ve kurallar dışında erişim için gerekli unsurlar temin edilmiş olsa bile usulüne uygun bir yetkilenme gerçekleşmediği için yetkisiz erişim söz konusu olacaktır. Ayrıca usulüne uygun alınmış bir kullanıcı adı ve şifresinin bir başka kişi tarafından sahibinin rızası hilafına hukuka aykırı bir şekilde temin edilmesi ve bu suretle erişimin sağlanması durumunda da yetkisiz erişimin gerçekleştiği kabul edilmelidir.

Bu hususta son olarak vurgulanması elzem görünen nokta da, usulüne uygun olarak alınmış bir yetkinin aşılması suretiyle erişimin gerçekleşmesi durumudur. Erişimi sınırlandırılmış bir internet sitesine erişim konusunda yetkilendirilen kullanıcının yetkisi de sınırlandırılabilir. Örneğin bir veri tabanına internet üzerinden erişimi mümkün kılan kullanıcı adı ve şifrenin girilmesiyle ilgili veri tabanına erişilmiş olmasına karşın bu durum veri tabanı içindeki veriler üzerinde her türlü işlemi yapma yetkisini otomatik olarak kullanıcıya vermeyebilir. Kullanıcıya verilen yetki sadece verinin okunmasıyla sınırlı olabilir. Veri

üzerinde işlem yapma, veriyi kopyalama veya nakletme yetkileri veriye erişen kullanıcı açısından da sınırlandırılmış olabilir. Bu sınırlandırmaya rağmen kullanıcı kendine tanınan yetki dışında bir işlem gerçekleştirmek suretiyle bir erişim sağlarsa hukuka uygun gerçekleşen erişim hukuka aykırı hale gelir ve yetkisiz erişim gerçekleşmiş olur.

iii.- Yetkisiz erişimi, internet açısından yapılan değerlendirmede sadece internet ortamında gerçekleşen eylemle sınırlı tutmak hata olur. Bilindiği gibi günümüzde internet aracılığıyla dünyanın her yerindeki bilgisayarlar birbirlerine bağlanmaktadır. Böylece internete bağlı tüm bilgisayarların içerik ve kayıtlarına internet aracılığıyla diğer kullanıcılar tarafından erişim teknik anlamda mümkün hale gelmiştir. Bu durum özellikle son yıllarda sayıları gittikçe artan casus veya kötücül yazılımlar aracılığıyla kötüye kullanılmakta ve tüm bilgisayarlarda kayıt altına alınmış tüm verilere sahibinin rızası olmaksızın erişilebilmekte ve bu veriler ele geçirilebilmektedir⁶⁵⁵. Bir bilişim sistemi olarak bilgisayarlara internet aracılığıyla hukuka aykırı olarak erişim sağlamışsa bunu da internet aracılığıyla gerçekleşmiş yetkisiz erişim olarak kabul etmek gerekmektedir.

243. maddenin *tipe uygun eylem unsuru* bakımından, kanunun kullandığı ifade ile “*bilişim sistemine hukuka aykırı girme*” yi internet açısından değerlendirdikten sonra ikinci unsur olan “orada, yani erişilen bilişim sisteminde, kalmaya devam etmek üzerinde durmakta fayda vardır. Yetkisiz erişim suçunun gerçekleşmesi için sadece sistemin bütününe ya da bir kısmına hukuka aykırı olarak girme yeterli olmamakta, sistemde kalınmaya devam edilmesi de gerekmektedir. Sisteme girme ve orada kalmaya devam etme, bir bütün olarak, md. 243’de düzenlenen yetkisiz erişim suçununun maddi unsurunu oluşturmaktadır.

Kapsam olarak yetkisiz erişimin sağlandığı sistemde bulunmaya devam etmek konusunda herhangi bir tartışmaya rastlanmamaktadır. *Kanaatimizce* bu hususta tartışılması gereken iki nokta vardır. Birincisi md. 243’deki suçun maddi unsuru bakımından bilişim sistemine girme ve orada kalmanın tek bir fiil olup olmadığı sorunu ikincisi de, bir bilişim sistemine hukuka aykırı olarak girildikten sonra orada kalma unsurunun aranmasının gerekli olup olmadığıdır.

⁶⁵⁵ Bu konudaki örnekler için bkz. **Kişisel Verilerin Kaydedilmesi, sh: 276. vd.**

Daha önce de değinildiği üzere 5237 sayılı TCK'nin TBMM görüşülmesi esnasında 234. maddede bir değişiklik önerisiyle tasarıda yer alan “*bir bilişim sisteminin tamamına veya bir kısmına hukuka aykırı olarak giren veya orada kalan ...*” hükmünde “veya” bağlacı “ve” olarak değiştirilmiştir. Bu değişikliğin gerekçesini de *Kurt* şöyle ifade etmektedir;

*“Sistemde kalmaya devam etmek’ tanımlamasının suçun tamamlayıcı unsuru haline getirilmesi, kötü niyeti olmayıp da kısa süreliğine giriş yapan, araştırma amacı taşıyan, ya da yazdığı yazılımın başarısını test etmek isteyen kişilerin yaptıkları sisteme girme eylemlerini de çok katı bir düzenleme ile münhasıran suç saymama düşüncesinden kaynaklanmaktadır.... Ancak, yine de bu düşüncelerle olsa dahi sadece sisteme girmeleri suça teşebbüs olarak değerlendirilecektir, Kanununun bu tarzda bu tür eylemleri aynı kefeye koymaması isabetli olmuştur.”*⁶⁵⁶

Bu ifadeden de anlaşılacağı üzere bu değişiklikle “*sistemde kalmaya devam etmek*” ile “*bilişim sistemine hukuka aykırı olarak girmek*” aynı fillin iki unsuru haline getirilmiştir. Girme ve orada kalmaya devam etmenin birbirinden bağımsız iki farklı hareketi oluşturmadığının kabul edilmesi halinde, maddede düzenlenen suçun mütemadi (kesintisiz) suç olduğunun kabulü bir zorunluluk olacaktır. Bu durumda sisteme girme sonrasında, sistemde kalmaya devam edilmesi şartı, suçun tamamlanmış sayılabilesinin belirli bir sürenin aranmasını da beraberinde getirecektir. *Karagülmez* göre, madde metninde yer alan “*orada kalmaya devam eden*” ifadesinin “*kalan*” ifadesinden daha geniş bir anlamı çağrıştırmakta ve yazar “*kalmaya devam etme*”nin, “*kalma*” ya göre daha nitelikli olduğunu, daha uzun süren bir temadiyi işaret ettiğini ve sonrasında kalmaya devam etme unsuru için yeterli süre araştırmasının her somut olayın özelliğine göre belirlenmesi gerektiğini savunmaktadır⁶⁵⁷. *Kurt* ise, sisteme girdikten sonra orada kalmaya devam etmenin sisteme giren failin sistem içerisinde bir süre kalması şeklinde gerçekleşebileceğini belirtmiştir. Bu süre zarfı içerisinde yetkisiz erişimi sağlayan fail sistem içerisindeki verileri kontrol edebilir, veri akışını izleyebilir, veriler üzerinde oynama yapabilir veya sistemi bozmaya yönelik işlemler yapabilir, yahut da hiçbir şey yapmayabilir.⁶⁵⁸

⁶⁵⁶ **KURT**, Bilişim Suçları, sh: 148.

⁶⁵⁷ **KARAGÜLMEZ**, Bilişim Suçları, sh: 168 – 169.

⁶⁵⁸ **KURT**, Bilişim Suçları, sh: 149.

Kanaatimizce, sistemde kalmaya devam etme gibi muğlak bir ifadenin uygulama bakımından sorunlara yol açacağı kesindir. Ayrıca her somut olayda bu sürenin belirlenmesinin önerilmesi de, tespitin her zaman kolaylıkla yapılamaması gerçeğinden hareketle sorunun aşılması bakımından kesin sonuç vermeyebilecektir. Şayet korunması amaçlanan hukuksal değer tercihinde bilişim sisteminin güvenliği de esas alınabilirse, o halde başka bir hukuksal değer ihlalinin yaşanmasını beklemek gereksizdir. Başka bir ifade ile bilişim sistemine yetkisiz erişim sağlandığı anda suçun işendiğinin kabulü daha amaca uygun bir düzenlemeyi işaret etmektedir. Hiç şüphe yok ki üzerinde tartışılan alan bilişim teknolojisinin en ileri seviyelerinden biri olan internettir ve genel anlamda bilişim teknolojileri için saniyeler ve hatta saliseler bile bazen sistemde yeteri kadar kalmayı sağlayabilecek zaman dilimlerini teşkil edebilir. Zaten maddenin devamında yetkisiz erişimle birlikte bir veri zararının söz konusu olması nitelikli hal olarak düzenlenmiştir. Ayrıca bir verinin transferi de bir sonraki madde olan 244. maddede göz önünde bulundurulmuştur. Bu nedenle bu düzenlemede kalmaya devam etme unsuru üzerinde ısrarcı olmayı isabetli görmemekteyiz.

Hukuka aykırılık unsuru konusunda rızanın bir hukuka uygunluk nedeni olarak dikkate alınıp alınmayacağı konusuna gelince, burada ikili bir ayrımı esas almak gerektiği *kanaatindeyiz*. Öncelikle erişimin sağlanması esnasında rızanın varlığı durumu, ikinci olarak da rıza ile girilen bir bilişim sisteminden rıza ortadan kalkmasına rağmen çıkmamak. Birinci alternatifte zaten erişimin yetkisiz olması suçun oluşmasını sağladığı ve rıza ile erişim için açık veya örtülü bir yetkilendirmenin söz konusu olduğu düşünülecek olursa erişim esnasında verilecek rızanın hukuka aykırılığı kaldırdığını kabul etmek yerinde olacaktır. İkinci ihtimalde ise, yasa koyucu tipe uygun eylem unsuru bakımından yetkisiz erişimin sağlanması ve orada kalmaya devam edilmesinin gerçekleştiği anda suçun tamamlandığını kabul ettiğine göre ve kanunilik prensibi gereğince her ne kadar isabetli bulsak da bu gerçek üzerinden hareket edileceğinden rıza ile girilen bir bilişim sisteminden rızanın ortadan kalkmasından itibaren çıkılmaması suç henüz tamamlanmadan hukuka uygunluk nedenin ortadan kalması nedeniyle eylemi hukuka aykırı hale getireceği *kanaatindeyiz*. Benzer bir yaklaşımın konut dokunulmazlığını ihlal suçunda da var olduğunu ifade etmek gerekmektedir. Akis yönde görüş belirten *Ketizmen* göre, söz konusu suçun kaleme alınışından anlaşılan odur ki, sisteme hukuka uygun bir şekilde girilmesi sonrasında rızanın ortadan kalkması ya da diğer nedenlerle

hukuka aykırılığın gerçekleşmesi durumunda failin sistemde kalmaya devam etmesi, girişin hukuka aykırı olması şartı arandığından, 243. madde kapsamında değildir.⁶⁵⁹

Yetkisiz erişim suçu bakımından suçu etkileyen haller değerlendirildiğinde 243. maddenin 2. fıkrasında, fiilin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi, cezada indirim sebebi olarak kabul edilirken 3. ve son fıkrasında fıkrada sistemin içerdiği verilerin değişmesi ve de yok olması halinin ise ağırlatıcı neden olarak düzenlendiği görülmektedir.

Maddenin ikinci fıkrasında düzenlenen bedeli karşılığı yararlanabilen sistemler dahilinde nelerin öngörüldüğü ve böyle bir durumun, yani bedeli karşılığı yararlanılan sistemlere yetkisiz erişimin niçin hafifletici neden hükmünde değerlendirildiği konusunda ne madde metninde bir açıklık ne de gerekçede bir değerlendirme bulunmaktadır. Bu konuda doktrinde farklı değerlendirmelere rastlamak mümkündür.

Dülger, bedeli karşılığı yararlanılabilen sistem ifadesinin genel olarak dört durumu kapsadığını ifade etmiştir. Yazara göre İnternet üzerinden ücret karşılığı hizmet veren web siteleri, “*internet kafe*” gibi yerlerde olduğu üzere belirli bir bedel karşılığı bilişim sisteminin kiralanması, bir kuruluş tarafından belli bir sistemin bedel karşılığında sunulması (örneğin sağlanan anlaşmayla kişilerin cep telefonlarına bilişim sistemi üzerinden reklam amaçlı mesaj çekilmesi) ve de belirli bir zaman ya da dönem sınırlaması ile İnternet bağlantı servisinin sağlanması bedeli karşılığı yararlanılabilen sistem kapsamındadır⁶⁶⁰.

Madde düzenlenmesinin karışıklıklara sebebiyet verecek ölçüde muğlak olduğunu savunan *Karagülmez*, dar bir yorumla belirli bir ücret karşılığında hizmet veren web sayfalarının bu kapsamda düşünülebileceğini belirtmektedir. Ancak yazar, tarafımızca da isabetli kabul edilen bir tespitle, internet kafe ve benzeri yerlerde bedeli karşılığında sistemin kullanılmasının bu kapsamda düşünülemeyeceğini ifade ederek maddede sistemin kullanıldığı

⁶⁵⁹ Aksi yönde AKIN, Akın, Bilişim Suçu, in: Yaklaşım, Y: 14, S: 157, Ankara, 2006, sh: 268.

⁶⁶⁰ DÜLGER, Bilişim Suçları, sh: 226-227.

mekanın değil sistem içerisindeki elektronik yapıda sunulan ücretli hizmetleri vurguladığını savunmaktadır.⁶⁶¹

Yazıcıoğlu ise, bu fıkrada düzenlenen hafifletici sebebi, ücreti karşılığı hizmet veren sistemlere girilmesi şeklinde yorumlamakta ve devamında ve bu düzenlemenin yetkisiz erişim suçunun uygulanmasının genişliğinden doğacak sakıncaları gidermesi bakımından isabetli olduğunu ifade etmektedir⁶⁶².

Kanaatimizce, böyle bir indirim nedeni, yukarıda yapılan hukuksal değer tercihi çerçevesinde isabetsiz olmuştur. Yinelenecek olursa, bu suçla hem bilişim sisteminin güvenliği hem de o sistemin kullanımının sadece yetkilendirilen kişilere açılmasından dolayı sistem içi veri mülkiyetinin veya zilyetliği koruması amaçlanmaktadır. Şayet bedeli karşılığı hizmet veren bir bilişim sistemine, örneğin bir web sayfasına, yetkisiz erişimi hafifletici bir durum olarak kabul edilecek olursa, o halde bedeli ödenmeden o sistemin kullanılıyor olmasından ötürü bilişim sistemin işleticisi ve onun sistem üzerindeki hakları ikinci plana atılmış olacaktır ki bu söz konusu düzenleme bakımından bir çelişkiye neden olmaktadır. Bu nedenle böyle bir hafifletici nedenine ihtiyaç olmadığı *kanaatindeyiz*.

Maddenin üçüncü ve son fıkrasında sisteme yetkisiz erişim sonucunda sistem içerisindeki verinin değişmesi veya yok olması ağırlatıcı neden olarak düzenlenmiştir. *Ketizmen* bu durumu 5237 sayılı TCK md. 23’de düzenlendiği şekliyle, neticesi sebebiyle ağırlaşan bir suç olarak kabul ederken ilgili ağırlatıcı nedenin uygulanabilmesi için failde verinin değiştirilmesi ya da yok edilmesi yönünde bir kastının olmaması gerektiğini ifade etmektedir⁶⁶³. Aksi takdirde kasıtlı olarak işlenmesi halinde 244. maddenin 2. fıkrasında yer alan hüküm gündeme gelecektir⁶⁶⁴. Konuya ilişkin detaylı açıklamalar md. 244’ün değerlendirilmesinde yapılacağı için bu bölümde bu belirlenimin ortaya konulmasıyla yetinilecektir.

⁶⁶¹ **KARAGÜLMEZ**, Bilişim Suçları, sh: 174-175.

⁶⁶² **YAZICIOĞLU**, Yeni Türk Ceza Kanunundaki Bilişim Suçları, sh: 407.

⁶⁶³ **YAZICIOĞLU**, Yeni Türk Ceza Kanunundaki Bilişim Suçları, sh: 407.

⁶⁶⁴ Aynı yönde **KARAGÜLMEZ**, Bilişim Suçları, sh: 177.

Son olarak da suçun özel görünüş şekilleri üzerinde durulacak olursa, md. 243'de düzenlenen yetkisiz erişim suçunun, hareketle netice arasında ayırım yapma imkanını varlığı dolayısıyla, teorik olarak teşebbüse elverişli olduğunu söylemek mümkündür. Zira yasa koyucu, yukarıda da ifade edildiği üzere, suçun oluşumu için başlı başına yetkisiz erişimin gerçekleşmesini değil bununla birlikte ayrıca belli bir süre sistem içinde kalmayı da aradığından, her somut durumda suçun gerçekleşmesini mümkün kılacak sürenin tamamlanmasından önce kendi iradesi dışında – örneğin sistemin güvenlik yazılımları tarafından sistem dışına çıkartılması veya işlem esnasında elektriklerin kesilmesi neticesinde sistemden otomatikman çıkma gibi - sistem dışına çıkartılırsa bu durumda md. 243'de düzenlenen yetkisiz erişim suçunun teşebbüs aşamasında kaldığı kabul edilebilir. Ancak teorik olarak mümkün görünen bu durumun uygulamada tespit edilmesinde bir takım güçlüklerin yaşanabileceği de ifade edilmelidir.

İştirak konusunda ayrıca bir değerlendirmeyi gerekli kılacak özellikli bir durum gözlenmezken içtima konusunda özellikle fikri içtima konusunda bir takım örneklerle değerlendirmelerde bulunmak gerekecektir. Suç tipinin özelliği gereğince md. 243'deki suç teşkil eden fiil icra edilirken aynı anda o bilişim sistemi üzerinden, özellikle internet üzerinden, kurulan haberleşmenin engellenmesi, herhangi bir verinin kasten tahrip edilmesi veya kullanılamaz hale getirilmesi, bir bilişim sisteminin yazılım ve donanımının bir bütün olarak ele alındığı bir durumda yetkisiz erişim esnasında kullanılamaz hale getirilen bir verinin veya programın donanımı da kullanılamaz hale getirmesi sonucu mala zarar vermenin gerçekleşmesi gibi durumlarda md. 44 anlamında fikri içtimanın söz konusu olduğunu ifade etmek mümkündür. Ancak burada dikkat edilmesi gereken husus tüm bu suçların fiil farklılaşmadan gerçekleşmesinin bir zorunluluk olmasıdır. Çünkü örneğin yetkisiz erişim sağlandıktan sonra yani md. 243 gerçekleştiikten sonra bahsi geçen neticelerin doğması nedeniyle diğer suçların işlenmesi halinde birbirinden bağımsız suçların gerçekleştiği kabul edilmelidir. Bir örnek vermek gerekirse, bedeli karşılığı yararlanılan bir web sitesine yetkisiz erişimin sağlandığı ve failin bu web sitesinin hizmetlerinden herhangi bir bedel ödemediği yararlandığı bir durumda, md. 243 sadece yetkisiz erişimi suç olarak düzenlediği için burada hem md. 243 anlamında yetkisiz erişim hem de md. 163/2 anlamında karşılıksız yararlanma suçu işlenmiş olacaktır.

1.3.7.- Bilişim Sistemini Engelleme, Bozma, Veriler Yok Etme veya Değiştirme

5237 sayılı TCK'de düzenlenen ve internetin bir araç olarak kullanılabilceği suçlar içinde en önemli suçların başında md. 244'de düzenlenen "bilşim sistemini bozma, engelleme, verileri yok etme veya deęiştirme" suçudur. Çünkü bu suç nitelik ve düzenleniş şekli bakımından birçok suç tipi ile oldukça yakın ilişkili olup bu suçlarla karıştırlma riskleri içermektedir. Aşağıda da deęerlendirileceęi üzere 765 sayılı TCK dönemi de dahil olmak üzere uygulamada bu suç ve bağlantılı dięer suçlar arasında çelişkili kararlara imza atılmaktadır. Özellikle maddenin birinci ve ikinci fıkraları ile md. 151'de düzenlenen mala zarar verme suçu, üçüncü üçüncü fıkrası ile md. 245'de düzenlenen banka ve kredi kartlarının kötüye kullanımı suçu ve nihayet dördüncü fıkrası ile md. 142/ 2- e'de düzenlenen nitelikli hırsızlık ve md. 158/ 1- f'de düzenlenen nitelikli dolandırıcılık suçları birbirleriyle karıştırlmaktadır. Bu ilişki bakımından kilit madde 244. madde olduğundan anılan suç tiplerinin bu madde kapsamında ele alınarak internet ile ilişkisinin deęerlendirilmesi *kanaatimizce* metodolojik açıdan daha isabetli olacaktır. Dolayısıyla 244. maddenin internet ile ilişkisi deęerlendirilirken mala zarar verme, nitelikli hırsızlık ve nitelikli dolandırıcılık suçlarının da internet ile ilişkisi de ele alınacaktır.

244. maddenin internet ile olan ilişkisi deęerlendirilirken, öncelikle korunması amaçlanan hukuksal deęer unsuru üzerinde durmak gerekecektir. İnceleme konusu maddenin Avrupa Konseyi Siber Suç Sözleşmesi'ndeki karşılığı olan 4. ve 5. maddelerdir. Buna göre md. 4'de verilere müdahale fiilleri düzenlenmiştir. Bu madde ile maddi varlığı olan şeylere yönelik zarar verme girişimlerine korumaya benzer bir şekilde bilgisayar veri ve programlarına yönelik fiillerin korunmak istendięi, bu açıdan verinin bütünlüğü ve düzgün bir şekilde çalışması ve kullanımının korunmasının amaçlandığı belirtilmektedir⁶⁶⁵. Buna karşın

⁶⁶⁵ Bu hükmün amacı, bilgisayar verilerini ve bilgisayar programlarını da, fiziksel nesnelere gibi, kasıtlı hasar verme girişimlerine karşı koruma altına almaktır. Burada koruma altına alınan yasal hak, saklanan bilgisayar veri ya da bilgisayar programlarının bütünlüğü ve uygun biçimde çalışmaları ve kullanımınıdır. Paragraf 1'de, örtüşen fiiller olarak "tahrip etmek" ve "bozmak", özellikle veri ve programların bütünlüğünün ya da bilgi içeriğinin olumsuz biçimde deęiştirilmesiyle ilişkilidir. Verilerin "silinmesi", fiziksel bir cismin imhasına eşdeğerdur. Veriler imha edilir ve tanınmaz hale getirilir. Bilgisayar verilerinin erişilmez kılınması, verilerin saklandığı bilgisayara ya da veri taşıyıcısına erişimi olan bir kişi için verilerin ulaşılabilirliğini önleyen ya da sona erdiren herhangi bir fiil anlamındadır. "Deęiştirme" terimi mevcut verilerin farklı bir hale getirilmesi anlamındadır. Virüs ve Truva atı gibi kötü amaçlı kodların sisteme sokulması da, bu nedenle, verilerin sonuçta farklı bir hale gelmesi gibi, bu paragrafın kapsamındadır. Yukarıdaki fiiller ancak "haksız biçimde" gerçekleştirildiği takdirde cezalandırılabilir. Ağların tasarımının ayrılmaz bir parçası olan yaygın faaliyetler veya işletmeyle ilgili ya da ticari yaygın uygulamalar -örneğin bir bilgisayar sisteminin güvenliğinin sahibi ya da işletmecisinin izniyle test edilmesi ya da korunması, ya da sistemin işletmecisi yeni bir yazılım edindiğinde (örneğin İnternet'e erişim sağlayan, daha önce yüklenmiş benzer programları çalışmaz hale getiren bir yazılım) bilgisayarın işletim sisteminin konfigürasyonunun deęişmesi- haklı biçimde gerçekleştirilmektedir ve dolayısıyla bu Madde

md. 5’de ise sisteme müdahale eylemleri düzenlemiştir. ,Bilgisayar sabotajı olarak da kabul edilen bu madde kapsamında da özellikle sistemin işleyişini engelleyecek veya zora sokacak eylemlerin engellenmesi, böylece hak sahibi kişi yada kuruluşların bilişim sistemlerini uygun bir biçime işletme haklarının korunduğu dile getirilmektedir⁶⁶⁶.

Doktrinde de konu ile ilgili farklı görüşler ortaya konulmuştur. 765 sayılı TCK döneminde bu suçun karşılığı olan md. 525/ b – 1’in mala zarar verme suçu ile ilişkisi üzerinde durulmuştur. Anılan hükümde yer alan bilişim sistemine ve veriye zarar verme suçu bakımından *Dönmezer*, bu suç ile sisteme ve içeriğine karşı mala zarar verme fiillerinin işlendiğini, bu bakımdan da bu maddeyle mülkiyet hakkının korunduğunu ifade etmektedir⁶⁶⁷. Benzer bir değerlendirme ile *Önder* de bu suçun klasik mala zarar verme suçu olarak değerlendirilmesi gerektiğini ifade etmiştir.⁶⁶⁸ Yine mala zarar verme suçundan hareket eden *Yazıcıoğlu* ise bu suçun klasik mala zarar verme suçunun özel bir şekli olduğunu, bu suçun sistem ve içeriğini esas alan mala zarar verme fiillerini kapsadığını ifade etmiştir⁶⁶⁹. *Ersoy* ise bu suç ile kişinin malvarlığının korunduğunu belirtmiştir⁶⁷⁰.

5237 sayılı TCK md. 244 düzenlemesi karşında mütalaa edilen hukuksal değer yaklaşımlarına da bakılacak olursa; yukarıda 765 sayılı TCK’de yapılan düzenleme çerçevesinde klasik mala zarar verme suçu görünümü nedeniyle mülkiyetin korunduğunu savunan *Yazıcıoğlu*, 5237 sayılı TCK md. 244 düzenlemesi karşısından verinin “mal”

çerçevesinde suç olarak tanımlanmamaktadır. Anonim iletişimleri kolaylaştırmak amacıyla trafik verilerinin farklı bir hale getirilmesi (örneğin anonim yeniden postalama sistemleri), ya da güvenli iletişim amacıyla verilerin farklı bir hale getirilmesi (örneğin şifreleme), ilke olarak gizliliğin meşru bir koruması olarak görülmeli ve haklı biçimde yapılmış oldukları kabul edilmelidir. Ancak, Taraflar, anonim iletişimle ilgili belli suiistimalleri, örneğin suçlunun kimliğini gizlemek için paket başlık bilgilerinin değiştirildiği durumları suç olarak tanımlamak isteyebilirler.

⁶⁶⁶ (89) 9 sayılı Tavsiyede bundan bilgisayar sabotajı olarak söz edilmektedir. Hükümün amacı telekomünikasyon olanakları da dahil olmak üzere bilgisayar sistemlerinin yasalara uygun şekilde kullanımının bilgisayar verileri kullanılarak ya da bu veriler etkilenerek uluslararası düzeyde engellenmesi fiilinin suç olarak tanımlanmasıdır. Korunan yasal hak, bilgisayar ya da telekomünikasyon sistemlerinin işletmeci ve kullanıcılarının bu sistemleri uygun biçimde işletme haklarıdır. Metin her tür işleyiş biçiminin koruma altına alınmasını sağlamak için tarafsız bir dille kaleme alınmıştır. "Engelleme" terimi, bilgisayar sisteminin uygun işleyişine müdahale eden fiiller için kullanılmıştır. Bu engelleme, bilgisayar verilerine yeni veriler ilave etmek, bilgisayar verilerini başka yerlere iletmek, tahrip etmek, silmek, bozmak, değiştirmek veya erişilmez kılmak yoluyla yapılmış olmalıdır.

⁶⁶⁷ **DÖNMEZER**, Kişilere ve Mala Karşı Cürümler, sh: 622.

⁶⁶⁸ **ÖNDER**, Ayhan, Şahıslara ve Mala Karşı Cürümler ve Bilişim Alanında Suçlar, İstanbul, 1994, sh: 509.

⁶⁶⁹ **YAZICIOĞLU**, Bilgisayar Suçları sh: 258. Aksi görüş için bkz. **DÜLGER**, Bilişim Suçları, sh: 160.

⁶⁷⁰ **ERSOY**, Bilişim Suçları, sh: 167.

kapsamı dahilinde düşünülmemesi nedeniyle birinci fıkrada bilişim sisteminin düzenli işleminin ikinci fıkra da ise verilerin güvenliğinin korunduğunu savunmaktadır. Bu haliyle yaklaşımının karma bir nitelik taşıdığı söylenebilir. *Dülger de*, bilişim sisteminin veri ve yazılımlardan oluşan soyut unsurları yanında donanım unsurunun da koruma altına alınması karşısında, suçun hukuki konusunun karma bir nitelik gösterdiğini belirtmiştir. Yazara göre; suçun hukuki konusunun bilişim sistemi ve bilişim sisteminin içerdiği veriler üzerinde tasarruf yetkisi bulunan kişinin, verilerle oluşturulan yazılım, ekonomik bilgiler, bilimsel çalışma, bilgi vb. değerlere herhangi bir engel, arıza ya da gecikme olmadan ulaşması ve kullanılmasındaki çıkardır⁶⁷¹. *Karagülmez de*, korunması amaçlanan hukuksal değerın mülkiyet hakkı olduğunun kabul etmektedir. Yazara göre, madde gerekçesi dikkate alındığında sisteme ve veriye yöneltilen ızzar fiilleri ile bağlantılıdır ve bu kapsamda hem bilişim sisteminin hem de sistem içerisinde yer alan veriler ve diğer unsurların zarar görmemesinin amaçlanmaktadır⁶⁷². Gerçekten de yazarın ifade ettiği üzere madde gerekçesinde şöyle md. 244. mala zarar verme suçunun özel bir hali olarak düşünülmüştür. Söz konusu ifade aynen şöyledir;

“...sistemlere yöneltilen ızzar fiilleri özel bir suç hâline getirilmiştir. Aracın fizik varlığı ve işleminin sağlayan bütün diğer unsurları, söz konusu suçun konusunu oluşturmaktadır. Fıkroda seçimlik hareketli bir suç meydana getirilmiştir.”

Kurt da, md. 244 kapsamında düzenlenen suçla mülkiyet hakkının korumasının amaçlandığını ve bu kapsamda sistem ve sistem içerisinde yer alan verinin dokunulmazlığının öncelikli hukuksal değer olduğunu savunmaktadır⁶⁷³. *Ketizmen* ise, sisteme ve veriye müdahalenin mala zarar verme suçunun özel şekli olduğu kabulü aynı zamanda Türk Ceza Hukukunda da sisteme ve veriye müdahalenin hukuksal değeri ile mala zarar vermenin hukuksal değerinin birbirine paralel olduğunu düşünmektedir. Yazara göre, 244. maddenin 1. ve 2. fıkralarında düzenlenen sistem ve veriye müdahale suçunun, klasik mala zarar verme suçunun bilişim sistemleri içerisinde sistemin yazılım yönünü oluşturan veri ve programlara yönelik müdahaleleri kapsayıp kapsamadığına ilişkin tartışmalara bir açıklık getirilmesi

⁶⁷¹ **DÜLGER**, Bilişim Suçları , sh: 160.

⁶⁷² **KARAGÜLMEZ**, Bilişim Suçları, sh: 187.

⁶⁷³ **KURT**, Bilişim Suçları sh: 161 v.d.

amacıyla düzenlenen bir suç olduğunu kabul ile bu suçun hukuki konusunun mala zarar verme suçunun hukuki konusuyla örtüşmektedir⁶⁷⁴.

Suçun *maddi unsurunu* internet açısından değerlendirirken birinci ve ikinci fıkrası ayrı ayrı almakta yarar görmekteyiz. Çünkü birinci fıkra bilişim sisteminin işleyişinin engellenmesi ve bozulmasını kapsamaktayken ikinci fıkra bilişim sistemindeki verilere karşı gerçekleştirilen müdahaleyi içermektedir. Kapsamları itibariyle iki ayrı konuyu ele alan bu fıkraları kendi bütünlükleri içerisinde değerlendirmek daha sağlıklı olacaktır.

Maddenin birinci fıkrasında kanun koyucu maddi unsur olarak bir bilişim sisteminin işleyişini engellemek veya bozmak fiillerini belirlemiştir. Burada öncelikle bilişim sisteminin işleyişinin engellenmesi ve bozulması kavramları üzerinde durulmalı ardından konunun internet ile olan ilişkisi ortaya konulmalıdır. Daha önce de vurgulandığı üzere kanun koyucu md. 243'ün gerekçesinde bilişim sistemini “*verileri toplayıp yerleştirdikten sonra bunları otomatik işlemlere tâbi tutma olanağını veren manyetik sistem*” olarak tanımlamıştır⁶⁷⁵. Buradan da anlaşıldığı gibi bir bilişim sisteminin işleyişinin temel ekseni; o bilişim sistemine, kanun gerekçesinde kullanılan ifade ile, yerleştirilen verilerin otomatik işleme tabi tutulması etrafında şekillenmektedir⁶⁷⁶. O halde bir bilişim sisteminin işleyişini kendisine gönderilen komutlara ve o komutlara uygun olarak veri işleme faaliyeti olarak kabul etmek gerekir. Bu faaliyetin, dışarıdan gerçekleştirilen bir müdahale ile amaçlanan işleyiş disiplininin kısmen ve/veya geçici olarak saptırılması durumu “*engellenme*”, tamamen ve/veya kalıcı olarak durdurulması durumu da “*bozma*” olarak kabul edilmelidir⁶⁷⁷.

Dülger, sistemin işleyişinin engellenmesinin sistemin çeşitli yönleriyle sürekli ya da geçici olarak iş görmesinin engellenmesi anlamına geldiği, bu bağlamda sisteme her türlü müdahalenin bu kapsamda değerlendirilmesi gerektiğini dile getirmiştir⁶⁷⁸. *Kurt* ise bilişim

⁶⁷⁴ **KETİZMEN**, Bilişim Suçları, sh: 157.

⁶⁷⁵ Eleştiriler için bkz. **KETİZMEN**, Bilişim Suçları, sh: 13 v.d.

⁶⁷⁶ Verilerin otomatik işleme tabi tutulmasının anlamı konusunda birinci bölümde internetin bir suçluluk alanı olarak normatif ceza hukuku düzenine alınması sürecine ilişkin yapılan açıklamalar göz önünde bulundurulabilir.

⁶⁷⁷ Türk Dil Kurumu Sözlüğünde engellemek, “*bir şeyin gerçekleşmesini veya yapılmasını önlemek*”; bozmak ise, “*bir şeyi kendisinden beklenen işi yapamayacak duruma getirmek*” olarak tanımlanmaktadır. Kaynak: <http://tdkterim.gov.tr/bts/?kategori=veritbn&kelimesec=112947> (Erişim Tarihi: 10.04.2009, Saat: 10:10)

⁶⁷⁸ **DÜLGER**, Bilişim Suçları, sh: 234. *Dülger'in* bu görüşüne kısmen katılmamaktayız. Çünkü bir bilişim sistemi üzerinde gerçekleştirilecek müdahale sürekli bir iş göremezlik içeriyorsa bu engellenme değil bozma olarak kabul edilmelidir. *Dülger'le* aynı yaklaşım için **KARAGÜLMEZ**, Bilişim Suçları, sh: 188.

sisteminin engellenmesi halinde sistemin bozulmasının söz konusu olmayıp normalde yerine getirdiği fonksiyonları ifa etmesinin engellendiğini kabul etmektedir⁶⁷⁹. Bir bilişim sisteminin bozulması ise sistemin tamamen çalışamaz hale gelmesi, sistemin olağan koşullarda yapması gereken işlevlerin değişikliğe uğratılması, haksız müdahale ile sistemin sağlıklı işleyişinin geçici veya sürekli şekilde ortadan kaldırılması⁶⁸⁰ olarak belirlenmektedir.

Bu açıklamalar ışığında kanun metninde seçimlik hareket olarak belirlenen “engelleneme” ve “bozma” fiillerinin internet aracılığıyla işlenebilirliğini şu şekilde değerlendirmek mümkündür: öncelikle bu fıkra kapsamında düzenlenen “bir bilişim sisteminin işleyişini engellemek veya bozmak” fiilleriyle bir bütün olarak bilişim sistemi esas alınmaktadır. Dolayısıyla sistem işleyişini devam ettirirken, sistem içindeki bir unsurun tüm sistemin işleyişini etkilemeyecek bir müdahaleye maruz kalmasıyla engellenmesi veya bozulması bu fıkra kapsamında değerlendirilmemelidir. Bilişim sistemi bir bütündür ve işleyişi de bir bütünlük arz etmektedir. Bu anlamda bilişim sistemi sadece herhangi bir unsuruna indirgenemez. Bu unsurda meydana gelen engelleme veya bozma tüm sistemin işleyişini etkileyecek düzeyde olmalıdır. Bu açıklama karşısında web sitesinin hacklenmesi suretiyle erişiminin engellenmesi veya internet ortamındaki bir verinin yok edilmesi, bir bilişim sistemi olarak internetin işleyişinin engellenmesi veya bozulması anlamına gelmemektedir. Çünkü ağların ağı olarak kabul edilen internet sadece sanal ortamdaki verilerle sınırlı değildir⁶⁸¹. Aynı zamanda teknik bir alt yapıya da sahiptir. Dolayısıyla ancak internetin veri ve teknik altyapı unsurlarının bir bütün halinde çalışmasını engelleyecek nitelikte eylemler bu kapsam dahilinde düşünülebilir. Yukarıda verilen örnekler aşağıdaki ele alınacak olan ikinci fıkra hükmü kapsamında değerlendirilmelidir.

Suçun seçimlik hareketlerinin doğrudan internet ortamında değil de internet aracılığıyla diğer bilişim sistemi unsurlarında gerçekleşmesi hususu bakımında da şunu söylemek mümkündür ki, her iki seçimlik hareket de internet aracılığıyla gerçekleştirilebilir. Daha önce incelenen suç tiplerinde ayrıntılarıyla ortaya konulduğu üzere internet aracılığıyla diğer kullanıcılara gönderilen ve onların bilişim sistemlerinde zarara neden olan birçok casus ve kötücül yazılımlar ile bunlara bağlı olarak gerçekleşen saldırılar mevcuttur. Özellikle bilgisayarlar açısından düşünüldüğünde bu saldırılar bilgisayarın gerek yazılım gerekse

⁶⁷⁹ KURT, Bilişim Suçları, sh: 164.

⁶⁸⁰ KARAGÜLMEZ, Bilişim Suçları s. 188. Yazar sistemin işleyişinin kısmen ya da tamamen bozulmasının kısmen veya tamamen sistemin işleyişine engel olma anlamına geldiğini bu nedenle fıkra bozma hareketine yer verilmeyebileceğini ifade etmiştir.

⁶⁸¹ İnternetin bir bilişim sistemi olarak kabulü ile ilgili olarak bkz. 3.2.6. Bilişim Sistemine girme, sh: 296 v.d.

donanım unsuruna zarar vermekte, sistemin işleyişini engellemekte ve hatta bozmaktadır. İşte bu noktada md. 244/1'in sadece yazılım unsurunu mu ya da sadece donanım unsurunu mu yoksa her ikisini de mi birden kapsadığı yönüne tartışmalara rastlanmaktadır. Bu tartışmanın önemi büyüktür. Çünkü getirilecek yanıtı göre 5237 sayılı TCK md. 151'de düzenlenen mala zarar verme suçu bu bağlamda bir anlam kazanacaktır. Çünkü teknik anlamda veri “mal” olarak kabul edilmemesine rağmen donanım unsurları “mal” kategorisinin içinde kaldığından, inceleme konusu fıkranın kapsam tespitine göre donanıma verilecek zararın şekli ve niteliği itibariyle md. 151 anlamında mala zara verme suçu kapsamında değerlendirilme imkanı vardır.

244. maddenin birinci fıkrasının kapsamı konusunda temel olarak iki görüşün varlığından bahsetmek mümkündür. Söz konusu fıkra ile ilgili baskın görüş, yazılım donanım ayırımı yapmaksızın sistemin işleyişini engelleyen veya bozan her türlü müdahalenin de bu fıkra kapsamında değerlendirilmesi gerektiği yönündedir⁶⁸². Bunun yanında 244. maddenin 1. fıkrasının sadece donanıma yönelik müdahaleleri kapsadığı görüşü de ileri sürülmüştür⁶⁸³.

Kanaatimizce md. 244/1 düzenlenişi itibariyle hem yazılım hem de donanım unsurunu kapsamaktadır. Şöyle ki; bilindiği üzere yazılım, donanım birimlerini istenen işleme yönlendirilen bir çalışma içerisinde kullanımını sağlayan bir dizi komut, prosedür gibi sanal tanımlardır⁶⁸⁴. Başka bir anlatımla bilgisayar ile kullanıcı arasındaki iletişimi sağlayan öğedir. Bilgisayarın çalışmasını, işlem yapmasını sağlayan bütün programlar yazılım grubunu oluşturur. Yazılımlar genel olarak Sistem Yazılımları (İşletim Sistemi, Bellek ve Disk hizmet yazılımları, Derleyiciler, Veri Tabanı, Yönetim Yazılımları, İletişim ve Haberleşme Yazılımları, Ağ Yönetim Yazılımları), Uygulama Yazılımları (Ticari Paket Yazılımları, Ofis Otomasyonu Yazılımları, Diğer Özel ve Genel Tüm Yazılımlar (Çizim, Tasarım, Dizgi vb.)) gibi gruplandırılmaktadırlar⁶⁸⁵. Dikkat edilirse yazılım unsuru bir bilgisayarın işlem

⁶⁸² **KURT**, Bilişim Suçları, sh: 164 v.d.; **KARAGÜLMEZ**, Bilişim Suçları, sh: 188.

⁶⁸³ **YAZICIOĞLU**, Yeni Türk Ceza Kanunundaki Bilişim Suçları, sh:408- 409. Yazar Türk Ceza Kanununun 2001 Tasarısının sisteme ve veriye müdahaleyi düzenleyen 347. maddesinin gerekçesinde yer alan “ fiiller, aracın fizik varlığını ve işlemlerini sağlayan bütün diğer unsurları kapsamaktadır” ifadesinden hareketle sistemin fiziki varlığını oluşturan donanımının 244. maddenin 1. fıkrası ile koruma altına alındığını belirtmektedir.

⁶⁸⁴ **ÖZCEYLAN**, Teber, Bilgisayara Giriş, sh: 5, Kaynak:[http://web.inonu.edu.tr/~tozceyhan/pdfs/BG\(Belge\).pdf](http://web.inonu.edu.tr/~tozceyhan/pdfs/BG(Belge).pdf) (Erişim Tarihi: 10.04.2009, Saat: 09:57).

yapmasını sağlayan programlardan oluşmaktadır. 243. maddenin gerekçesi de bakılacak olursa bu bölümde, 244. madde de dahil olmak üzere, “*veri*” kavramının kullanıldığı her yerde bilişim sistemi içindeki tüm soyut kavramlar anlaşılmaktadır. Bu anlamda programlar da kanunun çizdiği kapsam itibarıyla “*veri*” kabul edilmektedir. O halde sadece bir tür program olan yazılıma yönelik gerçekleştirilen engelleme ve/veya bozma eylemleri doğal olarak ceza hukuku tekniği anlamında “*verinin engellenmesi veya bozulması*” kabul edilecektir ki, birazdan incelenecek olan aynı maddenin ikinci fıkrasında sayılan tüm seçimlik hareketler (*verilerin bozulması, yok edilmesi, değiştirilmesi, erişilmez kılınması, var olan verinin başka bir yere gönderilmesi*) doğrudan verinin engellenmesi veya bozulması olarak kabul edilecek eylemlerdir.

Ancak yukarıda birçok kez ifade edildiği üzere bilişim sistemi yazılımı ve donanımıyla bir bütündür. Yazılım olmadan donanım, donanım olmadan da yazılım tek başına bir anlam ifade etmez. Tersinden hareket edilecek olursa yazılıma verilecek bir zarar hiç şüphe yok ki donanımın da işlevselliğine olumsuz yönde etkide bulunacaktır. Kanun koyucunun yaptığı bu ayırım karşısında veriye verilen bir zarar bilişim sisteminin maddi unsurunu da işlevsiz bıraktığı takdirde nasıl bir yol izlenecektir? Bir örnekle açıklamak gerekirse; yüksek kapasiteli ve yüksek hızlı, bilgisayara monte edilmiş, teknik müdahale haricinde çıkarılamayan, manyetik usullere göre bilgi okuyup yazan hard disk bir donanım unsurudur. Ancak hard disk tek başına maddi varlığı ile bu işlemleri gerçekleştiremez. Bu işlevleri gerçekleştirebilmesi için hard diske BIOS adı verilen yazılımın (programın) yüklü olması gerekmektedir. Bu anlamda bir bilgi işlem faaliyeti için yazılım – donanım uyumluluğunun zorunluluğu görülmektedir.

Gelinen nokta itibarıyla yanıtlanması gereken iki soru kendini göstermektedir. Birincisi, internet aracılığıyla gönderilen bir kötücül yazılım, bir donanım unsuru olan hard disk üzerindeki bir yazılım olan BIOS’u silerek, bozarak veya bunların dışında bir müdahale ile etkisiz hale getirerek hard diski ve haliyle bilgisayarı çalışmaz hale getirirse ya da yine internet üzerinden gönderilen bir kötücül yazılım hard diskte kayıtlı olan güç kaynağı dengelerine ilişkin verilerde değişikliğe neden olarak bilgisayara yüksek güçte bir enerji girişini sağlayıp bilgisayarın tüm donanım unsurlarını yakarsa, burada sadece yazılım unsuruna mı yoksa donanım unsuruna mı zarar vermek suretiyle bilişim sisteminin işleyişi

⁶⁸⁵ ÖZCEYLAN, Bilgisayara Giriş, sh: 5. Ayrıca yazılım teknolojisinin Türkiye’deki durumu ve yakın gelecekteki öngörülerini için bkz. YILDIRIM, Nihan/ ANSAL, Hacer, Türkiye’de Yazılım Teknolojisi için Teknoloji Öngörüsü, in: İTÜSBED, C:3, S: 1, sh: 27 v.d.

engellenmiş kabul edilecektir? İkincisi de, acaba burada donanım - yazılım ayrıt etmeden bir bilişim sisteminin işleyişi engellenmiş veya bozulmuş olduğu için sadece md.244/1 mi, yoksa yazılım “veri” hükmünde olduğu için veriye müdahale nedeniyle bilişim sisteminin işleyişinin engellendiği veya bozulduğu gerekçesiyle hem md. 244/1 hem de md.. 244/2 mi uygulanacaktır?

Birinci soruya verilecek cevapta, örnek bakımından donanım unsuru olan hard diskin devre dışı kalması, doğrudan hard diske yapılan bir müdahale ile değil hard disk işlevsel kılan yazılım olan BIOS programına yapılan müdahale ile gerçekleşmiştir⁶⁸⁶. Ancak bu sonuç, bir bilişim sistemin işleyişinin ancak yazılıma yapılacak müdahaleler ile engelleneceği veya bozulacağı anlamına gelmez. Çünkü hiçbir yazılım unsuruna müdahale etmeden de donanım unsurunun engellenmesi veya bozulması mümkündür. Örnek vermek gerekirse hard disk bünyesindeki bir boşluğa yerleşip kendini sürekli kopyalayarak çoğalan bir virüs hiçbir yazılıma zarar vermeden bilgisayar kapasitesini doldurarak bilgi işleme faaliyetini engelleyebilmektedir⁶⁸⁷. Aynı şekilde bir başka virüs de bilgisayarın internete bağlantısının gerçekleştiği ethernet girişini devre dışı bırakabilir. Bu örneklerde de görüldüğü gibi bilişim sisteminin işleyişi sadece donanım unsuruna zarar vermek suretiyle de engellenebilir veya bozulabilir.

Bu açıklamalar ikinci sorunun cevabıyla ilişkilendirilecek olursa; kanun koyucunun yaptığı tercih sonucu bir yazılım unsuruna müdahale nedeniyle bilişim sisteminin işleyişi engellenir veya bozulursa burada bilişim sisteminde yazılım – donanım uyumluluğunun zorunluluğu çerçevesinde artık md. 244/2 dikkate alınmaksızın sadece md.244/1 uygulanacaktır. Ancak bu engelleme veya bozma fiilleri doğrudan ve sadece veriye karşı gerçekleştirilmekle birlikte bir bütün olarak bilişim sisteminin işleyişini etkilemezse burada sadece md. 244/2’ nin uygulanması gerektiği kanaatindeyiz.

Gelinen bu nokta itibariyle incelemeye konu fıkranın internet aracılığıyla işlenebilirliği özelinde md.244/1 ile md. 151’de düzenlenen mala zarar verme karşılaştırılacak olursa, md. 244’ün gerekçesinde de vurgulandığı gibi bir bilişim sisteminin işleyişini engeller veya bozar nitelikte “*ızrar*” fiilleri suç haline getirmiştir. Daha önce de ifade edildiği gibi klasik mal zarar verme suçu kapsamında düşünülen bu suç 5237 sayılı TCK ile özel bir düzenleme olarak anlam kazanmıştır. Bu haliyle artık md. 244/1’in olduğu bir ortamda md.

⁶⁸⁶ Detaylı açıklamalar için bkz. YAVAŞ, Mustafa/ YILMAZ, Selami/ ALABAY, Nurettin, Bilgisayar Teknolojileri Kullanımı, Ankara, 2001, sh: 34.

⁶⁸⁷ Ayrıntılı Bilgi için bkz. CANBEK/ SAĞIROĞLU, Casus ve Kötücül Yazılımlar, sh: 122-123.

151 çerçevesinde mala zarar verme suçunu kabul etmek isabetli olmayacaktır. **Burada bilgisayarın veri işleme etkinliği üzerinde olması gerektiği husus üzerinde durulması gerekmektedir.**

244. maddenin 2. fıkrasında, “*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.*” hükmüne yer verilmiştir. İnceleme konusu fıkra düzenlenen seçimlik hareketler tek tek incelenecek olursa; ilk seçimlik hareket bilişim sistemi içerisindeki “*verinin yok edilmesi*”dir. *Dülger’e* göre verinin yok edilmesinin bilişim sistemi açısından sözlük anlamından farklı bir kapsama sahiptir. Yazara göre verinin yok olması demek, söz konusu veriye erişimin engellenmesi anlamına gelmektedir⁶⁸⁸. *Kurt* ise verinin yok edilmesinin veriye bir daha ulaşılamaması anlamına geldiğini belirterek daha dar bir anlam yüklemektedir⁶⁸⁹. 765 sayılı TCK md. 525/ 1-b’de verilerin yok edilmesi fiiline karşılık gelen silmek fiilinin aynı anlam içeriğine sahip olup olmadığı hususu da tartışılmaktadır. *Kurt* bu hususta da, verinin yok edilmesinin veriye bir daha ulaşılamaması anlamına geldiğini ifade ederek, verinin silinmesinin yukarıda aktarıldığı şekliyle verinin yok edilmesi anlamına gelmediğini, 244. maddenin 1. fıkrasında düzenlenen verinin erişilmez kılınması şeklindeki diğer bir hareketi oluşturduğunu ifade etmektedir⁶⁹⁰. *Ketizmen* de, verinin yok edilmesinin, verinin varlığına son verilmesi, ortadan kaldırılması ve verinin tamamen ya da büyük güçlüklerle elde edebilecek şekilde tasarrufundan çıkartılması olarak tanımlandığında, verinin silinmesi de verinin yok edilmesi olarak değerlendirilebileceğini kabul etmiştir⁶⁹¹. Bu bağlamda verinin teknik olarak tekrar edilebilmesi olanağı ya da olasılığının varlığından dolayı verinin silinmesinin verinin yok edilmesi kapsamı dışında tutulabilmesine ilişkin gerekçeyi kabul etmemektedir⁶⁹².

⁶⁸⁸ **DÜLGER**, Bilişim Suçları, sh: 235.

⁶⁸⁹ **KURT**, Bilişim Suçları, sh: 168.

⁶⁹⁰ **KURT**, Bilişim Suçları, sh: 168.

⁶⁹¹ **KETİZMEN**, Bilişim Suçları, sh: 172.

⁶⁹² Fakat hâlihazırdaki işletim sistemlerinde yer alan ve verinin yanlışlıkla ortadan kaldırılmasının engellenmesine ve veriye tekrar ulaşılabilmesine olanak sağlamak üzere, ara bir aşama olarak tanımlanabilecek geri dönüşüm kutusuna gönderilmesi ya da geçici klasörlere gönderilmesi hallerinde ya da verinin sistem içerisinde başka bir yere gönderilmesi ve bu şekilde saklanması hallerinde verinin yok edildiğinden söz edileceği tartışmalıdır. *Dülger* bu gibi hallerde de verinin yok edildiğinden bahsedilebileceğini belirtmekte burada veriye ulaşılamamasının bir şekilde engellendiğinden bahsetmektedir. **DÜLGER**, Bilişim Suçları, sh: 236.

Maddede yer alan diğ er bir seçimlik hareket biliş im sisteminin içindeki “*verinin bozulması*”dır. Verinin bozulması verinin içeriğine ya da yapısına müdahale suretiyle verinin kısmen ya da tamamen kullanılmayacak hale gelmesi olarak tanımlanabilir. Burada özellikle verinin içeriğine müdahalenin var olan verinin içerdiği bilgi ya da enformasyona olumsuz müdahaleyi kapsadığını belirtmek gerekir. Verinin yok edilmesinden farklı olarak burada verinin tasarruf alanından çıkartılmaması ya da ortadan kaldırılmaması söz konusudur. Bu açıklama doğrultusunda madde metninde yer alan verinin değiştirilmesi ise var olan verinin kullanılmasını engellemeyen fakat verinin içeriğinin ya da kendisinin orijinalliğini ortadan kaldıran her türlü değişiklik olarak tanımlanabilir⁶⁹³. Bu açıdan kötü amaçlı kodların veriye yerleştirilmesi bu kapsamda değerlendirilebilmektedir.

“*Verinin erişilmez kılınması*” ise, genel olarak verinin içerdiği bilgi ya da enformasyona müdahale edilmeden veriye olağan şekilde erişimin engellenmesi olup burada veri içerik bakımından bütünlüğünü korumaktadır. Veri ne yok edilmekte ne de bozulmakta, fakat verilere ulaşım için gereken işlem bağı koparılmaktadır. Sisteme DOS saldırıları ile bunun gerçekleştirilmesi de mümkün olmakla birlikte, 244. maddenin düzenlenişi bakımından, DOS saldırılarının sistemin işleyişine yönelik bir saldırı niteliğinde olması nedeniyle, sistemin işleyişinin engellenmesi ve kimi durumlarda da işleyişinin bozulması söz konusu olacağından burada sisteme yönelik saldırılar sonucunda veriye erişilememesi halinin 1. fıkra kapsamında olduğunu söylemek mümkündür. Veriye erişilmesi bakımından erişimin engellenmesinin geçici ya da daimi olması arasında bir fark yoktur.

İnceleme konusu fıkrada özellikle internet açısından en problemlili seçimlik hareket “*sistem içerisindeki verinin başka bir yere gönderilmesi*”dir. Her şeyden önce kanun koyucu bu seçimlik hareketi çok muğlak olarak düzenlemiş ve gerçek amacını ortaya koyamamıştır. Çünkü bir biliş im sisteminde gerçekleşecek her türlü işlem için mutlak suretle bir veri iletimi gerçekleşmek zorundadır. Bunun en basit bir komut olması veya kompleks bir işlem olması arasında bir fark yoktur. Veri iletiminden maksat da kanun koyucunun md. 244/2’de kabul ettiği anlamda sistem içerisindeki verinin başka bir yere gönderilmesi olarak düşünülebilir. Bir örnek vermek gerekirse, aynı veya farklı kullanıcı veya üreticinin iki yada daha fazla bilgisayarı arasında veri aktarılabilmesi ve ortak süreçlerin yürütülebilmesi karşılıklı çalışabilmenin sağlanabilmesi birlikte çalışabilme olarak adlandırılır. Karşılıklı çalışabilmenin sağlanabilmesi için alıcının, vericinin gönderdiği bilgiyi anlayabilmesi gerekir. Karşılıklı çalışma verici ile alıcı arasında kullanılacak işaretler, veri formatları ve temel aktarım birimlerinin değerlendirme yöntemleri üzerinde anlaşma ile mümkün olur. Veri transferi

⁶⁹³ KETİZMEN, Biliş im Suçları, sh: 170.

zamanlamasını düzenleyen kurallar dizisi olan protokoller bu anlaşmayı sağlarlar. Bu da sağlıklı bir veri işleme faaliyetini sağlar.

Dikkat edilirse bu örnek ile anlaşıldığı üzere, bir ağ aracılığı ile bilgisayarlar arası kurulan her türlü iletişim bir veri aktarımını zorunlu kılar. Peki şu halde kanun koyucunun, fıkra metninde herhangi bir hukuka aykırılığı özel olarak belirtmeden sadece bir bilişim sistemi içindeki verinin başka bir yere gönderilmesi tercihi nasıl sınırlandırılabilir? Bu gerçekten de önemli bir problemdir. Yine anlaşılıyor ki kanun koyucu aslında bilişim suçlarını düzenlerken bir bütünlük olarak bilişim sistemini değil sadece bilgisayarı ve hatta tek başına işlem gören bir bilgisayarı esas almıştır. Bugün internet üzerinde bir web sitesine erişmek için “*browser*”e adresi girdikten sonra enter tuşuna basıldığı anda, o web sayfasının kayıtlı olduğu sunucuya (sayfayı görüntüleme talebi olarak kabul edilebilir) bir komut yani kanunun bizzat kabul ettiği kavram ile “*veri*” gönderilmektedir. Yine bir e- mail yada eş zamanlı çoklu ortam yaratılarak gerçekleştirilen sohbetler, haber veya bir konu üzerine tartışma sayfasına yüklenen görüşler, paylaşım sitelerine gönderilen videolar ve hatta daha sonra özellikle üzerinde durulacağı üzere internet üzerinden gerçekleştirilen bankacılık hizmetleri de bir veri aktarımı esasına dayanmaktadır. *Kanaatimizce* bu seçimlik hareketin düzenleniş şekli maddenin “*ratio legis*”ine hizmet etmekten uzaktır.

Bununla beraber farklı bir problemlilik nokta daha dikkati çekmektedir. *Ketizmen’e* göre, verinin başka bir yere gönderilmesi verinin aslının veya kopyasının transfer edilmesidir. Verinin kopyalanması verinin çoğaltılması anlamına gelmektedir⁶⁹⁴. Verinin çoğaltılması ise verinin kendisine, verinin kullanımı ya da erişebilirliği açısından herhangi bir etkide bulunmayacak bir harekettir. Bu durumda verinin aslının bilişim sistemi içerisinde kalması halinde sistem içerisindeki veriye yönelik herhangi olumsuz bir hareketin gerçekleşmediği anlamına gelmektedir. Bu durum ise maddenin düzenleniş amacı ile bağdaşmamaktadır⁶⁹⁵. Yine *Ketizmen’e* göre, bu kapsamda verinin başka bir yere gönderilmesinin yine verinin bütünlüğünü bozmayan fakat sistem içerisindeki veriye erişimi zorlaştıran bir hareket olarak dar yorumlanabilmesi, bu haliyle de veriye erişimin engellenmesi kapsamına girebilecek bir olasılığın maddede ayrıca düzenlendiği sonucuna varılabilmemesi mümkündür.

⁶⁹⁴ **KETİZMEN**, Bilişim Suçları, sh: 172- 173.

⁶⁹⁵ **KETİZMEN**, Bilişim Suçları, sh: 173.

Birinci ve ikinci fıkra anlamında kanun koyucunun *manevi unsur* olarak genel kastı dikkate aldığı, *suça etki eden neden* olarak da sadece üçüncü fıkrada söz konusu eylemlerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halini ağılaştırıcı neden olarak düzenlediği görülmektedir. Bu belirtilen hususlar konusunda çok fazla soruna rastlanmamaktadır. Maddenin gerek uygulama gerekse doktrin tarafından en çok tartışılan, birinci ve ikinci fıkra düzenlemeleriyle de çok yakından ilişkili bulunan dördüncü madde düzenlemesi yani bilişim sistemleri aracılığıyla yarar sağlama suçuna göz atmak yerinde olur.

Günümüzde gerek doktrinde gerekse uygulamada üzerinde en çok tartışılan hususlardan birini hiç şüphe yok ki md. 244/4'de düzenlenen bilişim sistemi aracılığıyla yarar sağlama suçu oluşturmaktadır. Özellikle bankacılık işlemlerinin internet ortamında yapılmasının yaygınlaşmaya başladığı dönemden beri, internetin boşluklarından faydalanarak uygulanan teknik yöntemlerle kişilerin çok büyük ekonomik zararlara uğratılması durumu söz konusudur. Bilindiği gibi bu yönde internet aracılığıyla gerçekleştirilen birçok yöntem vardır. Bunların bazı önemli yöntemleri kişisel veriler aleyhine işlenen suçlarda aktarılmıştı. Bunlar dışında en çok kullanılan yöntem *phishing* yöntemidir.

Phishing sözcüğü, eskiden telefon sistemlerinden ücretsiz görüşme yapmak için kullanılan bir aldatmaca sistemi olan "*phreaking*" ve balık avlama anlamına gelen "*fishing*" sözcüklerinin birleşmesinden oluşuyor. Tanım olarak *phishing*, genellikle e-posta ya da Web sitelerindeki açılır pencereler yoluyla kendini gösteren ve hem kişisel, hem finansal anlamda zararlar sonuçlanabilme potansiyeli yüksek bir nevi bilgi hırsızlığı yöntemidir. *Phishing* dolandırıcıları kullanıcıdan kişisel bilgilerini ya da finansal şifrelerini çalmak için, hizmet alınan kurumların kurumsal kimliğini taklit eden mesajlarla kendilerini göstermektedirler. Tüm bu mesajların ortak amacı, bir nedenle hesabınızla ilgili bilgilerin güncellenmesi gerektiği konusunda kullanıcıyı ikna edebilmektir⁶⁹⁶.

Genellikle söylenen yapılmadığı takdirde kullanıcının dezavantajlı konuma getirecek bir durumun varlığı da mesaja eklenerek bir an önce harekete geçmeyi teşvik etmektedirler. Örneğin sürekli işlem yapılan bankadan geliyor süsü verilmiş bir mesajla kullanıcının online bankacılık hesabına ait şifre bilgilerini değiştirilmesi gerektiğini söylerken, bunun bir hafta içinde yapmadığı takdirde tüm hesapların güvenlik nedeniyle bloke edileceğine benzer bir

⁶⁹⁶ ERALP, Özgür, İnternet Bankacılığı, in : Bilişim ve Hukuk, Y:2, S: 7, Ankara, 2008, sh: 10. v.d.

bilgi vererek kullanıcıyı bir an önce işlem yapmaya zorlamaktadır. Bu aldatmacaya inanıp mesajda yer alan sahte bağlantıya tıklanırsa, bu kez her zaman kullanılan güvenilir kurumsal sitenin taklit edilmiş bir kopyasına erişilmiş olur. Ancak yönlendirilen sahte sitedeki ilgili boşluklara kişisel bilgiler girildiği anda tüm bilgiler karşı tarafın eline geçmiş oluyor. Bundan sonra o kullanıcının bankacılık şifreleri kullanılarak banka ve kredi kartı hesaplarının boşaltılması ya da bankadan edinilecek detaylı kişisel bilgiler yardımıyla işlenen bazı suçların aldatılan kullanıcı üzerine yıkılması⁶⁹⁷.

Bunun dışında yine sistem üzerinde girilen şifreleri yakalayıp kaydeden casus yazılımlardan şifre yakalayıcıları veya soyguncuları olarak bilinen “*Password Capture and Password Hijacker*” de bu yönde verilebilecek örneklerden biridir⁶⁹⁸. Son olarak da doktrinde de sık olarak vurgulanan bir tekniğe yer vermekte fayda vardır. Programlara müdahale yoluyla dolandırıcılık suçuna “*salam tekniği*” adı verilen yöntemi örnek göstermek mümkündür. Bu yöntemde hedef banka hesap ya da hesaplarından çok küçük miktarda paranın failin belirlediği hesaba aktarılması söz konusudur. Bu yöntemin başarısı yeterli miktarda hesaba ulaşılabilmesine ve hedef hesaplardan transfer edilen küçük miktardaki meblağların transfer edildiğinin hesap sahibi ya da diğer ilgili kişiler tarafından fark edilmemesine bağlıdır. Bilgisayar sistemi içerisindeki programlara müdahale edilmesi suretiyle ya da yeni bir program eklenmesi suretiyle bu yöntemin gerçekleştirilmesi mümkündür⁶⁹⁹.

Daha önce üzerinde detaylı bir şekilde durulan internetin sınır ötesi etkisinin en ciddi bir biçime hissedildiği bu alanla ilgili olarak sadece ulusal değil uluslar arası reflekslere de rastlamak mümkündür. Bunlardan en önemlisi Avrupa Konseyi Siber Suç Sözleşmesidir. Siber Suç Sözleşmesinde yer verilen bilgisayar aracılığıyla dolandırıcılık suçu ile ilgili olarak Sözleşmenin açıklayıcı raporunda, teknolojik gelişim sonucu olarak kredi kartı dolandırıcılığı da dâhil olmak üzere dolandırıcılık fiilleri gibi ekonomik suçların işlenme olanaklarının hızla çoğaldığı ve bilgisayar sistemlerinde temsil edilen ya da yönetilen ekonomik değerlerin, geleneksel olarak cezai müeyyideler ile korunan malvarlığına yönelik ihlallere benzer şekilde

⁶⁹⁷ *Phishing* tekniğine ilişkin uygulama örnekleri için bkz. **ERALP**, İnternet Bankacılığı, sh: 14- 15.

⁶⁹⁸ **CANBEK/ SAĞIROĞLU**, Casus ve Kötücül Yazılımlar, sh: 127.

⁶⁹⁹ **DÜLGER**, Bilişim Suçları, sh: 71.

manipülasyonların hedefi olduğu şeklinde ifade edilmiştir⁷⁰⁰. Bunun sonucu olarak, bilgisayar aracılığıyla para ya da diğer ekonomik değerlerin elde edilmesine yönelik bu tür fiillerin etkin olarak cezalandırılabilmesi amacıyla, söz konusu fiillere özgü düzenleme yapılması yoluna gidilmiştir.

Türk Ceza Hukuku anlamında da gerek 765 sayılı gerekse 5237 sayılı TCK uygulamasında sürekli tartışılan bir husus olmuştur. 765 sayılı TCK'nin 525/b 2. fıkrasında yer alan, "*Bilgileri otomatik işleme tabi tutmuş bir sistemi kullanarak kendisi veya başkası lehine hukuka aykırı yarar sağlayan kimseye...*" hükmü ile bilişim aracılığıyla yarar sağlama fiilinin düzenlendiği ifade edilmiştir. Dikkat edilecek olursa bu düzenleme itibarıyla herhangi bir sınırlamayla karşılaşılmemekte ve çok geniş bir düzenleme kapsamını içermektedir. Nitekim *Ersoy*, yarar sağlamak kavramını ekonomik yararlar dışındaki yararları da kapsayacak şekilde ele almış, yarar sağlamanın bu şekilde geniş bir anlama sahip olması ile birlikte özellikle hırsızlık, dolandırıcılık, güveni kötüye kullanma gibi "maddi çıkar"a yönelik fiillerinin bilişim sistemlerinin kullanılması suretiyle işlenmesi halinde nasıl bir çözüme ulaşılabileceği konusunda bir çelişkinin yaşanacağını ortaya koymuştur⁷⁰¹.

Ünver de suçun kapsamına ilişkin soruna işaret etmiş ve söz konusu maddenin hırsızlık, dolandırıcılık, güveni kötüye kullanma gibi birçok suçu kapsayan bir düzenleme olduğunu, bu şekliyle her türlü haksız eylemi cezalandıran genel bir hüküm olduğundan belirginlik ve kanunilik ilkesine aykırılık itirazların ileri sürülebileceğini ifade etmiştir⁷⁰².

⁷⁰⁰ Teknoloji devrimiyle birlikte kredi kartı sahtekarlıkları da dahil olmak üzere sahtekarlık gibi ekonomik suçları işleme fırsatları arttı. Bilgisayar sistemlerinde temsil edilen ya da yönetilen varlıklar (elektronik fonlar, banka parası) geleneksel mülkiyet biçimleri gibi manipülasyon hedefi haline geldiler. Bu suçların başlıcaları bilgisayara yanlış verilerin girildiği veri ekleme manipülasyonları, program manipülasyonları ve veri işleme sürecine yapılan diğer müdahalelerdir. Bu Maddenin amacı mülkiyeti yasadışı biçimde nakletmek amacıyla veri işleme sürecine yapılan kanunsuz manipülasyonları suç olarak tanımlamaktır. Bütün olası ilgili manipülasyonları kapsam dahiline almak için Madde 8 (a)'daki "yeni veriler ekleme", "değiştirme", "silme" veya "erişilmez kılma" şeklindeki teşkil edici unsurlara Madde 8(b)'deki "bir bilgisayar programı ya da sisteminin işleyişine müdahale" şeklindeki genel fiil eklenmiştir. "Veri ekleme, değiştirme, silme ve veya erişilmez kılma" unsurları, bir önceki Maddedekiyle aynı anlamdadır. Madde 8(b), donanım manipülasyonları gibi fiilleri, yazıcı çıktıların erişilmez kılmaya yönelik fiilleri ve verilerin kaydedilmesini ya da akışını ya da programların çalışma sırasını etkilemeye yönelik fiilleri kapsamaktadır. Bilgisayar sahtekarlığı manipülasyonları, başka bir kişinin mülkiyetinin doğrudan ekonomik ya da zilyetlik kaybına yol açıyorsa ve fail kendisi ya da bir başkasına kanunsuz ekonomik kazanç sağlamayı amaçladıysa suç olarak tanımlanır. Geniş bir kavram olan "mülkiyetin kaybı" terimi, paranın, ekonomik değeri olan maddi ve gayri maddi varlıkların kaybını kapsar.

⁷⁰¹ **ERSOY**, Bilişim Suçları, sh: 178-179.

⁷⁰² **ÜNVER**, TCK ve Ceza Kanunu Tasarısının Değerlendirilmesi, sh: 99; **DÜLGER**, Bilişim Suçları, sh: 166.

Doktrindeki bu endişeler o dönem Yargıtay uygulamalarında da kendini göstermiş ve kimi durumlarda dar yorumlanmış kimi durumlarda ise geniş yorumlanmıştır. Bu yorum farklılıklarına örnekler vermek gerekirse, bir kararda Ziraat Bankası şubesinde tasarruf servisinde memur olarak çalışan sanığın *"İkinci derecede imzaya yetkili olması, bilgisayar şifresi bulunması, doğrudan vazülyet olmamakla beraber Bankanın paraları üzerinde muhafaza ve denetim sorumluluğu bulunması; buna dayanarak bir kısım mudilerin hesaplarına suretiyle para aktarılıp banka parasını mal edilmesi şeklinde oluşan"* fiili nitelikli zimmet suçunu oluşturacağına karar verilmiştir⁷⁰³. Yine başka bir kararında; kendi bilgisayar şifresi ile her türlü işlem yapabilen bu nedenle bankanın paralarının korunmasından sorumlu olan sanığın, bazı hesaplara müdür şifresini kullanarak faiz tahakkuku ile başka hesaplara aktarıp hesap sahiplerine vezneden çektirerek mal edinmesi eylemi *"nitelikli dolandırıcılık"*; diğer mudilerin hesaplarına faiz tahakkuku yapmadan sadece tahsil ve ödeme fişleri düzenleyerek faizleri başka mudilerin hesaplarına aktarıp onların aracılığıyla vezneden alarak mal edinmesinin *"zincirleme basit zimmet"* suçunu oluşturduğu kabul edilmiştir⁷⁰⁴. Bir

⁷⁰³ Ziraat Bankası Yıldızevler Şubesinde çalıştığı sırada müteselsil şekilde sahte evrak düzenlemekten, bilişim alanında menfaat temin etmekten ve dolandırıcılık suçundan sanık Ali Yozgatın yapılan yargılaması sonunda; TCK.nun 342/1, 504/7, 80, 522, 71. maddeleri gereğince 4 yıl 12 ay 20 gün ağır hapis, 405.747.221 lira ağır para cezasıyla mahkumiyetine, 149.050.000 lira zararın müdahale ödenmesine bilişim alanında menfaat temin etmek suçundan beraetine dair (ANKARA) 1. Ağır Ceza Mahkemesinden verilen 21.3.1996 gün ve 1995/197 Esas, 1996/71 Karar sayılı hükmün süresi içinde Yargıtayca incelenmesi müdahil ve sanık tarafından istenilmiş olduğundan dava evrakı C.Başsavcılığından tebliğname ile daireye gönderilmekle incelendi. Sanık vekilinin yasal sürenin geçmesinden sonra vaki duruşma isteğinin CMUK.nun 318. maddesi uyarınca reddiyle duruşmasız inceleme yapılmasına karar verildikten sonra gereği düşünüldü: Yapılan yargılamaya, toplanıp karar yerinde gösteriten delillere, mahkemenin tahkikat neticelerine uygun olarak tecelli eden kanaat ve takdirine, tetkik olunan dosya münderecatına göre yerinde görülmeyen sair temyiz itirazlarının reddine, ancak; bir Kamu İktisadi Teşebbüsü olan Ziraat Bankasının Yıldız evler Şube-sinin tasarruf servisinde memur olarak çalışan sanığın ikinci derecede imzaya yetkili olması, bilgisayar şifresi bulunması ve hesaptan hesaba aktarma yapabilmesi dikkate alındığında paraya doğrudan vazülyet olmamakla beraber, bankanın paraları üzerinde muhafaza, denetim ve sorumluluğu bulunduğu anlaşılması ve buna dayanarak düzenlemiş olduğu gerçeğe aykırı mahsup fişleri ile bir kısım mudilerin hesaplarına virman suretiyle para aktarıp, ele geçirdiği, o mudilere ait bankkarıtlar ile hesaplarından muhtelif tarihlerde bu paraları çekmek suretiyle toplam 149.050.000 lira banka parasını mal edindiği mahkemece de kabul edilmesi karşısında dava konusu yapılan tüm eylemlerinin müteselsil şekilde nitelikli zimmet suçunu oluşturduğu gözetilince bir kısım eylemlerinin sahtecilik ve dolandırıcılık niteliğinde görülüp yazılı şekilde mahkumiyetine ve bir kısım eyleminden de beraatine karar verilmesi, Yasaya aykırı, müdahil vekilinin temyiz itirazları bu itibarla yerinde görüldüğünden hükmün (BOZULMASINA) oybirliğiyle karar verildi. Yargıtay 5. CD, 12.02.1997, E. 1997/168 – K. 1997/363. (Kaynak: Kazancı İçtihat Programı – Offline)

⁷⁰⁴ Zimmet suçundan sanık Arif'in yapılan yargılaması sonunda; eylem zincirleme biçimde dolandırıcılık niteliğinde görüldüğünden TCK.nun 504/7, 80, 522/1, 523/1,59, 647 sayılı Kanununun 6. maddeleri gereğince, 8 ay 16 gün ağır hapis, 5.035.341.666. lira ağır para cezasıyla mahkumiyetine ve cezasının ertelenmesine 100.000.000 lira güvence parasının CMUK.nun 122. maddesi gereğince sanığa iadesine dair (Erzincan Ağır Ceza Mahkemesi)nden verilen 23.3.2000 gün ve 1998/84 Esas, 2000/14 Karar sayılı hükmün süresi içinde Yargıtayca incelenmesi müdahil tarafından istenilmiş olduğundan dava evrakı C. Başsavcılığından tebliğname ile daireye gönderilmekle incelenerek gereği düşünüldü: Yapılan yargılamaya toplanan delillere hükmün dayandığı gerekçe ve takdire göre, sair temyiz itirazlarının reddine, ancak; 1- Sanığın, mudiler Ali, Ebubekir, Zarif, Mustafa ve M. Ali'nin hesaplarına bir şekilde öğrendiği müdür konumundaki bilgisayar şifresini kullanarak faiz tahakkuk ettirip daha sonra düzenlediği tahsil ve tediye fişleriyle tahakkuk ettirdiği 5.877.000.000 lirayı şubedeki diğer mudilerin hesaplarına aktarıp onlara vezneden çekirip temellük etmesinin nitelikli dolandırıcılık olarak kabulünde bir isabetsizlik yoksa da, 4.6.1999 günlü müfettiş raporunun, 51.

başka kararında ise Ziraat Bankası'nda staj yapan bir öğrencinin bilgisayar aracılığıyla "fiş ve kasa yatan işlem kodu" ile 5000.000.000. lira para yatırmış gibi işlem yaparak, başka birinin vadesiz mevduat hesabının bakiyesini yükseltmesi suretiyle iştirak halinde suç işledikleri diğer sanıkla birlikte haksız çıkar sağlaması eylemlerinin dolandırıcılık suçuna vücut verdiğine hükmedilmiştir⁷⁰⁵.

Ancak Yargıtay aynı kanun döneminde aynı kanun maddesi ile aksi yönde de kararlar vermiştir. Örneğin bir kararında, bankanın otomasyon bölge merkezinde görev yapan sanığın, görevi nedeniyle sık sık gidip personeli ile yakınlık kurduğu aynı bankanın İzmir Şubesine gidip müdür şifresini öğrendiği ve memur E.K.un bilgisayarının başında bulunmadığı bir sırada onun şifresiyle H.Ö. adına sıfır bakiyeli vadeli hesap açarak aynı gün şube mudilerinden İ.A.nun hesabını 8 milyar düşürüp H.Ö. adına açtığı hesabı, aynı miktarda yükseltmek suretiyle gerçekleştirdiği eylemin, TCK.nun 504/7 maddesinde düzenlenen dolandırıcılık suçunu değil, TCK.nun 525/b-2 maddesindeki "bilgileri otomatik işleme tabi tutmuş bir sistemi kullanarak hukuka aykırı yarar sağlamak" suçunu oluşturduğuna karar verilmiştir⁷⁰⁶. Aynı şekilde internet üzerinden bankacılık sistemlerine girilerek veya

sahifesinde vurgulandığı gibi, kendi bilgisayar şifresi ile virman, tahsil ve tediye işlemleri yapabilen, bu nedenle bankanın paralarının muhafazasından sorumlu olduğu anlaşılan sanığın, adı geçen mudiler dışındaki 60 mudinin hesaplarına faiz tahakkuku yapmadan sadece tahsit ve tediye fişleri düzenleyerek bu mudilerin hesaplarındaki 2.362.650.000 lirayı bankada diğer mudilerin hesaplarına aktarıp ve onların vasıtasıyla vezneden alarak maledinmesi eyleminin müteselsil basit zimmet niteliğinde olduğunun gözetilmemesi, 2-Müddahilinün müstakil faiz talebi hakkında müteadid paraların iç ediş tarihleri ile ödeme tarihleri nazarı itibari alınarak bilirkişi incelemesi yaptırılıp sonucuna göre bir hüküm kurulması gerekirken yazılı gerekçeyle hukuk mahkemesine dava açmakta muhtariyetine karar verilmesi, yasaya aykırı, temyiz itirazları bu itibarla yerinde görüldüğünden hükmün CMUK.nun 321. maddesi gereğince (BOZULMASINA), 11.10.2001 gününde oybirliğiyle karar verildi. Yargıtay 5. CD., 11.10.2001, E. 2001/536 – K. 2001/ 5249. (Kaynak: Kazancı İçtihat Programı – Offline)

⁷⁰⁵ Yargıtay 6. CD. 11.03.2002 , E. 2001/16187 – K. 2002/ 2789 (**KURT**, Bilişim Suçları, sh: 173'den naklen.)

⁷⁰⁶ "Dolandırıcılık suçundan sanık A.İ.E.'in yapılan yargılanması sonunda; TCK.nun 504/7, 61, 251 ve 522. maddeleri gereğince 12 ay 24 gün ağır hapis ve 8.533.333.332.-TL ağır para cezasıyla mahkumiyetine dair İZMİR 4. Ağır Ceza Mahkemesinden verilen 01.02.2001 gün ve 2000/349 Esas, 2001/37 Karar sayılı hükmün süresi içinde Yargıtay'ca incelenmesi sanık vekili tarafından istenilmiş olduğundan dava evrakı C. Başsavcılığının onama isteyen 30.04.2002 tarihli tebliğnamesi ile daireye gönderilmekle incelenerek gereği görüldü: Yapılan duruşmaya, toplanıp karar yerinde gösterilen delillere, mahkemenin tahkikat neticelerine uygun olarak tecelli eden kanaat ve takdirine, tetkik olunan dosya içeriğine göre yerinde görülmeyen sair temyiz itirazlarının reddine; ancak: **1.** ... Bankası İzmir otomasyon bölge merkezinde şef olarak görev yapan sanığın, icra ettiği görev nedeniyle sık sık gidip personeli ile yakınlık kurduğu aynı bankanın İzmir Şubesine gidip müdür şifresini öğrendiği ve memur E.K.'un bilgisayarının başında bulunmadığı bir sırada O'nun şifresiyle H.Ö. adına sıfır bakiyeli vadeli hesap açarak aynı gün şube mudilerinden İ.A.'nun hesabını 8 milyar lira düşürüp H.Ö. adına açtığı hesabı, aynı miktarda yükseltmek suretiyle gerçekleştirdiği eylemin TCK.nun 525/b-2. maddesindeki bilgileri otomatik işleme tabi tutmuş bir sistemin kullanarak hukuka aykırı yarar sağlamak suçunu oluşturduğu, icrai hareketlerin tamamlanmaması nedeniyle suçun eksik kalkışma aşamasında kaldığı gözetilmeden, suçun nitelendirilmesinde yanlışlığa düşülerek TCK.nun 504/7. maddesi uyarınca mahkumiyetine hükümlenmesi, **2.** Kabule göre de; KİT personeli olması nedeniyle uygulama alanı bulunmayan TCK.nun 251. maddesiyle artırım yapılarak sanığa fazla ceza hükümlenmesi, kanuna aykırı, sanık vekilinin temyiz itirazları bu itibarla yerinde görülmüş olduğundan hükmün bu sebeplerden dolayı CMUK'nun 321 nci maddesi uyarınca BOZULMASINA,

bankamatik kartlarıyla bankaların ağına girilerek gerçekle olmayan hayali hesaplara para yatırılması, telefon şirketlerinin bilişim sistemlerine girilerek telefon görüşmelerinin yapılmamış gibi gösterilmesi⁷⁰⁷, üniversite giriş sınavı kazanılmadığı halde ÖSYM'nin sistemine girilerek sınavın kazanılmış gösterilmesi⁷⁰⁸ gibi durumlarda da bilişim sistemi aracılığıyla hukuka aykırı menfaat temin edildiği kabul edilmiştir.

5237 sayılı TCK'de ise 765 sayılı TCK döneminde yaşanan bu yorum farklılıklarının önüne geçmek için md. 244'de bir düzenleme yapılmıştır. TCK'nin 244. maddesinin son fıkrasında 244. maddenin birinci fıkrasında düzenlenen fiillerin işlenmesi suretiyle failin kendisi veya başkasının yararına haksız çıkar sağlanması düzenlenmiştir. Suçun maddi unsurunun 244. maddenin 1. ve 2. fıkrasında yer alan fiillerin gerçekleştirilmesi suretiyle yarar sağlanması olarak düzenlenmesi sonucunda 765 Sayılı TCK'nin 525/b maddesine göre suçun unsurlarının daha belirgin hale getirilmek istendiği görülmektedir. 244. maddenin 1. ve 2. fıkralarında yer alan hareketlerin gerçekleştirilmesi suretiyle yarar sağlanması esas alınması suretiyle suçun maddi unsuru bakımından kapsamının 765 Sayılı TCK'deki düzenlemeye göre daraltıldığı görülmektedir. Nitekim 244. maddenin son fıkrası incelendiğinde suçun işlenebilmesi için ya 244/1. maddede yer aldığı şekliyle sistemin işleyişinin engellenmesi veya bozulması ya da aynı maddenin 2. fıkrasında belirtildiği şekliyle bilişim sistemi içerisindeki verilerin bozulması, yok edilmesi, değiştirilmesi, sisteme veri yerleştirilmesi, var olan verilerin başka bir yere gönderilmesi gerekmektedir.

244. maddenin son fıkrası incelendiğinde, fiilin başka bir suç oluşturmaması halinde söz konusu maddenin uygulanacağı hükmünün, madde metninde yer aldığı görülmektedir. Bu hükme göre, fiil, TCK ve diğer özel kanunlarda yer alan başka bir suçu oluşturuyorsa, bu madde kapsamında değerlendirilmeyecek ve ilgili maddelerde düzenlenen suçlara göre hüküm kurulacaktır.

Maddede, *“başka bir suçu oluşturmaması”* hükmüne yer verilmiş iken, madde gerekçesinde, *“Ancak, bu fıkra hükmüne istinaden cezaya hükmedilebilmesi için, fiilin daha*

24.10.2002 gününde oybirliğiyle karar verildi. Yargıtay 11. CD., 24.10.2002, E. 2002/5711 – K. 2002/8416” (Kaynak: Kazancı İçtihat Programı – Offline).

⁷⁰⁷ DÜLGER, Bilişim Suçları, sh: 185.

⁷⁰⁸ DÜLGER, Bilişim Suçları, sh: 185.

ağır cezayı gerektiren başka bir suç oluşturmaması gerekir. Bu bakımdan, fiilin örneğin dolandırıcılık, hırsızlık, güveni kötüye kullanma veya zimmet suçunu oluşturmaları hâlinde, bu fıkra hükmüne istinaden cezaya hükmedilmeyecektir.” ifadesine yer verilmiştir. Hüküm ile gerekçe arasında bir çelişkinin var olduğu açıkça görülmektedir. Maddede yer alan ifadeden fiilin daha ağır cezayı gerektirip gerektirmediğine bakılmaksızın başka bir suç oluşturmaları halinde ilgili suçun uygulanacağı sonucu çıkartılmakta iken, gerekçe bunu daraltmakta ve ilgili suçun daha ağır ceza gerektirmesi şartını öngörmektedir. Bu durum karşısında gerekçe ile hükmün çeliştiği ve gerekçenin bağlayıcı olmaması nedeniyle gerekçeye itibar edilmemesi gerektiği yönündeki görüşe katılmaktayız⁷⁰⁹.

Yargıtay 5237 sayılı TCK md. 244/4 düzenlemesinin interneti ilgilendiren boyutları açısından verdiği kararlara bakılacak olursa “ *başka bir suçun oluşmaması – daha ağır bir suçun oluşmaması*” çelişkinin etkileri görülebilir. Keza bu değerlendirmelerin ardından inceleme konusu fıkra ile en çok çelişki yaratan md. 142/ 2-e’de düzenlenen nitelikli hırsızlık ve md. 158/ 1-f’de düzenlenen nitelikli dolandırıcılık suçları internet açısından değerlendirilip karşılaştırmalı bakış açısıyla md. 244/4 hükmü bakımından konuları netleştirilecektir.

Yargıtay bir kararında, sanık tarafından internet üzerinden gerçekleştirilen EFT işlemiyle oluşacak suçun tamamlanma anı tartışılırken, sanığın eylemine uyan fiilin md. 244/4 kapsamında bilişim sistemleri kullanılmak suretiyle haksız menfaat temin etme suçuna vücut verdiğini kabul etmiştir⁷¹⁰. Aynı şekilde internet üzerinden bir şirketin banka hesabına yetkisiz olarak erişip daha sonra hesaptaki paraları sahte olarak açılmış bir başka hesaba aktarma suretiyle gerçekleşmiş maddi menfaat teminini md. 244/4 hükmüncü değerlendirmiştir⁷¹¹. Bu uygulama örnekleri ve fıkra hükmü birlikte değerlendirilecek olursa;

⁷⁰⁹ Eleştiri için Bkz. **KARAGÜLMEZ**, Bilişim Suçları, sh: 193.

⁷¹⁰ “*Gerçek Kişinin Resmi Belgede Sahteciliği ve Nitelikli Dolandırıcılığa Teşebbüs suçlarından sanık Levent Korku’un yapılan yargılaması sonunda: nitelikli dolandırıcılığa teşebbüs suçunun değişen vasfına göre ‘Bilişim Sistemindeki Verilen Değiştirmek Suretiyle Haksız Menfaat Elde Etmek’ ve Resmi Belgede sahtecilik suçlarından 5237 Sayılı TCK. nun 204/1 35/2 ve 62 maddeleri gereğince mahkumiyetine dair İSTANBUL 5. Ağır Ceza Mahkemesinden verilen 16.11.2006 gün ve 2006/265 Esas, 2006/314 Karar sayılı hükmün süresi içinde Yargıtay’ca incelenmesi sanık müdafli tarafından istenilmiş olduğundan dava evrakı C.Başsavcılığının bozma isteyen 28.02.2007 tarihli tebliğnamesi ile daireye gönderilen ekle incelenerek gereği görüşüldü: Bilişim sistemindeki verileri değiştirmek suretiyle haksız menfaat elde edilmesi suçunun sanık tarafından EFT şikayetçi şirketin hesabından sahte ol olduğu hesaba intikali anında tamamlandığı gözetilmeyerek eylemin teşebbüs aşamasında kaldığından bahisle eksik ceza tayini aleyhe temyiz olmadığından bozma sebebi sayılmamıştır. Yapılan duruşmaya toplan karar yerinde gösterilen delillere, mahkemenin soruşturma neticelerine uygun şekilde oluşan inanç ve takdirine, incelenen dosya içeriğine göre sanık müdafinin bir sebebe dayanmayan ve yerinde görülmemeyen sair temyiz itirazlarının reddine...” Yargıtay 11. CD., 25.06.2007, E. 2007/2168 – K. 2007/4372. (Kaynak: Kazancı İçtihat Programı - Offline)*

⁷¹¹ “*Hırsızlık suçundan kurulan mahkumiyet hükmüne yönelik temyiz itirazlarına gelince;*

md.244/4'ün uygulanabilmesi için iki temel şartın gerçekleşmiş olması aranmalıdır. Birincisi eylem neticesinde bir menfaat teminin gerçekleşmiş olması ikincisi ise menfaat temini neticesinin aynı maddenin birinci ve ikinci fıkrasında düzenlenen hareketlerin gerçekleştirilmesi suretiyle ortaya çıkmasıdır. Yukarıda birinci ve ikinci fıkrada düzenlenen seçimlik hareketlerin neyi kapsadığı üzerinde ayrıntılı bir biçimde durulmuştur. Özellikle birinci fıkrada düzenlenen seçimlik hareketler olan bir bilişim sisteminin işleyişinin engellenmesi veya bozulması suretiyle haksız çıkar elde edilmesine bir örnek verilecek olursa, bir bilişim sistemi olarak internetin sağlıklı bir şekilde çalışması bağlantının kesilmesi suretiyle engellenmesi ya da sistemin önemli parçaları olan internet süjelerinin devre dışı bırakılması suretiyle haksız bir menfaat elde edilirse md.244/4 uygulama alanı bulacaktır. Yine maddenin ikinci fıkrasında verilerin bozulması, yok edilmesi, değiştirilmesi, erişilmez kılınması, sisteme bir verinin yerleştirilmesi veya var olan bir verinin başka bir yere gönderilmesi suretiyle bir haksız menfaat temin edilecek olursa uygulanacak hüküm md. 244/4'dür. Her iki fıkra hükmünün de uygulanma alanı bulabileceği bir örnek vererek konuyu daha da somut bir hale getirmek mümkündür. İnternet ortamında gerçekleşen bir açık artırmada, katılımcılardan biri yönlendirdiği bir kötücül bir yazılımla online açık artırmanın yapıldığı programa müdahale edilip, ki bu müdahale sistemi engelleme veya bozma şekline olabilir, açık artırmının usulüne aykırı olarak sonlandırılması neticesinde haksız bir menfaat temin etmiş olsun. Yine aynı örnek üzerinden farklı bir ihtimal düşünülecek olursa, online açık artırmanın katılımcılarından biri, diğer katılımcılara yönlendirdiği bir virüs programıyla bu katılımcıların ethernet girişini devre dışı bırakarak internet bağlantılarını kesip açık artırmanın yapıldığı sistemden çıkmalarını sağlayarak bir haksız menfaat temin etsin.

Dikkat edilecek olursa yukarıda verilen örneğin birinci versiyonunda, doğrudan açık artırmanın yapıldığı programa bir müdahalede bulunulmuştur. Daha önce açıklandığı gibi programlar 5237 sayılı TCK sisteminde program “veri” hükmünde sayıldığı için bu müdahale

Sanığın evrakı tefrik edilen suç ortaklarıyla birlikte fikir ve eylem birliği içinde X şirketi adına bankası Kayseri Ticari Şubesinde bulunan nolu YTL hesabına internet üzerinden girerek mevduatta bulunan 7.250.00 YTL parayı aynı bankanın Konya şubesinde kendi fotoğrafının yapıştırıldığı V.T'ye ait kimlik bilgilerini içeren nüfus cüzdanı ile açtığı nolu banka hesabına havale edip bu şekilde hesaba yatan paradan 5.000.00 YTL'yi bankadan çektikten ve bakiye parayı çekmek isterken yakalandığı, oluşa uygun şekilde kabul edilmiş olmasına göre eylemin 5237 s. TCK 244/4 maddesinde öngörülen bilişim suçunu oluşturduğu gözetilmeden suçun nitelendirilmesinde yanlıya düşülerek hırsızlık suçundan yazılı şekilde hüküm kurulması, Yasaya aykırı görüldüğünden bozulmasına 26.09.2007 gününde oybirliğiyle karar verildi.” Yargıtay 11.CD., E. 2007/6122 – K. 2007/ 5897 (Kaynak: Kazancı İçtihat Programı - Offline)

md. 244/2 kapsamında değerlendirilecek ve bu eylem neticesinde bir haksız menfaat temin edildiği için md. 244/4 söz konusu olacaktır. İkinci versiyonda ise, açık artırma doğrudan bir veriye karşı değil ancak sistemin işleyişine karşı gerçekleştirildiği için bu kez de md. 244/1 gündeme gelecek ve bu eylem neticesinde de bir menfaat temin edildiği için yine md. 244/4 geçerli olacaktır. Yine başka bir örnek gerekirse mevduat sahibi, bankadaki hesabına internet ortamında ulaşılmasını tamamen yasaklayabileceği gibi, yapılacak işlemleri kısıtlama yoluna da gidebilir. Bu durumda, mevduat hesabı, verilen talimatta belirtilen işlemlerle sınırlı olarak internet ortamına açılmış olur. Mevduat sahibi, bankaya verdiği bir talimatla interaktif bankacılık alanının bütün para aktarma işlemlerine kapatılmasını sağlayabilir. Benzer şekilde, bankaya önceden bildirilecek hesap numaraları dışında, havale veya EFT yapılmasına yasaklama getirmek de mümkündür. Ancak mevduat sahibinin interaktif bankacılık şifresini kırıp (md.244/2) interaktif bankacılık alanına girdikten sonra ilgili bankanın merkezi bilişim sistemine internet aracılığıyla girerek bu işlem kotaları bir veriye (md. 244/2) veya doğrudan sistemin işleyişine (md.244/1) müdahale etmek suretiyle kaldırılır ve haksız menfaat temin edilirse md. 244/4 gündeme gelecektir.

Bu fıkra hükmünün uygulanması bakımından aslında en problemli alan internet bankacılığı hizmetleri dolayısıyla elde edilen haksız kazanç ve bu kazancın elde ediliş tarzıyla ilgilidir. İnternet bankacılığı, bankanın merkez veya şubelerini kullanmaksızın bankanın hesap merkezine veya işlemlerin otomatik olarak gerçekleştirildiği ortama internet aracılığıyla erişim sağlanması yoluyla bankacılık işlemlerinin yapılması olarak tanımlanabilir⁷¹².

İnternet bankacılığı çeşitli şekillerde ve değişik yapılarda ortaya çıkabilmektedir. Bazı türlerinde şubeler, internetten işlemler yaparken, diğer bir gelişim türünde ise bankanın ayrı isim ve ayrı personel ve bilgisayar altyapısıyla yeni bir banka oluşturarak internet üzerinden bankacılık faaliyetlerini gerçekleştirmektedir. Bugün itibarıyla bankaların web sayfalarında birçok farklı işlemler gerçekleştirilmekle birlikte bazı hizmetlerle bankacılık işlemlerini de aşan faaliyetler gerçekleştirilebilmektedir. Banka müşterisi olarak internet kullanıcısı, bankacılık faaliyetleri ile ilgili olarak bilgilendirilmenin yanında, kredi işlemlerini yapabilmekte, para transferlerini gerçekleştirebilmekte, fatura ödeyebilmekte ve borsa

⁷¹² 14.09.2007 tarih ve 26643 sayılı Resmî Gazete’de yayınlanan Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelerle İlişkin Tebliğ md. 3/1-j’ye göre internet bankacılığı “Müşterilerin banka tarafından sunulan hizmetlere internet yoluyla ulaşmalarını ve yapmak istedikleri işlemleri gerçekleştirmelerini sağlayan bankacılık hizmeti dağıtım kanalını” olarak tanımlanmaktadır.

işlemlerini gerçekleştirebilmektedir. Bütün bu faaliyetler de internet bankacılığı içinde düşünülmelidir⁷¹³.

İnternet ortamında işlem yapmak isteyen kişinin, internete bağlı bir bilgisayarla birlikte banka tarafından verilen bir müşteri numarası ve 6 haneli bir sayıdan oluşan şifre ile işlemlere girişmesi mümkündür. İnteraktif bankacılık şifresi, bilgisayar sistemi tarafından otomatik olarak verilir ve banka personeli de dahil hiç kimse tarafından bilinmez. Kullanıcı müşteri, internet bağlantısı bulunan bir bilgisayar aracılığıyla önce bankanın web sayfasına ve buradan da interaktif bankacılık işlemlerinin yapılabileceği alana geçiş yapar. Bu alanda, öncelikle banka tarafından sözleşme aşamasında müşteriye verilen müşteri numarası girilir, daha sonra ise mevduat sahibinin adı, soyadı internet bankacılığı şifresi ile birlikte kişiye özel bilgilerden oluşan bir sorunun cevabı verilmek suretiyle kullanıcı müşterinin işlem yapabileceği sisteme girilmektedir. Mevduat sahibi kendisine tahsis edilen işlem alanı içinde, hesabıyla ilgili bilgi almanın dışında her türlü bankacılık işlemini de yapabilir⁷¹⁴.

Bu derece önemli bir kolaylık olan internet bankacılığı aynı zamanda da birçok riski beraberinde getirmektedir. Bunların temelinde internet bankacılığı hizmetleri için öngörülmuş güvenlik sistemlerinin aşılması suretiyle haksız kazan elde edilmesi yatmaktadır. Bilindiği gibi bu neticeyi ortaya koyacak ve internet aracılığıyla gerçekleştirilebilecek birçok teknik mevcuttur. İşte kullanılacak bu tekniklere göre de elde edilecek haksız menfaat 5237 sayılı TCK'nin birden çok suçu gündeme getirecektir. Bu suçlar md. 244/4 çerçevesinde haksız menfaat temin etmek, md. 142/2-e maddesinde düzenlenen nitelikli hırsızlık ve md. 158/1-f hükmünde nitelikli dolandırıcılıktır. İnceleme konusu olan md. 244/4 ile nitelikli hırsızlık ve nitelikli dolandırıcılık arasındaki ilişkiyi Yargıtay'ın son dönemde ortaya koyduğu ve artık istikrar kazanan yaklaşımı ile değerlendirmek isabetli olacaktır.

Yargıtay son dönemde verdiği kararlarda md. 244/4 ile bilişim sistemlerini kullanmak suretiyle gerçekleştirilen nitelikli dolandırıcılığın düzenlendiği md. 158/1-f arasındaki farkı ortaya koyarken, gerçekleştirilen eylemin kime veya neye karşı gerçekleştirildiği kriteri

⁷¹³ MEMİŞ, Tekin, Elektronik Bankacılıkta Bankanın Yükümlülük ve Sorumlulukları, sh: 2, Kaynak: <http://hukukcu.com/modules/smartsection/makepdf.php?itemid=116> (Erişim Tarihi: 10.04.2009, Saat: 09:36)

⁷¹⁴ MEMİŞ, Elektronik Bankacılık, sh:2, Kaynak:<http://hukukcu.com/modules/smartsection/makepdf.php?itemid=116> (Erişim Tarihi: 10.04.2009, Saat: 09:36)

üzerinden hareket etmektedir. Buna göre hile ve desise içerikli fiil şayet herhangi bir bilişim sistemi kullanılmak suretiyle bir kişiye karşı gerçekleştiriliyor ve bu fiil neticesinde de haksız bir kazanç elde ediliyorsa burada bir bilişim sistemi kullanılmak suretiyle nitelikli dolandırıcılık suçunun işlendiği kabul edilmektedir. Örneğin bir kişi başka bir kişinin MSN parola ve şifresini ele geçirdikten sonra o kişinin listesindeki şahıslarla kurduğu internet iletişimi esnasında sanki o hesabın gerçek kullanıcısıymış gibi kendisine ait bir hesaba havale yapmalarını istemiş ve bu isteği yerine getirilerek haksız bir kazanç elde etmişse artık burada bir bilişim sisteminin araç olarak kullanılması durumu söz konusu olacağından md. 158/1-f'nin gerçekleştiği kabul edilecektir. Keza Yargıtay bir kararında durumu aynen şöyle izah etmiştir⁷¹⁵:

“Sanığın, şikayetçilere ait hesaplardan internet aracılığı ile kendi hesabına para aktarmaktan ibaret eyleminde gerçek kişiye yönelik hile ve desise bulunmadığı gözetilmeden 5237 Sayılı TCK. nun 244/4. maddesi yerine suç vasfında hataya düşülerek dolandırıcılık suçundan hüküm kurulması , ...”

Bu karardan da anlaşılacağı üzere, şayet hile teşkil eden hareketler bir bilişim sistemi aracılığıyla doğrudan bir kişiye karşı gerçekleştiriliyorsa, burada md. 244/4 değil md. 158/1-f çerçevesinde nitelikli dolandırıcılık suçu işlenmiş olacaktır. Buna başka bir örnek de internet üzerinden pazarlamacılık yaptığı izlenimi veren birinin, internet sitesinde teşir ettiği bir mal almak isteyen kişinin yine internet üzerinden tüm ödeme işlemlerini tamamlamasına rağmen söz konusu malı alıcısına ulaşturmaması hali de bir bilişim sistemi kullanılmak suretiyle nitelikli dolandırıcılık olarak değerlendirilebilir.

Özellikle Yargıtay'ın ortaya koyduğu bu ölçüt çerçevesinde md. 244/4 ile md. 158/1-f arasında uygulama sorunları nispeten giderilmesi mümkündür. Ancak kanaatimizce esas tartışmalı nokta özellikle interaktif bankacılık hizmetleri aracılığıyla internet üzerinden para transferinin gerçekleştiği durumda md. 244/4'nin mi yoksa nitelikli hırsızlığın düzenlendiği md. 142/2-e' nin mi uygulanacağıdır. Bilindiği üzere Yargıtay, yukarıda da sunduğumuz kararda da görüldüğü üzere, başkasına ait bir hesaptan internet aracılığıyla kendi hesabına para transfer eden failin eylemini md. 244/4 kapsamında değerlendirmektedir. Burada öncelikle gerçekleştirilen eylemin niteliğine bakılmalıdır. İnteraktif bankacılık hizmetleri kullanmak suretiyle internet üzerinden bir hesaptan başka bir hesaba havale işlemi gerçekleşir gerçekleşmez, havale edilen tutar kadar bir mal varlığı değeri – yani para – havale edilen

⁷¹⁵ Yargıtay 11. CD, 18.09.2007, E: 2007/6963 – K: 2007/5533 (Kaynak: Kazancı İçtihat Programı – Offline)

hesabın sahibinin tasarruf alanından çıkarak başka bir hesap sahibinin tasarruf alanına girmektedir. Bu tespit yine Yargıtay kararları dahilinde de ispat edilebilir niteliktedir. Çünkü Yargıtay haksız menfaatin elde edilme anını havale edilen paranın bankadan çekilmesi ve fiili olarak üzerinde doğrudan hakimiyet kurulması olarak değil bizatihi havale işleminin tamamlandığı anı esas almaktadır⁷¹⁶. Dolayısıyla şayet, bir kişi başka bir kişinin interaktif bankacılık bilgilerini herhangi bir şekilde ele geçirdikten sonra o şahsın hesabından kendi hesabına internet üzerinden para havalesi yaptığı takdirde, havale yapılan hesabın sahibinin rızası hilafına, onun tasarruf yetkisi dahilinde bulunan bir mal varlığı değerini, ki burada kastedilen havale yapılan paradır, kendi tasarruf alanına sokmaktadır. Bu eylemi itibariyle de kanaatimizce bilişim sistemlerinden olan interneti kullanmak suretiyle nitelikli hırsızlık suçu işlenmiş kabul edilmelidir. Ancak Yargıtay bu durumda md. 244/4’de düzenlenen ve inceleme konusu olan suçun işlendiğini kabul etmektedir. Yukarıda da ifade edildiği üzere, kanun metninde açıkça “ *başka bir suç oluşturmaması halinde...*” ifadesi kullanılmaktadır. Burada artık nitelikli hırsızlık suçu oluştuğu için ayrıca md. 244/4’ün de oluşup oluşmadığını incelemeye gerek yoktur. Ancak Yargıtay bu görüşü benimsememekte ve yukarıda da belirtildiği gibi sorunu md. 244/4’ü uygulayarak çözmektedir. Nihai olarak Yargıtayın görüşüne katılmadığımızı bir kez daha vurgulayarak, vermiş olduğu ve istikrar kazandırdığı kararlarında da çelişkilerin var olduğunu dile getiriyoruz.

Tüm bu değerlendirmelerin ardından md. 244’ü bir bütün halinde değerlendirerek suçun özel görünüş şekilleri incelenecek olursa, suçun gerek birinci ve ikinci fıkralarda düzenlenen hali gerekse dördüncü fıkrada ayrı bir suç olarak düzenlenen hali bakımından teşebbüsün mümkün olduğunu ve yine her üç hal bakımından iştirakin özel bir nitelik arz etmediğini, genle hükümlerin uygulanabileceğini söylemek mümkündür.

İçtima konusunda ise öncelikle md. 244 ile mala zarar verme suçunun düzenlendiği md. 151 arasındaki ilişkiye bakmakta fayda vardır. Taşkın’a göre, md. 244’deki suçta, suçun konusu bilişim sistemi ve bu sistemi oluşturan verilerdir. Dolayısıyla mala zarar verme suçunun düzenlendiği md. 151 ile md. 244 birbirinden tamamen farklı iki suçtur. Bu açıdan her iki suç tipi bakımından bir özel norm – genel norm ilişkisi kurulmamış, kast unsuru temelinden her iki suç tipinden birisi tespit edilmelidir. Bu değerlendirmeye yukarıda yapılan

⁷¹⁶ Yargıtay 11. CD, 18.09.2007, E: 2007/6963 – K: 2007/5533 (Kaynak: Kazancı İçtihat Programı – Offline)

açıklamalar ve madde gerekçesinde belirtilen hususlar nazarı dikkate alındığında katılmak mümkün değildir. Zira madde gerekçesinde açıkça “... Böylece sistemlere yönelik ızzar filleri özel bir suç haline getirilmiştir. Aracın fiziki varlığı ve işlemlerini sağlayan bütün diğer unsurları söz konu suçun konusunu oluşturmaktadır...” demek suretiyle bilişim sistemi kavramı dahilinde sadece yazılımı değil aynı zamanda donanım unsurlarını da suçun konusu kapsamı dahilinde değerlendirmiştir. Dolayısıyla, örneğin internet üzerinden gönderilen bir virüs nedeniyle bir bilgisayarın kullanılmaz hale gelmesi durumunda, sadece md. 244/1’in uygulanması yeterli olacaktır, ayrıca mala zarar verme suçundan dolayı md. 151’in uygulanması gerekmemektedir. Ancak derhal burada suç tipinden kaynaklanan bir ayırım yapmak gerekmektedir. İnceleme konusu maddenin birinci fıkrasında “ Bir bilişim sisteminin işleyişin engelleyen veya bozan kişi,...” demek suretiyle yasa koyucu suça konu bilişim sistemi unsurlarının veri işleme faaliyetinde olan faal unsurlar olmasını aramaktadır. Başka bir anlatımla, bir elektronik eşya mağazasında vitrinde duran, herhangi bir işlem görmeyen bir bilgisayar her ne kadar tek başına bir bilişim sistemi unsuru olsa da, bu anlamda md.244/1 anlamında bir bilişim sistemi unsuru kabul edilemez. İşte böyle bir bilgisayara karşı gerçekleştirilen harici bir müdahale md. 244/1’i değil sadece md. 151 anlamında mala zarar verme suçunu gündeme getirecektir.

SONUÇ

Modern toplumun en önemli kaynaklarından biri olan internetin bir suçluluk alanı olarak kullanılması ve bu alanda kendini hissettiren klasik veya münhasır suçlarla mücadele konusunda gerek ulusal gerekse uluslar arası ve uluslar üstü boyutta yapılanların ve yapılması gerekenlerin irdelendiği bu tez çalışmasında varılan sonucu şu üç madde kapsamında özetlemek mümkündür.

1- İnternetin her geçen gün artan oranda bireysel ve toplumsal hayatı etkiliyor olması, birçok alanla beraber hukuk alanında bilhassa da ceza hukuku alanında sorunlara neden olmaktadır. Bu sorunların kaynağına ve yine bu sorunlar karşısında ceza hukukunu özelliği kılan hareket noktalarına ilişkin birinci bölümde detaylı bir çözümleme yapılacaktır. Bu çözümlemenin ortaya koyduğu teorik arka planın ardından internete ilişkin ceza hukuku sisteminin normatif yapısı ele alınacak olursa her şeyden önce ceza hukuku bakımından internetin gelmiş olduğu durumun kısa bir değerlendirmesi yapılmalıdır.

2- Modern ceza hukuku anlayışının teknik olarak ortaya konulması ve internet suçluluğunun bu anlayış içindeki yerinin sabitlenmesi için ceza hukukunun tarihsel gelişim süreci içerisinde kat ettiği çizginin göz önünde bulundurulması gerekmektedir. Bu çerçevede “Klasik veya geleneksel ceza hukuku” olarak tanımlanan ceza hukuku anlayışının uğradığı dönüşümün neticesi olarak modern ceza hukuku anlayışı mutlak suretle klasik ceza hukuku anlayışı ile birlikte düşünülmeli ve tartışılmalıdır. Başka bir ifade ile; klasik ceza hukukunun temel özelliklerini dikkate almadan ve söz konusu dönüşümü karşılaştırmalı olarak ortaya koymadan modern ceza hukuku anlayışının bugün geldiği nokta üzerinden, modern toplumun belirleyici aracı niteliğindeki internet ekseninde şekillenen bir suçluluk alanını çözümlenmek güçtür. Öyle ki böyle bir tercih internet suçluluğuna ilişkin düzenlemelerin arkasındaki kanun koyucu inisiyatifinin yorumlanması bakımından da anlamlı olacaktır.

3- Avrupa Konseyi Siber Suç Sözleşmesi, kürselleşen dünyanın en önemli problemlerinden biri olan internet suçluluğu ile mücadele konusunda uluslar üstü standartları belirleme ve uygulamaya yöneltme bakımından çok büyük önemi haizdir. Türkiye bu Sözleşmeye imza koymasına rağmen henüz onaylamamış, dolayısıyla da uygulama alanına yansıtamamıştır. Sözleşmenin henüz onay safhasından geçememiş olmasında, sözleşme hükümleri ve düzeni konusundaki bir takım çekinceler önemli rol oynamaktadır. Bu çekincelerin en önemlisi bu sözleşme ve bu sözleşmeyle birlikte ya da paralelinde kabul edilen ek protokollerin gerektirdiği teknik ve bilgisayar alt yapının hazırlanamamış olması ile

Avrupa Birliđince belirlenen standartlarının yakalanmasında yařanan güçlükler gösterilmektedir. Ancak biliřim teknolojilerinin her geen gün geliřerek yenilenmeleri ve dođalarından kaynaklanan süreçsellikleri dolayısıyla tüm hazırlıkların veya kořulların tamamlanmıř olmasını beklemek isabetli görülmemektedir.

KAYNAKÇA

AKGÜL, Mustafa, Bilgi Toplumuna Göre İnternet, <http://bid.ankara.edu.tr/start/Internet/bil-toplum.html> (Erişim Tarihi: 19.09.2007).

AKGÜN, Fatma/ **BULUŞ**, Ercan/ **ŞEN**, Şenol, Bilgisayar Ağları Üzerinde İletilen Verilere Zarar Vermek İçin Kullanılan Önemli Teknikler ve Koruma Yollarının İncelenmesi, Kaynak: <http://ercanbulus.trakya.edu.tr/yayin/11%20ulusal%20kong%2068-BILGISAYAR%20AGLARI%20.pdf>. (Erişim Tarihi: 06.02.2007, Saat: 11:31).

AKINCI, Hatice/ **ALIC**, A.Emre/ **ER**, Cüneyt. Türk Ceza Kanunu ve Bilişim Suçları, in: İnternet ve Hukuk (Der: Yeşim ATAMER), İstanbul, 2004.

ALBRECHT, Peter, Alexis, Das Strafrecht auf dem Weg vom liberalen Rechtsstaat zum sozialen Interventionsstaat – Entwicklungstendenzen des materiellen Stafrechts, in: KritV 1988.

ALBRECHT, Peter, Alexis, Die Fonktionalisierung des Opfers im Kriminaljustizsystem, in: Die Stellung des Opfers im Rechtssystem (Hrgs: Bernd SCHUHNEMANN, Markus Dirk DUBBER), 2000.

ALİBABA, Arzu, Uluslar arası Ceza Mahkemesinin Kuruluşu, in A.Ü.H.F.D., C: 49 , S: 1-4, Ankara, 2000.

ARAL, Fahrettin, Borçlar Hukuku – Özel Borç İlişkileri, 5. Baskı, Ankara, 2003.

ARNOLD, Jörg, Beş Tezde Düşman Ceza Hukukunun Gelişim Süreçleri (Çev: İlker TEPE), in: Karşılaştırmalı Ceza Hukuku Serisi – 8 “Terör ve Düşman Ceza Hukuku” (Derleyen: Yener ÜNVER), Ankara, 2008.

ARISOY, Mine, Hakaret, in: TBBD., Sayı: 72, Ankara, 2007.

ARTUK, Mehmet Emin/ **GÖKCEN**, Ahmet/ **YENİDÜNYA**, Caner, Ceza Hukuku Özel Hükümler, Ankara, 2006.

ARTUK, Mehmet Emin, Cinsel Taciz Suçu (TCK M. 105), in: HPD, Sayı: 07, İstanbul, 2006.

ARKUT, Refik C./ **ARKUT**, İbrahim C. , İnternette Çoklu Ortam: Sorun ve Çözümler, Kaynak: <http://inet-tr.org.tr/inetconf10/bildiri/29.pdf> (Erişim Tarihi: 11.02.2008, Saat: 08:35).

AVCI, Nabi, Kitle Kültürü ve Enformatik Cehalet, Genişletilmiş 3. Baskı, Ankara, 1990.

AYDIN, Devrim, Uluslar arası Ceza Hukukunun Gelişimi, in A.Ü.H.F.D. C:51 - S: 4, Ankara, 2002.

AYDIN, Devrim, Suça Teşebbüs, sh:110, Kaynak: <http://auhf.ankara.edu.tr/dergiler/auhfd-arsiv/AUHF-2006-55-01/AUHF-2006-55-01-Aydin.pdf> (Erişim Tarihi: 07.02.2008, Saat: 10:26).

BAKIRCI, Sedat, Ceza Hukuku Genel Hükümler, Ankara, 2007.

BAŞPINAR, Veysel/ **KOCABEY**, Doğan, İnternette Fikri Hakların Korunması, Ankara, 2008.

BAYDEMİR, Erdal, Cinsel Dokunulmazlığa, Kişi Hürriyetine ve Genel Ahlaka Karşı Suçlar, Ankara, 2007.

BECENİ, Yasin, Siber Uzayda Mahremiyet, İstanbul, 2004, Kaynak: http://www.bilisimsurasi.org.tr/hukuk/docs/siber_uzayda_mahremiyet.pdf (Erişim Tarihi: 22.09.2007).

BEICHNER, Serway, Fizik – 2 (Çeviri Editörü: Kemal Çolakoğlu), Beşinci Baskıdan Çeviri, Ankara, 2002.

BEISER, Arthur, Modern Fiziğin Kavramları (Çev: Gülşen ÖNENGÜT), İstanbul, 1997.

BIÇAK, Vahit, Avrupa İnsan Hakları Mahkemesi Kararlarında İfade Özgürlüğü, Ankara, 2002.

BREMER, Karsten, Strafbare Internet- Inhalte in internationale Hinsicht, (Diss.), (Kaynak: <http://deposit.ddb.de/cgi-bin/dokserv?idn=963762524>) (Erişim Tarihi: 08.11.2007, Saat: 22:20).

BOESE, Oliver, Strafrechtliche Verantwortlichkeit für Verweisungen durch Links im Internet (Diss.), Kaynak: <http://deposit.ddb.de/cgi-bin/dokserv?idn=963762524> (Erişim Tarihi: 08.11.2007, Saat: 14:10)

CAN, Osman, Anayasa Değişiklikleri ve Düşünceyi Açıklama Özgürlüğü, www.anayasa.gov.tr/eskisine/anyarg19/can.pdf (Erişim Tarihi: 18.09.2007)

CAN, Osman, Düşünceyi Açıklama Özgürlüğü Anayasal Sınırlar Açısından Neler Değişti?, <http://ogrenci.hacettepe.edu.tr/~b0122202/Inetpub/wwwroot/hukuk/anayasahukuk/dusunceyi%20Aciklama%20ozgurugu.htm> (Erişim Tarihi: 18.09.2007)

CANBEK, Gürol/ **SAĞIROĞLU**, Şeref, Kötücül ve Casus Yazılımlar: Kapsamlı Bir Araştırma, in: GÜMFD, Cilt:22/1, Ankara, 2007.

CANBEK, Gürol/ **SAĞIROĞLU**, Şeref, Bilgisayar Sistemlerine Karşı Yapılan Saldırıları ve Türleri: Bir İnceleme, in: EÜSBED, Cilt: 23 (1-2), 2007.

CENTEL, Nur/ **ZAFER**, Hamide/ **ÇAKMUT**, Özlem, Kişilere Karşı İşlenen Suçlar, Cilt: 1, İstanbul, 2007.

CİN, Onursal, İnsan Üzerinde Deney ve Organ Nakli, Kaynak: <http://www.ceza-bb.adalet.gov.tr/makale/147.doc> (Erişim Tarihi: 06.02.2008, Saat: 10:54).

COLLARDIN, Markus, Straftaten im Internet, in: CR, 1995.

ÇAKIR, Hüseyin/ **YALÇIN**, Nursel, İnternet ve İnternete Dayalı Sanal Dershane Sistemi, Kaynak: <http://www.ksef.gazi.edu.tr/dergi/pdf/Cilt-14-No1-2006Mart/101-112.pdf> (Erişim Tarihi: 06.02.2008, Saat: 13:24).

ÇELİK/ERASLAN, İnternet Toplumu Oluşum Süreci, <http://inettr.org.tr/inetconf9/bildiri/45.doc> (Erişim Tarihi: 18.09.2007, Saat: 14:10).

ÇETİN, Erol, Yeni Türk Ceza Yasasındaki Hakaret Suçları, 2. Baskı, Ankara, 2007.

ÇINAR, Ali Rıza, Tehdit Suçu, Ankara, 2002.

ÇOBAN, Hasan, Bilgi Toplumuna Planlı Geçiş: Gelecekte Kaçılmaz: Bilgi Toplumuna Planlı Geçiş İçin Stratejik Planlama ve Yönetim Bilgi Sistemi Uygulamaları, İstanbul, 1997.

ÇÖLKESEN, Rifat/ **ÖRENCİK**, Bülent, Bilgisayar Haberleşmesi ve Ağ Teknolojileri, İstanbul, 2003.

DAŞKIRAN, Levent, Sanal Tehdit: Bilgisayar Virüsleri, in: Bilim ve Teknik/ Ek – Mayıs, Ankara, 2005.

DEĞİRMENCİ, Bilişim Suçları Alanında Yapılan Çalışmaları ve Bu Suçların Mukayeseli Hukukta Düzenlenişi (Kaynak: <http://www.caginpolisi.com.tr/37/59-60-61-62-63-64.htm>, Erişim Tarihi: 08.11.2007, Saat: 00:15).

DEMİRBAŞ, Timur, Ceza Hukuku Genel Hükümler, 5. Baskı, Ankara, 2007.

DÖNMEZER, Sulhi, Genel Ceza Hukuku Dersleri, İstanbul, 2002.

DÖNMEZER, Sulhi. Kişiler ve Mala Karşı Cürümler, 16. Baskı, İstanbul, 2001.

DURU, Nevcihan, Etkileşimli İnternet, in: Türkiye Bilişim Ansiklopedisi Baş Editörler: Tuncer ÖREN, Tuncer ÜNEY, Rifat ÇÖLKESEN), İstanbul, 2007.

DURŞUN, Selman, İnternette Kaynaklanan Ceza Sorumluluğundaki Gelişmeler, in: MHB, Yıl 23/Sayı 1-2, İstanbul, 2003.

DÜLGER, Murat Volkan, Bilişim Suçları (**DÜLGER**, Bilişim Suçları), Ankara, 2004.

EICKER, Andreas, Ceza Hukukunun Prosedürleştirilmesi Işığında Terörle Mücadele Kanunu Yapma (Çev. Ali Kemal YILDIZ), in: Karşılaştırmalı Ceza Hukuku Serisi – 8 “Terör ve Düşman Ceza Hukuku” (Derleyen: Yener ÜNVER), Ankara, 2008.

EKİNCİ, Mustafa/ **ESEN**, Sinan, Hırsızlık, Yağma, Güveni Kötüye Kullanma, Dolandırıcılık, Hileli ve Taksirli İflas, Karşılıksız Yararlanma, Belgelerde Sahtecilik ve Bilişim Alanında Suçlar, Ankara, 2005.

ER, Cüneyt, Biyometrik Yöntemler ve Özel Hayatın Gizliliği Hakkı, Ankara, 2007.

EREM, Faruk/ **TOROSLU**, Nevzat, Türk Ceza Hukuku Özel Hükümler, 8. Baskı, Ankara, 2000.

ERGÜN, İsmail, Siber Suçların Cezalandırılması ve Türkiye’de Durum, Ankara, 2008.

ERK, Şevket, Fizik Ders Notları – Elektrik ve Manyetizma, Cilt 3, İstanbul, 1989.

ERKAN, Hüsnü, Bilgi Toplumu ve Ekonomik Gelişme, Ankara, 1993.

ERKUNT, Hamdi/ **AKPINAR**, Yavuz, İnternet Tabanlı ve İnternet Destekil Eğitim: Kurumsal Bir Eğitim Yönetim Sistemi Örneği, Kaynak: <http://cet.boun.edu.tr/faculty/erkunt/papers/AUUE2002bildiri.pdf> (Erişim Tarihi: 06.02.2008, Saat: 12:42).

ERMAN, Barış, Alman Hukukunun İnternette Kaynaklanan Ceza Sorumlulukları, in: İÜHF. Cilt: LIX , Sayı: 1-2, İstanbul , 2001.

ERMAN, Sahir, Hakaret ve Sövme Suçları, İstanbul, 1989.

ERSOY, Eren, Gizlilik, Bireysel Haklar, Kişisel Verilerin Korunması, <http://ab.org.tr/ab06/bildiri/6.doc> (Erişim Tarihi: 22.09.2007).

ERSOY, Yüksel, Genel Hukuki Koruma Çerçevesinde Bilişim Suçları (**ERSOY**, Bilişim Suçları), in : AÜSBFD, Cilt 49 Sayı: 3-4; Ankara, 1994.

ERZİN, Engin, Konuşma ve Ses Sıkıştırma, in: Türkiye Bilişim Ansiklopedisi (Baş Editörler: Tuncer ÖREN, Tuncer ÜNEY, Rifat ÇÖLKESEN), İstanbul, 2007.

ESER, Albin, Internet und Internationales Strafrecht, in: Rechtsfragen des Internet und der Informationsgesellschaft: Symposium der rechtswissenschaftlichen Fakultäten der Albert-Ludwigs-Universität Freiburg und der Städtischen Universität Osaka, Heidelberg, 2002.

GEDİK, Ömer, Türkiye’de Kitle İletişim Özgürlüğü, Ankara, 2008.

GORNIG, Gilbert – Hanno, Aeusserungsfreiheit und Informationsfreiheit als Menschenrechte, Berlin, 1988.

GROPP, Walter, Strafrecht Allgemeiner Teil, Leibzig, 1997.

GÜNDÜZ, H. Coşkun/ **SEVİNÇ**, Emre, eMBA: İnternet Tabanlı Yükseköğretimde Başarılı Bir Sistem, Kaynak: <http://cs.bilgi.edu.tr/~cgunduz/emba-baku-makale.pdf> (Erişim Tarihi: 06.02.2008, Saat: 12:48).

GÜRGEN, Fikret, Çokluortam Hizmetleri, in: Türkiye Bilişim Ansiklopedisi Baş Editörler: Tuncer ÖREN, Tuncer ÜNEY, Rifat ÇÖLKESEN), İstanbul, 2007.

GÜVEN, Bilhan, Hasta Kayıtlarının Gizliliği Prensibi, in: Uğur Alacakaptan’a Armağan – 1 (Der: Mehmet Murat İNCEOĞLU), İstanbul, 2008.

HAKERİ, Hakan, Ceza hukuku Genel Hükümler, 7. Baskı, Ankara, 2008.

HAKERİ, Hakan. Tötungsdelikte Im Türkischen Stgb-Entwurf 1997,(http://www.akader.info/KHUKA/7_2000_ekim/totungsdeligte.htm, Erişim Tarihi: 08.07.2007)

HASSAMER, Winfried, Absehbare Entwicklungen in Strafrechtsdogmatik und kriminalpolitik, in: Strafrechtprobleme an der Jahrtausendwende (Hrsg: Cornelius Prittwitz/ Ioannis Manelokadis) , 2000.

HASSAMER, Winfried, Kennzeichen und Risiken des Modernen Strafrechts, in Zeitschrift für Rechtspolitik, Heft: 10, 1992.

HASSAMER, Winfried, Staat, Sicherheit und Information, http://www.alfred-buellesbach.de/PDF/21_Hassemer_Staat.pdf (Erişim Tarihi: 18.09.2007, Saat: 14:44).

HASSAMER, Winfried, Symbolische Strafrecht und Rechtsgüterschutz, NStZ, Heft 12, 1989.

HECKER, Bernd, Europäisches Strafrecht als Antwort auf transnationale Kriminalität?, in: JA, Heft 8/9, 2002.

HEINRICH, Bernd, Aktuelle Probleme des Internetstrafrecht, Kaynak : <http://thinklaw.wordpress.com/2006/11/30/prof-dr-bernd-heinrich-aktuelle-probleme-des-internetstrafrechts> (Erişim Tarihi: 08.11.2007, Saat: 09:50).

HEINRICH, Bernd, Einführung eines Straftatbestands für das so genannte Stalking, Kaynak: <http://www.rewi.hu-berlin.de/jura/ls/hnr/lehre/studienarbeiten/stalking.pdf> (Erişim Tarihi: 06.02.2008, Saat: 15:46).

HELVACIOĞLU, Aslı Deniz, Avrupa Konseyi Temel Siber Suç Sözleşmesi Temel Hükümlerinin İncelenmesi, in: İnternet ve Hukuk (Der: Yeşim ATAMER), İstanbul, 2004.

HERZOG, Felix, Gesellschaftliche Unsicherheit und strafrechtliche Daseinvorsorge, Heidelberg, 1991.

HILGENDORF, Eric/ **FRANK**, Thomas/ **VALERIUS**, Brain, Computer- und Internetstrafrecht , Berlin – Heidelberg, 2005.

HILGENDORF, Eric/ **HONG**, Seung – Hee, Cyberstalking – Eine neue Variante der Internetkriminalität, in: Kommunikation & Recht, 2003.

HILGENDORF, Eric (Unter Mitarbeiter von Thomas FRANK, Brain VALERIUS), Die deutsche Strafrechtsentwicklung 1975 – 2000- Reformen im Besonderen Teil und neue Herausforderungen (**HILGENDORF**, Die deutsche Strafrechtsentwicklung 1975 – 2000), in: Das Strafgesetzbuch, Sammlung der Änderungsgesetze und Neubekanntmachungen (Hrsg: Thomas Vormbaum/Jürgen Welp), Berlin, 2004.

HILGENDORF, Eric, Die Neuen Medien und das Strafrecht (**HILGENDORF**, Die Neuen Medien), in: Zeitschrift für die Gesamte Strafrechtswissenschaft 113, Heft 4, Berlin/Newyork, 2001.

HILGENDORF, Eric, Ist das Internet ein rechtsfreier Raum? in: Kriminalität im Internet - Strategien zu ihrer Bekämpfung. Kooperationstagung der dbb akademie und der Deutschen Polizeigewerkschaft im dbb am 12.11. 2001/ München, Bonn 2002.

HILGENDORF, Eric, Nationales oder transnationales Strafrecht? Europäische Strafrecht, Völkerstrafrecht und Weltgrundsatz im Zeitalter der Globalisierung, in: Raum und Recht , Festschrift für 600 Jahre Würzburger Juristischenfakultät (Der: Horst DREIER, Hans FORKEL, Klaus LAUBENTHAL), Berlin, 2002.

HILGENDORF, Eric, Strafrechtliche Produzentenhaftung in der “Rizikogesellschaft” (**HILGENDORF**, Strafrechtliche), Berlin, 1993.

HILGENDORF, Eric, Tendenzen und Probleme einer Harmonisierung des Internetstrafrechts auf Europaeischer Ebene, in: Internet- Recht und Strafrecht (Hrsg: Christian SCHWARZENEGGER/ Oliver ARTER /Florian S. JÖRG), Bern, 2005.

HILGENDORF, Eric, Yeni Medya Araçları ve Ceza Hukuku (Çev: Mehmet Cemil OZANSÜ) (**HILGENDORF**, Yeni Medya Araçları), in: Karşılaştırmalı Güncel Ceza Hukuku Serisi, Cilt:7 “Özel Yaşam, Medya ve Ceza Hukuku, (Derleyen: Yener ÜNVER) Ankara, 2007.

HONG, Seung- Hee, Flexibilisierungstendenzen des modernen Strafrechts und das Computerstrafrecht (**HONG**, Flexibilisierungstendenzen) , <http://w3.ub.uni-konstanz.de/v13/volltexte/2003/954/pdf/Hong.pdf> (Erişim Tarihi : 17.09.2007, Saat: 08:00).

HONG, Seung Hee, Compu-Serve Davası (Çev: İlker TEPE) (**HONG**, Compu- Serve) , in: Karşılaştırmalı Ceza Hukuku Serisi - 7 “Özel Yaşam, Medya ve Ceza Hukuku” (Der: Yener ÜNVER), Ankara, 2007.

HONG, Seung Hee, Auschwitz Yalamı (Çev:Emin KOÇ), in: Karşılaştırmalı Ceza Hukuku Serisi - 7 “Özel Yaşam, Medya ve Ceza Hukuku” (Der: Yener ÜNVER), Ankara, 2007.

HONG, Seung Hee, Çocuk Pornografisi (Çev:Pınar BACAKSIZ), in: Karşılaştırmalı Ceza Hukuku Serisi - 7 “Özel Yaşam, Medya ve Ceza Hukuku” (Der: Yener ÜNVER), Ankara, 2007.

İNANICI, Haluk, Bilişim ve Yazılım Hukuku Uygulama İçinden Görünüşü, in: İBD, Cilt: 70/7-8-9, İstanbul, 1996.

İÇEL, Kayıhan Avrupa Konseyi Siber Suç Sözleşmesi Bağlamında “Avrupa Siber Suç Politikasının Ana İlkeleri, in: İHFM, C. LIX, S. 1-2, 2001.

İÇEL, Kayıhan/**DONAY**, Süheyl, Karşılaştırmalı ve Uygulamalı Ceza Hukuku – Genel Kısım – (**İÇEL/ DONAY**, Ceza Hukuku) , 4. Baskı, İstanbul, 2005.

İÇEL, Kayıhan, Haberleşme Özgürlüğü, in: İ.Ü.H.F.M., C:XLI - S: 1-2, İstanbul, 1975,

İÇEL, Kayıhan, Suç Teorisi (**İÇEL**, Suç Teorisi), 2. Baskı, İstanbul, 2000.

İÇEL, Kayıhan/ **ÜNVER**, Yener, Kitle Haberleşme Hukuku, 7. Bası, İstanbul, 2007.

İLKİZ, Fikret, İnternet Ortamında Yayınlar, in: İnternet ve Hukuk (Der: Yeşim ATAMER), İstanbul, 2004.

JAKOBS, Günther, Düşman Ceza Hukuku?- Hukukiliğin Şartlarına Dair Bir İnceleme (Çev: Mehmet Cemil OZANSÜ), Karşılaştırmalı Ceza Hukuku Serisi – 8 “Terör ve Düşman Ceza Hukuku” (Derleyen: Yener ÜNVER), Ankara, 2008.

JAKOBS, Günther, Yurttaş Ceza Hukuku ve Düşman Ceza Hukuku (Çev: Mehmet Cemil OZANSÜ), in: Karşılaştırmalı Ceza Hukuku Serisi – 8 “Terör ve Düşman Ceza Hukuku” (Derleyen: Yener ÜNVER), Ankara, 2008.

JESCHECK, Hans Heinrich/ **WEIGEND**, Thamas, Lehrbuch des Strafrechts/ Allgemeiner Teil (**JESCHECK/ WEIGEND**, Lehrbuch), 5. Baskı, Berlin, 1996.

JUNKER, Markus, Anwendbares Recht und internationale Zuständigkeit bei Urheberrechtsverletzungen im Internet, sh: 47, Kaynak: <http://www.upress.uni-kassel.de/online/frei/978-3-933146-78-6.volltext.frei.pdf> (Erişim Tarihi: 12.02.2008, Saat: 11:17)

KABOĞLU, İbrahim, Pozitif Anayasa Hukukunda Düşünce Özgürlüğünün Sınırları, Düşünce Özgürlüğü (Derleyen: Hayrettin ÖKÇESİZ), İstanbul, 1998.

KABOĞLU, İbrahim, Özgürlükler Hukuku, 4. Baskı, İstanbul, 1998.

KANGAL, Zeynel, Fransa'da İnternet Yoluyla İlenen Suçlardan Doğan Ceza Sorumluluğu, in: İÜHFM, LIX / 1-2, İstanbul, 2001.

KAPLAN, Yavuz, İnternet Ortamında Fikri Hakların Korunmasına Uygulanacak Hukuk, Ankara, 2004.

KARAGÜLMEZ, Ali, Bilişim Suçları ve Soruşturma – Kovuşturma Evreleri (**KARAGÜLMEZ**, Bilişim Suçları), Ankara, 2005.

KARAHASAN, Mustafa Reşit, Türk Borçlar Hukuku Genel Hükümler, Cilt – 1, İstanbul, 1992.

KETİZMEN, Muammer, Türk Ceza Hukukunda Bilişim Suçları (**KETİZMEN**, Bilişim Suçları), Ankara, 2008.

KESKİN, Serap Avrupa Konseyi Siber Suç Sözleşmesinde Ceza Muhakemesine İlişkin Hükümlerin Değerlendirilmesi, İHFM, C. LIX, S. 1-2, İstanbul, 2001.

KOÇAK, Mustafa, Düşünceyi Açıklama ve Yayma Özgürlüğünün Bir Sınırlanma Nedeni Olarak “Cumhuriyetin Nitelikleri, <http://www.e-akademi.org/makaleler/mkocak-1.htm>, (Erişim Tarihi: 15.01.2008).

KOCA, Mahmut, YTCK'da Hukuka Uygunluk Nedenleri (**KOCA**, Hukuka Uygunluk Nedenleri), in: CHD (Ed: Veli Özer ÖZBEK), Sayı: 1, Ankara, 2006.

KOCH, Arnd, Nationales Strafrecht und globale Internet – Kriminalitaet, in: GA – 2002.

KÖKSAL, Aydın, Bilişim Devrimi, Küreselleşme ve Uygarlıklar Çatışması Ortamında Kimliğini Arayan Türkiye, Kaynak: http://www.bilisimltd.com.tr/akoksal/yayinlar/2003/Bilisim_Devrimi_Kuresel_Uygar_Catismasi.html (Erişim Tarihi: 18.09.2007, Saat: 22:00)

KÖKSAL, Aydın, Bilişim Toplumu, in: Türkiye Bilişim Ansiklopedisi (Baş Editörler: Tuncer ÖREN, Tuncer ÜNEY, Rifat ÇÖLKESEN), İstanbul, 2007.

KUÇURADİ, İoanna, Düşünce Özgürlüğü: Nedir Acaba?, in: Düşünce Özgürlüğü (Derleyen: Hayrettin ÖKÇESİZ), İstanbul, 1998,

KURT, Levent. Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Hukukundaki Uygulaması, Ankara, 2005.

KUTLU, Işıl, İnternet: Olanaklar ve Hayaller, Kaynak: <http://www.bianet.org/bianet/yazdir/8729> (Erişim Tarihi: 06.02.2008, Saat: 16:10).

KUZU, Burhan, Düşünceleri Açıklama Özgürlüğü Alanında Geldiğimiz Nokta, in İÜHF. C: LIX – S:1-2, İstanbul, 2001,

LAMPE, Ernst- Joachim, Düşünce Özgürlüğü, İfade Özgürlüğü, Demokrasi (Çev: Nihat ÜLNER), in: Düşünce Özgürlüğü (Derleyen: Hayrettin ÖKÇESİZ), İstanbul, 1998.

MALEK, Klaus, Düşman Ceza Hukuku – 2006 Yılı 30. Müdafiler Günündeki “Düşman Ceza Hukuku – Hukuk Devletindeki Hortlak” Çalışma Grubuna İlişkin Birkaç Düşünce (Çev: Yener ÜNVER), in: Karşılaştırmalı Ceza Hukuku Serisi – 8 “Terör ve Düşman Ceza Hukuku” (Derleyen: Yener ÜNVER), Ankara, 2008.

MALEK, Klaus, Strafsachen im Internet, Heidelberg, 2005.

MAHMUTOĞLU, Fatih S., Karşılaştırmalı Hukuk Bakımından İnternet Süjelerinin Ceza Sorumluluğu, in: İÜHF. C: LIX / 1-2, İstanbul, 2001.

MEMİŞ, Tekin, Hukuki Açından Kitlelere E- Posta Gönderilmesi (Spamming), Kaynak: <http://inet-tr.org.tr/inetconf7/bildiriler/12.doc> (Erişim Tarihi: 06.02.2008, Saat: 14:00).

MEYER, Frank, Strafbarkeit und Strafwürdigkeit von “Stalking” im deutschen Recht, in: ZStW, 2003.

MEYDAN, Nihat/ **YAPAL**, Fadime, İctihatlı Türk Ceza Kanunu, II. Cilt, İstanbul, 2004.

NAUCKE, Wolfgang, Über die Zerbrechlichkeit des rechtsstaatlichen Strafrecht, Baden-Baden, 2000.

NEUBACHER, Frank/ **ROLLO**, Giorgia, Çocuk Pornografisi ve İnternet – Karşılaştırmalı Hukuk Çerçevesinde Genel Bir Bakış (Çev:İlker TEPE), in: Karşılaştırmalı Ceza Hukuku Serisi – 4 “Çocuklar, Suç ve Ceza” (Der: Yener ÜNVER), Ankara, 2005.

NIGGLI, Marcel Alexander, İrk Ayrımcılığı ve İnternet (Çev:İlker TEPE), in: Ceza Hukuku Dergisi, Yıl: 2 Sayı:1, Ankara, 2007.

OGILVIE, Emma, Cyberstalking, Kaynak: <http://www.aic.gov.au/publications/tandi/ti166.pdf> (Erişim Tarihi: 06.02.2008, Saat: 15:31).

OSKAY, Ünsal, XIX. Yüzyıldan Günümüze Kitle İletişimin Kültürel İşlevleri – Kuramsal Bir Yaklaşım , Ankara, 1992

ÖCAL, Fatih/ **BİLGE**, Hasan Şakir, Güvenli İletişim İçin Donanımsal Şifreleme Sistemi, in: Ulusal Elektronik İmza Sempozyumu – Bildiriler Kitabı, Ankara, 2006.

ÖKÇESİZ, Hayrettin, “Düşman Ceza Hukuku” Düşüncesinin Eleştirisi (**ÖKÇESİZ**, Eleştirisi) , in: Karşılaştırmalı Ceza Hukuku Serisi – 8 “Terör ve Düşman Ceza Hukuku” (Derleyen: Yener ÜNVER), Ankara, 2008.

ÖKÇESİZ, Hayrettin, Düşüncenin Özgürlüğü Üzerine Düşünceler, in : HFSA (Der: Hayrettin ÖKÇESİZ), Sayı – 6, İstanbul, 2002.

ÖNDER, Ayhan, Ceza Hukuku Genel Hükümler C: II, İstanbul, 1989.

ÖZBEK, Veli Özer, 21. Yüzyılda Ceza Adaleti, in: HFSA(Der: Hayrettin ÖKÇESİZ), Sayı: 13, İstanbul, 2005.

ÖZBEK, Veli Özer, TCK İzmir Şerhi, 3. Baskı, Ankara, 2006.

ÖZCAN, Onur, Türk Hukukunda Çevre Suçları, in: Uğur Alacakaptan’a Armağan -1 (Der: Mehmet Murat İNCEOĞLU), İstanbul 2008.

ÖZDİLEK, Ali Osman, İnternet ve Hukuk, İstanbul, 2002.

ÖZDİLEK, Ali Osman, İntihar ve İnternet, <http://www.turk.internet.com/abone/login.php?l=2&location=/haber/yazigoster.php3?yaziid=6532> (Erişim Tarihi: 10.12.2007).

ÖZEL, Cevat. Bilişim Suçları İle İletişim Faaliyetleri Yönünden Türk Ceza Kanunu Tasarısı, İstanbul Barosu Dergisi, Cild – 75/ Sayı 7,8,9, İstanbul, 2004.

ÖZEL, Cevdet, 5237 Sayılı Türk Ceza Kanunu’nun Basın Yayın Yoluyla İlenen/ İşlenmesi Mümkün Olan Suçlar Yönünden İncelenmesi, http://www.turkhukuk sitesi.com/makale_713.htm (Erişim Tarihi: 10.12.2007).

ÖZEN, Mustafa, Ceza Hukukunda Fikri İçtima, in: TBBD., Sayı:73, Ankara, 2007.

ÖZGENÇ, İzzet, Türk Ceza Hukuku Genel Hükümler, 2. Baskı, Ankara, 2007.

ÖZTAN, Bilge, Şahsın Hukuku, 7. Baskı, Ankara, 1997.

ÖZTÜRK/ERDEM, Uygulamalı Ceza Hukuku ve Güvenlik Tedbirleri Hukuku (**ÖZTÜRK/ERDEM**, Uygulamalı Ceza Hukuku) , 9. Baskı, Ankara, 2006.

PARLAR, Ali/ **HATİPOĞLU**, Muzaffer, Açıklamalı – İçtihatlı Özel Ceza Yasaları, Ankara, 2003.

PRADEL, Jean, Ceza Hukukunun Küreselleşmesi: Beklentiler ve Perspektifler (Çev: Zeynel T. KANGAL), in: MHB, Yıl: 24, Sayı:1-2, İstanbul, 2004.

PRITTWITZ, Cornelius, Risiken des Risikostrafrechts (**PRITTWITZ**, Risiken) , in: Konstruktion der Wirklichkeit durch kriminalität und Strafe (Der: Detlev FREHSEE, Gabi LÖSPER, Gerlinda SMAUS), Baden – Baden, 1994.

RÜTHER, Werner, Phänomene der Internetdelinquenz, Kaynak: www.cyber-crime.info/medien-material/internetdelinquenz/ (Erişim Tarihi: 08.11.2007, Saat: 11:16).

RYSER, Dominic, “Computer Forensics”, eine neue Herausforderung für Das Strafprozessrecht, in: Internet – Recht – Strafrecht, Bern, 2005.

SALİHPAŞAOĞLU, Yaşar, Türkiye’de Basın Özgürlüğü, Ankara, 2007.

SANCAR, Türkan Yalçın, Alenen Tahkir ve Tezyif Suçları, 2. Baskı, Ankara, 2006.

SANCAR, Türkan Yalçın, Ceza Hukuku – Politika İlişkisi ve TCK’nın 301. maddesi Bağlamında Düşünce Özgürlüğü Sorunu, in: HFSA (Der: Hayrettin ÖKÇESİZ), Sayı – 15, İstanbul, 2006.

SANCAR, Türkan YALÇIN, Teni Türk Ceza Kanununda Zincirleme Suç, in: TBBD, Sayı: 70, Ankara, 2007.

SAYAR, Hande/ **DALKILIÇ**, Mehmet E., İnternet’te Kişisel Bilgi Güvenliği İçin Anonimleştirici Servisler Üzerine Bir İnceleme, Kaynak: <http://ab.org.tr/ab05/tammetin/133.pdf> (Erişim Tarihi: 06.02.2008, Saat: 11:06).

SCHREIBER, Wolfgang, Phänomenologie und Lagebilder der Intenetkriminalität, Vortragmanuskript, Europäische Polizeiakademie, **CEPOL**- Seminar, Rechtsprobleme im Zusammenhang mit der Internet, Münster, 2001.

SCHWARZENEGGER, Christian, Die internationale Harmonisierung des Computer- und Internetstrafrechts durch die Convention on Cybercrime von 23 November 2001, in: Strafrecht, Strafprozessrecht und Menschenrechte – Festschrift für Stefan **TRECHSEL** zum 65. Geburtstag (Hrsg.: Andreas DONATCH, / Marc FORSTER / Christian SCHWARZENEGGER), Zürich, 2002.

SELÇUK, Sami, Düşün Özgürlüğü, in: HFSA (Der: Hayrettin ÖKÇESİZ), Sayı – 12, İstanbul, 2005.

SEROZAN, Rona, Borçlar Hukuku Özel Bölüm, İstanbul, 2002.

SEVÜK, Handan Y., 5237 Sayılı Türk Ceza kanununda Cinsel Saldırı ve Cinsel Taciz Suçları, in: TBBD, Sayı: 57, Mart/Nisan, Ankara, 2005.

SEZAL, İhsan, “Enformasyon Toplumu ve Demokrasi”, in : Sosyoloji Konuşmaları, (Derleyen: Saadettin ELİBOL), Ankara, 1991.

SIEBER, Ulrich, Ceza Hukukunun Sınırları (Çev: Feridun YENİSEY), in: Alman Ceza Hukukuna Giriş, İstanbul, 2007.

SIEBER, Ulrich, Internationales Strafrecht. Das Territorialitätsprinzip der §§3, 9 StGB im globalen Cyberspace, in : NJW, 1999.

SINAR, Hasan, İnternet ve Ceza Hukuku (**SINAR**, İnternet) , İstanbul, 2001.

SÖZÜER, Adem, Basın Suçlarında Ceza Sorumluluğu, İstanbul, 1996.

STEPHAN, Nadine, Zum Phänomen und Zum Umgang mit Cyberstalking, Kaynak : <http://www.uni-bonn.de/~ujr701/Startseite/Texte/Vonwem/CyberCrime-CyberCrimeKontrolle-SS2003/SammlungCyberCrime/>

[Stephan.pdf \(Erişim Tarihi: 06.02.2008, Saat: 15:35\)](#)

STILO, Leo, Çocuk Pornografisine Karşı Avrupa Birliği Müdahalesi: 22 Aralık 2003 Tarihli 2004/ 68 GAI Konseyin Çerçeve Kararı Hakkında Bir Yorum (Çev: Vesile Sonay EVİK), in: Karşılaştırmalı Güncel Ceza Hukuku Serisi, Cilt: 4 “Çocuklar ve Suç- Ceza” (Der: Yener ÜNVER), Ankara, 2005.

SÜREN, Özlem KOÇAK, Organ Naklinin Yasal ve Etik Açından İncelenmesi, in: TBBD., Sayı: 73, Ankara, 2007.

ŞAHBAZ, İbrahim, Karşılaştırmalı Düşünceyi Açıklama Özgürlüğü, Ankara, 2007.

ŞAŞIOĞLU, A. Betül/ **ACAR**, Doğan/ **GÜNEŞ**, İs posta/ **BAHADIR**, Ömer/ **ÇAKMAKKAYA**, Zerrin, Güvenli Kurumsal Mesajlaşma Uygulamaları

ŞEN, Ersan, Devlet ve Kitle İletişim Araçları Karşısında Özel Hayatın Gizliliği ve Korunması, İstanbul, 1996.

ŞEN, Ersan, Hürriyete Karşı İşlenen Suçlar, in: YÜHFD, Cilt:II Sayı:2, İstanbul, 2005.

TANILIR, Mehmet Niyazi, İnternet Suçları İle Mücadele Ederken Bireysel Mahremiyetin Korunması: Hükümetlerin İkilemi (Kaynak: http://w3.icisleri.gov.tr/ortak_icerik/w3.icisleri/tezler_internetsuclari.doc, Saat: 22:15).

TEKELİ, Hasan, Bilgi Çağı: Bilgi Çağının Sosyal, Kültürel, Ekonomik Etkileri, İstanbul, 1994.

TARHAN, Emine Ülker, Yeni Türk Ceza Yasasında Tehdit ve Hakaret Suçları, Ankara, 2007.

TAŞKIN, Şaban Cankat, Bilişim Suçları, Bursa, 2008.

TIEDEMANN, Klaus Bilgisayarla (Kompüter) İşlenen Suçların Ceza Hukuku Yönünden İncelenmesi (Çev.: Feridun Yenisey), in: İÜHFM, C.:XLI, S.:1-2, İstanbul, 1975.

TOROSLU, Nevzat, Ceza Hukuku Özel Kısım, Ankara, 2007.

TUNCER, Murat/ **TAŞPINAR**, Mehmet, Sanal Eğitim – Öğretim ve Geleceği, in: Elektronik Sosyal Bilimler Dergisi, Cilt: 6 – Sayı: 20, 2007, sh: 119 (Kaynak: <http://www.e-sosder.com/dergi/20112-132.pdf>, Erişim Tarihi: 06.02.2008, Saat: 13:00).

TURHAN, Faruk, Yeni Türk Ceza Kanununda Uluslar arası Suçlar, <http://www.ceza-bb.adalet.gov.tr/makale/101.doc> (Erişim Tarihi: 22.09.2007).

TURAN, Mehmet, Düşünce Özgürlüğü ve 1982 Anayasası, Düşünce Özgürlüğü ve 1982 Anayasası”, in: DÜHFD, Sayı 4, Diyarbakır, 1990.

ÜLGEN, Halil İbrahim/ **SAĞIROĞLU**, Şeref/ **YÜNCÜ**, Selma, Güvenli Bir E- Posta Uygulaması: Gü- Posta, in: UEİS, Ankara, 2005.

ÜNVER, Yener, Avrupa Biyo- Hukuk Sözleşmesi'nin Türk Hukukuna Etkileri, in: KHUKA, Ekim, 2005.

ÜNVER, Yener, Ceza Hukukuyla Korunması Amaçlanan Hukuksal Değer (**ÜNVER**, Hukuksal Değer) , Ankara, 2003.

ÜNVER, Yener, Ceza Hukukunda İzin Verilen Risk, İstanbul, 1998.

ÜNVER, Yener, TCK ve CK Tasarısı'nın İnternet Açısından Değerlendirilmesi (**ÜNVER**, , in: İÜHFMD, Cilt: LIX, Sayı: 1-2, İstanbul, 2001,

ÜNVER, Yener, Uluslar arası Bir Ceza Hukuku Sempozyumundan Notlar, in KHUKA -7, 2000

ÜNVER, Yener, Yeni Türk Ceza Hukukunda Kusurluluk, in: CHD (Ed:Veli Özer ÖZBEK) Yıl:1, Sayı: 1, Ankara, 2006

ÜZÜLMEZ, İlhan, Cinsel Dokunulmazlığa Karşı Suçlar, <http://www.cezabb.adalet.gov.tr/makale/122.doc> (Erişim Tarihi: 10.12.2007, Saat: 16:44)

ÜZÜLMEZ, İlhan, Tehdit, Şantaj ve Cebir Kullanma Suçları, Ankara, 2007.

ÜZÜLMEZ, İlhan, Yazışmaların İhlali Cürümü ve Bu Bağlamda Elektronik Postalara (e-Postalara) Yönelik Saldırıların Durumu, in: AÜHFMD., C: 53, S:1, Ankara, 2004.

VASSILAKI, E. Irini, Materielles Strafrecht, Strafprozessrecht, Rechtsinformatik und Informations-gesellschaft, Freundesgabe Büllsbach, 2002, sh: 348 vd. (Kaynak: http://www.alfred-buellesbach.de/PDF/33_Vassilaki_Materielles.pdf, Erişim Tarihi: 14.10.2007, Saat: 18:50).

VEC, Milos, Internet, Internationalisierung und nationalstatlichen Rechtsgüterschutz, in: NJW, Heft: 21, 2002.

VON BUBNOFF, Eckhart, Krimineller Missbrauch der neuen Medien im Spiegel europäischer Gegensteuerung, in: Strafrecht und Kriminalität in Europa (Hrsg: Frank ZIESCHANG/ Eric HILGENDORF / Klaus LAUBENTHAL), IUS EUROPAEUM, Band 23, Baden – Baden, 2003

WENNING, Rigo, Das Internet – ein rechtsfreier Raum?, Kaynak: <http://www.jurpc.de/aufsatz/19970016.htm> (Erişim Tarihi: 07.02.2008, Saat: 09:27);

WESSELS, Johannes, Strafrecht Allgemeiner Teil, 28. Auflage, Münster, 1996.

WIELAND, Kornad, Meinungsfreiheit im Internet, sh: 15 v.d. Kaynak: http://www.law.tuwien.ac.at/bakk_arbeit_wieland.pdf (Erişim Tarihi: 10.01.2009, Saat:10:10).

YALÇIN, Cemal, Sosyolojik Bir Bakış Açısıyla İnternet (**YALÇIN**, Sosyolojik) , in: CÜSBED, Mayıs 2003, Cilt: 27, No:1,

YARSUVAT, Duygun, Yeni Türk Ceza Kanunu Genel Hükümleri, Genel Değerlendirme, İlkerler ve Genel Kurallar, in: YÜHFMD, C. II/ S 2, İstanbul, 2005

YAVUZ, Cevdet, Borçlar Hukuku Dersleri (Özel Hükümler), 4. Baskı, İstanbul, 2006.

YAZICIOĞLU, Yılmaz. Kriminolojik, Sosyolojik ve Hukuki Boyutları İle Bilgisayar Suçları, İstanbul (**YAZICIOĞLU**, Bilgisayar Suçları), Ankara, 1997.

YAZICIOĞLU, Yılmaz, Bilgisayar Marifetiyle İşlene Suçlar: Sanal Suçlar (**YAZICIOĞLU**, Bilgisayar Marifetiyle) , in: Panel – Bilişim Suçları(Adalet Bakanlığı Hakim ve Savcı Adayları Eğitim Merkezi Başkanlığı), Ankara, 2001.

YAZICIOĞLU, Yeni Türk Ceza Kanunundaki Bilişim Suçlarının Değerlendirmesi, YÜHFD, C. II/ S 2, İstanbul, 2005.

YENİDÜNYA/DEĞİRMENCİ. Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları, İstanbul, 2003.

YILDIZ, Ali Kemal, 5237 Sayılı Türk Ceza Kanunu, İstanbul Barosu Yayınları, İstanbul, 2007.

YILDIZ, Sevil, Suçta Araç Olarak İnternetin Teknik ve Hukuki Yönden İncelenmesi, Ankara, 2007.

YILMAZ/ERKEN, Uluslar arası Ceza Mahkemesi Hakkında, http://www.ucmk.org.tr/index.php?option=com_content&task=view&id=32&Itemid=49 (Erişim Tarihi: 22.09.2007);

ZEVKLİLER, Aydın, Borçlar Hukuku – Özel Borç İlişkileri, 7. Baskı, Ankara, 2002.

ZILLIOĞLU, Merih, İletişim Nedir?, 2. Baskı, İstanbul, 1999.

Düşünce Özgürlüğü – Avrupa İnsan Hakları Sözleşmesinin10. Maddesine İlişkin İçtihatlar, T.C. Başbakanlık Basım – Yayın ve Enformasyon Genel Müdürlüğü, http://www.byegm.gov.tr/YAYINLARIMIZ/kitaplar/avrupa/bolum_1.htm (Erişim Tarihi: 18.09.2007).

Ö Z G E Ç M İ Ş

Adı ve SOYADI : İlker TEPE

Doğum Tarihi ve Yeri : 10.03.1983 - Afşin

Medeni Durumu : Evli

Eğitim Durumu

Mezun Olduğu Lise :Karatay Lisesi (Yabancı Dil Ağırlıklı Bölüm)

Lisans Diploması : Akdeniz Üniversitesi Hukuk Fakültesi

Yükseklisans Diploması: Akdeniz Üniversitesi Sosyal Bilimler Enstitüsü

Tez Konusu : Modern Ceza Hukuku Anlayışında İnternet Suçluluğu ve Türk Ceza Hukukundaki Yansımaları

Yabancı Dil / Diller : Almanca, İngilizce

Bilimsel Faalivetler

- 1- 30.09.2007 – 01.10.2007 tarihlerinde Almanya’da Würzburg Üniversitesi’nde düzenlenen **“Das Strafrecht im deutsch- türkischem Rechtsvergleich”** adlı Sempozyum. Bu Sempozyumda *“Neuere Entwicklungen im türkischen Strafrecht am Beispiel des Internetstrafrechts”* başlıklı bir bildiri sunulmuştur.
- 2- 15 – 30 Ekim 2006 tarihleri arasında Almanya’da Friedrich Alexander (Erlangen) Üniversitesi Hukuk Fakültesi Ceza Hukuku ve Hukuk Felsefesi Kürsüsü Başkanı Prof. Dr. Hans KUDLICH ile birlikte gerçekleştirilen ve *“Bir Öldürme Saiki Olarak Kan Gütme”* konusunda Türk ve Alman Ceza Hukuku düzenleme ve uygulamalarını kapsayan Karşılaştırmalı Ceza Hukuku Araştırma Projesi. Bu projenin neticesi olarak *“Das Tötungsmotiv "Blutrache" im deutschen und im türkischen Strafrecht”* başlıklı bilimsel makale hazırlanmıştır.
- 3- 25.09.2008 – 29.09.2008 tarihleri arasında İstanbul’da İstanbul Barosu ve Hukuk Felsefesi ve Sosyolojisi Arkivi tarafından Gerçekleştirilen **“Hukuka Felsefi ve Sosyolojik Bakışlar -IV”** başlıklı Sempozyum. Bu Sempozyumda *“Ceza Hukuku Felsefesi Perspektifinden İnternetin Güncel Problemleri”* başlıklı bir bildiri sunulmuştur.
- 4- Yeditepe Üniversitesi Hukuk Fakültesi tarafından 13- 15.03.2009 tarihleri arasında İstanbul’da organize edilen **III. Türk – Alman Karşılaştırmalı Ceza Hukuku Sempozyumunda** *“ Türk Ceza Hukukunda Fiyatları Etkileme Suçu”* konulu bir tebliğ sunulmuştur.
- 5- 14.05.2009 tarihinde Würzburg Üniversitesi Hukuk Fakültesi tarafından yürütülen **“Globale Systeme und Interkulturelle Kompetenz ”** adlı proje kapsamında *“ Multikulturalismus und Blutrache”* konulu bir tebliğ sunulmuştur.

İş Deneyimi**Stajlar** : -**Projeler** : -**Çalıştığı Kurumlar** : 1) Akdeniz Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı (2006 – 2009).
2) Dokuz Eylül Üniversitesi Hukuk Fakültesi Ceza ve Ceza Usul Hukuku Anabilim Dalı (2009 - ...)**Adres** : Kozağaç Mah., 282/3 Sok., No:39/1, Buca - İZMİR**Tel. no** : 05444968794