T.C.
SAKARYA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ

AMERİKA BİRLEŞİK DEVLETLERİ HUKUKU, AVRUPA İNSAN HAKLARI MAHKEMESİ İÇTİHATLARI VE TÜRK HUKUKUNDA İLETİŞİMİN DENETLENMESİ

DOKTORA TEZİ

Mehmet Murat YARDIMCI

Enstitü Anabilim Dalı: Kamu Yönetimi

Tez Danışmanı: Doç. Dr. Ömer ANAYURT

MART- 2008

T.C.
SAKARYA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ

AMERİKA BİRLEŞİK DEVLETLERİ HUKUKU, AVRUPA İNSAN HAKLARI MAHKEMESİ İÇTİHATLARI VE TÜRK HUKUKUNDA İLETİŞİMİN DENETLENMESİ

YÜKSEK LİSANS TEZİ

Mehmet Murat YARDIMCI

Enstitü Ana Bilim Dalı: Kamu Yönetimi

Bu tez .../.../2008 tarihinde aşağıdaki jüri tarafından Oybirliği ile kabul edilmiştir.

_____	_____	_____
Jüri Başkanı	**Jüri Üyesi**	**Jüri Üyesi**
□ Kabul	□ Kabul	□ Kabul
□ Red	□ Red	□ Red
□ Düzeltme	□ Düzeltme	□ Düzeltme

İÇİNDEKİLER

KISALTMALAR

ABD :Amerika Birleşik Devletleri

AİHK :Avrupa İnsan Hakları Komisyonu

AİHM :Avrupa İnsan Hakları Mahkemesi

AİHS :Avrupa İnsan Hakları Sözleşmesi

Bk. :Bakınız

C. :Cilt

CALEA :Communications Assistance for Law Enforcement Act(İletişimin Denetlenmesinde Kolluk Kuvvetlerine Yardım Kanunu)

CD :Ceza Dairesi

CGK :Ceza Genel Kurulu

CIA :Central Intelligence Agency (Merkezi Haberalma Ajansı)

CMK :Ceza Muhakemesi Kanunu

CMUK :Ceza Muhakemeleri Usul Kanunu

CYY :Ceza Yargılaması Yasası

Dp. :Dipnot

ECPA :Electronic Communication Privacy Act (Elektronik İletişim Mahremiyet Kanunu)

EFF :Electronic Frontier Foundation (Elektronik Sınırlar Vakfı)

EPIC :Electronik Privacy Information Center (Elektronik Mahremiyet Bilgi Merkezi)

FISA :Foreign Intelligence Surveillence Act (Dış İstihbarat Güvenlik Kanunu)

FBI :Federal Bureau of Investigation (Federal Soruşturma Bürosu)

GÜHFD :Gazi Üniversitesi Hukuk Fakültesi Dergisi

İET :İnternet Erişim Tarihi

IP :İnternet Protocol(İnternet Protokol)

İÜHF :İstanbul Üniversitesi Hukuk Fakültesi

NSL :National Security Letters(Milli Güvenlik Mektupları)

NSA :National Security Agency(Milli Güvenlik Ajansı)

Pr. :Paragraf

RIPA :Regulation of Investigatory Powers Act(Soruşturma Yetkilerinin Düzenlenmesi Kanunu)

s. :Sayfa

S. :Sayı

TCK :Türk Ceza Kanunu

TİB :Telekomünikasyon İletişim Başkanlığı

U.S.C. :United States Code (Amerika Birleşik Devletleri Külliyatı)

Vd. :Ve devamı

Vb. :Ve benzeri

Vs. :Ve saire

SAÜ, Sosyal Bilimler Enstitüsü **Doktora Tez Özeti**

Tezin Başlığı: Amerika Birleşik Devletleri, Avrupa İnsan Hakları Mahkemesi İçtihatları ve Türk Hukukunda İletişimin Denetlenmesi

Tezin Yazarı: Mehmet Murat YARDIMCI **Danışman:** Doç. Dr. Ömer Anayurt

Kabul Tarihi: 26 Mart 2008 **Sayfa Sayısı:** IX (ön kısım) + 310(tez)

Anabilimdalı: Kamu Yönetimi

İletişimin denetlenmesi tedbiri, kolluk güçleri tarafından en etkin ve en geniş şekilde uygulanmak istenmektedir. Bu isteğin doğal bir sonucu olarak, iletişimin denetlenmesine ilişkin ülke uygulamalarında ciddi artışlar ortaya çıkmıştır. Ülkeler yeni tehdit türleriyle baş edebilmek bakımından bu tedbiri daha etkin olarak kullanabilmek için mevzuatlarını güncellemek zorunda kalmışlardır. Bu zorunluluğu gören kanun koyucumuz da, bu konu ile ilgili yeni bir mevzuat çalışması yapmıştır. Bu çalışma yapılırken, Avrupa İnsan Hakları Sözleşmesi ve Avrupa İnsan Hakları Mahkemesi (AİHM) içtihatlarından yararlanılmış olmakla birlikte, teknolojik gelişmeleri çok yakından izleyen Amerika Birleşik Devletleri'ndeki (ABD) güncel mevzuat ve uygulama hakkındaki bilgilere yeterince ulaşılmış olduğu söylenemez.

İletişimin denetlenmesi kavramını uluslararası bir bakış açısıyla ele almayı hedefleyen çalışmamızda; ABD hukuku, AİHM hukuku ve Türk hukuku incelenmiştir. Çalışma üç bölümden oluşmaktadır. ABD'nin iletişimin denetlenmesine ilişkin mevzuatı ve uygulaması hakkında bilgi verilen birinci bölümde, bu ülkenin, özellikle 11 Eylül olayları ile değişen tavrı çerçevesinde adli ve önleyici amaçlı iletişimin denetlenmesi irdelenmiştir. İkinci bölümde, iletişimin denetlenmesi ile ilgili olarak AİHM içtihatları incelenmiştir. Üçüncü bölümde ise, Türk Hukukunda adli amaçlı iletişimin denetlenmesi ve önleyici amaçlı iletişimin denetlenmesi kavramları mercek altına alınmıştır.

ABD'deki iletişimin denetlenmesi mevzuatı, ana hatlarıyla, iletişim içeriğinin denetlenmesine ilişkin hükümler ihtiva eden Teknik Dinleme Kanunu'nun yanısıra, Numara ve Rota Tespit Kanunu ve Dış Güvenlik İstihbarat Kanunu'nda yer almaktadır. İletişimin denetlenmesi sistemi çok geniş bir mevzuata dayandırılmasına rağmen, yer yer mevzuattan kaynaklanmayan yetkilere başvurulduğu, bazen de yasal yetkilerin sınırlarının olması gerekenden fazla genişletildiği gözlemlenmektedir.

1412 sayılı Ceza Muhakemeleri Usulu Kanunu döneminde kıyas ya da yorum marifetiyle uygulanan iletişimin denetlenmesi sistemimizin, yapılan mevzuat çalışmaları sonrasında, ana hatları itibariyle, AİHM standartlarına uyumlu hale getirildiği söylenebilir. Adli amaçlı iletişimin denetlenmesi alanındaki gelişmelerin oldukça tatminkar boyutlara ulaştığı, bununla birlikte önleme amaçlı iletişimin denetlenmesi uygulamasının birçok önemli eksiklikler ve boşluklar ihtiva ettiği görülmektedir. İletişimin denetlenmesi tedbirinin denetimindeki eksiklikler ile ilgili mevzuattaki boşluk ve muğlaklıklar gibi hususlar, AİHM'ye yapılabilecek muhtemel başvurular sonucunda Ülkemiz aleyhine yeni ihlal kararlarının verilmesine neden olabilecektir.

Anahtar kelimeler: İletişimin denetlenmesi, telefon dinlenmesi, Avrupa İnsan Hakları Mahkemesi, Amerika Birleşik Devletleri, Ceza Muhakemesi Kanunu

Sakarya University Institute of Social Sciences Abstract of PhD Thesis

Title of the Thesis: 'Interception of Communication in the Jurisdictions of the United States of America, European Court of Human Rights and Turkey'

Author: Mehmet Murat YARDIMCI **Supervisor:** Assoc. Prof. Ömer Anayurt

Date: 26 March 2008 **Nu. of Pages :** IX (pre text)+ 310 (Thesis)

Department: Public Administration

Interception of communication tool has been desired to be utilised by the law enforcement units in the most effective and broad manner. As a natural outcome of this desire, dramatic increases have been seen in the implementation phase. So as to combat these brand new threats, states have been obliged to update their related legislation pieces in order to more efficently use this tool. Turkish legislator, being aware of this obligation, has undertaken a new legislative study. In the course of these legislative steps, 'European Convention for the Protection of Human Rigths and Fundamental Freedoms' and the decisions of the European Court of Human Rights (ECHR) have been taken into consideration. Nevertheless, it cannot be said that the updated documents and information as to the legislation pieces and implementation of the United States of America (USA), which closly follows technological develepments, have been benefited.

Our study, which aims to examine the interception of communication notion through an international standpoint, has scrutinized the USA, ECHR and Turkish jurisdictions respectively. The study consists of three chapters. The first chapter, sheding light on the USA legislation and implementation with regard to interception of communication, examines the judicial and preventive interception in the context of the USA attitude which changed particularly after the 9/11 era. In the second chapter, the jurisdiction of ECHR has been examined. In the last chapter, both judicial and preventive interception of communication notions in Turkish law are focused on.

The legislation pieces with regard to interception of communication consists mainly of the 'Wiretap and Electronic Surveillence Act', which covers the provisions as to the content of the communication, along with the Pen/Trap Statute and the Foreign Intelligence Surveillence Act. Even though the USA implementation as to the interception of communication system is based upon a broad legislation piece, it has been observed that some of the authorities do not take their roots from the related legislation or some powers of the law enforcement agengies have been unduly broadened.

The interception of communication system of Turkey, which used to apply deductive reasoning or interpretation tools at the time of the ancient Criminal Procedure Law numbered 1412, has, to an important extent, been aligned with the standards of the ECHR. The developments in the field of 'judicial interception' have reached to a rather satisfactory level, however, the practice with respect to the 'preventive interception of communication' lacks some important elements and accomodates some lacunas. The loopholes and the ambiguities in the legislation regarding the interception of communication along with the deficiencies concerning the control mechanism over the interception transactions may give rise to violations in case they are brought before the ECHR.

Keywords: Interception of communication, telephone tapping, European Court of Human Rights, United States of America, Criminal Procedure Law

GİRİŞ

İnsanlar, tabiatları itibariyle, sadece kendilerine mahsus ve dış dünyaya kapalı bir alana sahip olmayı değerli kabul etmekte, bu hususa saygı duyulmasını ve bu özel alana yönelik muhtemel tecavüzlerin önlenmesini temin etmek amacıyla gerekli tüm tedbirlerin alınmasını talep etmektedirler. Bu talep doğrultusunda birçok önemli adım atılmış ve özel hayatın korunmasını sağlamaya yönelik ulusal ve uluslararası[1] nitelikte birçok düzeyde birçok hukuksal metin kaleme alınmıştır.

Günümüz dünyasında, suçla mücadelede büyük önem taşıdığı muhakkak olan iletişimin denetlenmesi tedbiri, kolluk güçleri tarafından en etkin ve en geniş şekilde uygulanmak istenmektedir. Kolluğun bu isteğini haklı çıkaran sayısız olay gündelik hayatımızda karşımıza çıkmakta, alınacak tedbirlerle önlenmesi mümkün olan bu olayların vuku bulması toplumda rahatsızlıklara neden olmaktadır. Bununla birlikte, 'başkaları' için mutlaka kullanılması istenen bu yöntemler, 'başkalarının' alanından çıkıp kişinin kendi 'özel'ine girdiği ve aslında herkesin bu 'iki tarafı keskin bıçağın' tehdidine maruz kaldığı fark edildiğinde, suçla mücadele ile özel hayatın korunması arasında bir denge kurulması gereği daha yüksek sesle ifade edilmektedir.

19. yüzyılın sonlarına doğru icat edilen telefon, en baştan beri kolluk kuvvetleri için bir ilgi odağı olmuş, insanların 'özel'ine tanıklık eden bu cihazın dinlenmesi için yeni yollar ve yöntemler bulunmaya çalışılmıştır. 20. yüzyılın son çeyreğinde, iletişimin denetlenmesine ilişkin ülke uygulamalarında ciddi artışlar ortaya çıkmıştır. Ülkeler hem yeni tehdit türleriyle baş edebilmek, hem de gelişen teknolojinin getirdiği yenilikler karşısında eskidiği anlaşılan mevzuatlarını güncellemek zorunda kalmışlardır. Bu zorunluluğu gören kanun koyucumuz da, iletişimin denetlenmesi ile ilgili yepyeni bir

---

[1] Birleşmiş Milletler Siyasi ve Medeni Haklar Sözleşmesi'nin "Özel Hayat Hakkı" başlıklı 17. maddesinde "Hiç kimsenin özel ve aile yaşamına, konutuna veya haberleşmesine keyfi veya hukuka aykırı olarak müdahale edilemez; onuru veya itibarı hukuka aykırı saldırılara maruz bırakılamaz. Herkes bu tür saldırılara veya müdahalelere karşı hukuk tarafından korunma hakkına sahiptir." hükmü yer almaktadır. (International Covenant on Civil and Political Rights) http://www.unhchr.ch/html/menu3/b/a_ccpr.htm (İET:4.12.2007) Tüm Göçmen İşçilerin ve Aile Fertlerinin Haklarının Korunmasına Dair Uluslararası Sözleşme'nin 14. maddesi benzer hükmü havidir. Anılan maddede, "Hiçbir göçmen işçinin veya aile ferdinin özel hayatına, ailesine, konutuna, mektuplaşmasına veya diğer şekilde haberleşmesine keyfî ve gayrî kanunî müdahalelerde bulunulamaz; şeref ve haysiyetlerine gayrî kanunî saldırılar yapılamaz. Her bir göçmen işçi ve aile ferdî bu tür saldırılara ve müdahalelere karşı kanunun öngördüğü korumadan yararlanma hakkına sahip olacaktır" denilmektedir. http://www.unhchr. ch/html/ menu3/ b/m_mwc_p3. htm (İET:4.12.2007) Birleşmiş Milletler Çocukların Korunması Sözleşmesinin 40. maddesinin 2/7 başlıklı fıkrasıyla, taraf devletlerin, kovuşturmanın her aşamasında özel hayatın gizliliğine tam saygı gösterilmesini garanti altına aldıkları belirtilmiştir.(Convention on the Rights of the Child) http://www.unhchr.ch/html/menu3/b/k2crc.htm (İET:4.12.2007).

mevzuat ortaya koymuştur. Bu mevzuat çalışması yapılırken, hukukumuzu en çok etkileyen Avrupa'dan esinlenilmiş, Avrupa İnsan Hakları Sözleşmesi (AİHS) ve Avrupa İnsan Hakları Mahkemesi (AİHM) içtihatları da bir deniz feneri vazifesini üstlenmiştir.

Çalışmanın Amacı

İletişimin denetlenmesi kavramını bu boyutu itibariyle incelemeyi hedefleyen çalışmamızda, Amerika Birleşik Devletleri (ABD) hukuku, AİHM hukuku ve Türk hukuku incelenmiştir. Her ne kadar, ABD hukukunun iletişimin denetlenmesi alanında mevzuatımıza Kıta Avrupası hukuku düzeyinde bir yansıması sözkonusu değilse de, yeni dünyadakilerin bu konuya bakışını anlamak ve teknolojik gelişmeleri çok yakından izleyen bu ülkedeki güncel mevzuat ve uygulamayı araştırmak hedeflenmiştir. ABD'nin iletişim teknolojisindeki yeri dikkate alındığında, iletişimin denetlenmesi alanındaki en orijinal yaklaşımların bu ülkeden çıkabileceğine ilişkin bir düşünce, bu çalışmanın teşvik edici unsurları arasında yer almıştır. Çalışmamızda, yer yer atıflar yapılmış olsa da, Avrupa ülkelerinin mevzuat ve uygulamalarına fazlaca girilmemiştir. Bunun en önemli sebebi de, bu ülke uygulamalarının AİHM süzgecinden geçiriliyor olmalarıdır. Bu üç sistemin incelenmesi, ortak ve farklı noktalarının bulunması ile hukukumuza ithal edilebilecek birtakım kurumların keşfedilmesi bakımından önemlidir.

Çalışmanın Önemi

İletişimin denetlenmesi, gerek Ülkemizde gerekse mukayeseli hukukta çok iyi bilinmeyen bir kavramdır. Bu konudaki bilgi eksikliği, bu kavramın son zamanlarda ortaya çıkmasıyla ilgili olduğu gibi, her geçen gün iletişim teknolojisindeki gelişmelerin ortaya koyduğu yeniliklerle de ilgilidir. Gerçekten de, haberleşme kavramının bu çağdaş formu, her geçen gün yeni bir yüzüyle karşımıza çıkmaktadır. Bu konuda en eski hukuksal düzenlemelere ve mahkeme kararlarına sahip olan ABD'de bile bu kavram tam olarak tabii mecrasını bulabilmiş değildir. Çalışmamızda ayrıntılı bir şekilde anlatılacağı üzere, iletişim hürriyetinin özel hayat alanı kapsamında kabul edilmesi için çok uzun bir zamanın geçmesi gerekmiştir. Hukukumuzda, iletişimin denetlenmesi alanında yapılan kanunların birkaç yıllık mazisinin olması da bu durumu izah etmektedir.

Bu yeni kavram, birçok şeyin tecrübe edilerek öğrenilmesi ve yapılan yanlışların tekrar edilmemesi suretiyle doğru yolun bulunması çabasını beraberinde getirmiştir. Daha birkaç yıl öncesine kadar, Ceza Muhakemeleri Usulu Kanunu'ndaki (CMUK), konuyla ilgili olmayan birkaç madde hükmünün kıyasla genişletilmesi ya da geniş yorumlanması

yoluyla başvurulan iletişimin denetlenmesi, bugün daha sistematik bir şekilde uygulanmaya çalışılmaktadır. Bu konudaki tecrübesizlikten kurtulmanın iki yolu olabilir. Bunlardan ilki, zamanın geçmesini beklemek ve hayatın akışı içinde edinilen tecrübelerden doğruları bulmaktır. Bir tür deneme-yanılma metodu olarak da isimlendirebileceğimiz bu yol hem pahalı, hem yorucu hem de risklidir. Doğru yol ve yöntem bulununcaya kadar harcanan para ve emek bu sürecin doğal sonuçları olarak görülebilir ve tolere edilebilir. Ancak hakları çiğnenen, özel hayatları ihlal edilen kişilerin zararlarını maddi ve manevi olarak tazmin etmek mümkün olmayabilir. İkinci yol ise, hem daha az riskli ve hem de para ve emek bakımından daha ekonomik bir yaklaşımı içerir. Bu da, benzer tecrübeleri daha önceden yaşamış ülke tecrübelerini inceleyip onların yaptığı hataları yapmamaktır. ABD ve AİHM hukuklarındaki anlayışı ve bakış açısını anlamayı ve Ülkemiz bakımından yorumlamayı hedefleyen çalışmamızın, bu bakımdan çok önemli olduğunu düşünüyoruz.

Çalışmanın Yöntemi

Çalışma üç bölümden oluşmaktadır. Birinci bölüm, ABD'nin iletişimin denetlenmesine ilişkin mevzuatı ve uygulaması hakkında bilgi vermeyi amaçlamaktadır. Yakın tarihlere kadar hürriyetlerin beşiği olarak tanınan ve en kabul edilemez düşüncelere bile kucak açan bir ülkenin, özellikle 11 Eylül olayları ile değişen tavrı ve suçla mücadele adına yaptığı düzenlemelerin anlatıldığı bu bölümde, adli ve önleyici amaçlı iletişimin denetlenmesi, bu konu hakkında yazılmış Türkçe eserlerin bulunmaması nedeniyle, bizzat birinci elden kaynaklara inilerek irdelenmiştir. Cornell Hukuk Fakültesi'nin (Cornell University Law School), günlük olarak yenilenen güncel mevzuat sitesi vasıtasıyla, ilgili mevzuat elde edilmiş, konu gerek ABD'de daha yaygın olan hukuk dergilerinden (law journal), gerek Amerikan Adalet Bakanlığı ve FBI gibi resmi kurumların internet sitelerinden, gerekse gayrıresmi söylemi ifade eden Electronic Privacy Information Center (EPIC), Electronic Frontier Foundation (EFF) gibi sivil toplum kuruluşlarının iletişimin denetlenmesi ile ilgili İnternet sitelerinden yararlanılmıştır. 51 başlık[2] halindeki ABD kanun külliyatına ilişkin bilgileri, yine bu İnternet sayfasından ulaşılabilen 'listing on the House server' isimli adres vasıtasıyla teyit etmek mümkündür. Bahse konu Üniversitenin mevzuata ilişkin sayfasında, 'İçerik ve Bağlam' (Contents and Context) başlığı altında, mevzuatın temin ve sunum tarzı ile

[2] Bu 51 başlığa http://www.law.cornell.edu/uscode/ adresi marifetiyle ulaşılabilmektedir.

güncelleştirilmesine ilişkin bilgiler mevcuttur[3]. Çalışmamızda, münferit konularda değişik başlıklara gidilmiş ise de, daha çok 18 nolu 'Crimes and Criminal Procedure' (Suç ve Cezai Usul) başlığı ile 50 nolu War and National Defense (Savaş ve Milli Savunma) başlıkları altındaki kanunlardan yararlanılmıştır. Diğer bir ifade ile, Teknik Dinleme Kanunu, Numara ve Rota Tespit Kanunu ve Dış Güvenlik İstihbarat Kanunu bu iki başlık altında düzenlendiğinden bu iki başlık en çok başvurulan bölümler olmuştur.

İkinci bölümde, iletişimin denetlenmesi ile ilgili olarak, AİHS ve AİHM içtihatları incelenmiştir. AİHM'nin konuya ilişkin yaklaşımı, özellikle yabancı kaynaklardan yararlanılarak anlatılmıştır. AİHM kararları çalışmamızda önemli bir yer tuttuğundan, Strasbourg Mahkemesi kararları bizzat incelenmek suretiyle aracısız bilgi elde edilmeye çalışılmıştır. Kararlara, AİHM'nin resmi İnternet sitesi HUDOC (http://cmiskp.echr.coe.int) vasıtasıyla ulaşılmıştır. Mahkeme kararlarına atıf yapılırken; ismi, tarihi, başvuru numarası yazılmak suretiyle kararın künyesi yazılmıştır. Mahkeme kararlarından bahsedilirken kararın adından hemen sonra ülke ismi verilmesi yöntemi (Örneğin, Leander-İsveç) tercih edilmiştir.

Üçüncü bölümde ise, Türk Hukukunda iletişimin denetlenmesi ana hatlarıyla ele alınmıştır. Konunun tarihçesi hakkında genel bir bilgi verildikten sonra, adli amaçlı iletişimin denetlenmesi ve önleyici amaçlı iletişimin denetlenmesi kavramları tartışılmıştır. Hukukumuza yeni giren bir kavram olan iletişimin denetlenmesinin AİHM içtihatlarına uygun olup olmadığı ilgili yerlerde incelenmiş, spesifik bir kurum ya da uygulamanın ABD hukukuyla karşılaştırması yapılmış, ülkemizde olmayan ya da olsa bile farklılık arz eden kurumların Ülkemizde de ihdas edilmesine ilişkin öneriler getirilmiştir. Bununla birlikte, öneri ve değerlendirmeye ilişkin nihai ifadeler sonuç bölümüne havale edilmiştir.

Her ne kadar, terim birliği bakımından 'iletişimin denetlenmesi' kavramı kullanılmışsa da, karşılaştırmalı hukukta konular açıklanırken, terim bütünlüğünü sağlamak bakımından ve bazen de o ülkede uygulanan bir sistemi daha iyi ifade etmek amacıyla iletişime müdahale, iletişimin engellenmesi, ayrıca alt başlıklarda da iletişimin dinlenmesi, teknik takip, telefon dinlenmesi, teknik dinleme kavramları da kullanılmıştır.

[3] Sitede mevzuatı bulmaya ilişkin yöntem anlatılmaktadır. Kongre ile doğrudan irtibat halinde olan bu site tüm güncellemeleri 24 saat içinde kamuoyuna sunmaktadır. Bk. http://www.law.cornell.edu/uscode/ .

Konu sınırlaması yapılırken; teknolojik gelişmelerin hızı ve ‘iletişim’ kavramının genişliği dikkate alınarak, çalışma daha çok ‘telefon iletişimi’ne odaklanmıştır. Nitekim, İnternet, telefona göre daha geniş ve yeni terimler içeren bir alan olduğundan, bu konuda yeterli teknik bilgiye sahip olmadan yapılacak çalışmanın birtakım problemler ve yanlış anlamaları da beraberinde getirmesi kaçınılmaz olurdu. Öte yandan, çalışmamız esas itibariyle iletişimin denetlenmesine ilişkin hukuksal düzenleme ve uygulamaları incelemek olduğundan, yabancısı olduğumuz teknik boyuta girilmekten özellikle kaçınılmıştir.

Hukukilik boyutunun yanı sıra siyaseti de yakından ilgilendiren bir konu olan iletişimin denetlenmesi hakkındaki bu çalışmamızda, hukuk ve siyasetin birbirleriyle içiçe geçtiği yerlerde, meselenin hukuksal boyutunu ayıklamak oldukça güç bir iş olarak karşımıza çıktığından, konunun iyi bir şekilde anlatılması bakımından yer yer hukuk dışı noktalara da temas edilmiştir.

BÖLÜM 1. AMERİKA BİRLEŞİK DEVLETLERİ'NDE İLETİŞİMİN DENETLENMESİ

1.1. ABD Hukukunda İletişimin Denetlenmesinin Tarihsel Gelişimi

Teknolojik alanda olağanüstü değişikliklerin meydana geldiği ve dijital çağ olarak da adlandırılan günümüzde, bireylerin gerek devlet, gerekse özel sektör alanından gelebilecek müdahalelere karşı kendilerinin sayılabilecek bir alan oluşturup oluşturamayacakları, merak edilen bir husus haline gelmiştir. Gerçekten de, enformasyon teknolojisi, bilgi toplamayı olağanüstü bir şekilde artırmış ve kişisel bilgilerin akışını görülmemiş bir oranda kolaylaştırmıştır[4].

Özel hayat kavramı, Hakim Brandeis ve Warren tarafından 'yalnız bırakılma hakkı' olarak tanımlandığı 1898 yılından bu yana ciddi değişimlere uğramıştır. Bu kararı takip eden zaman diliminde, bilgi teknolojisinin artışı ile birlikte, özel hayatla ilgili olarak ortaya çıkan yeni kavramlar ve tanımlar, bu kavram üzerinde daha geniş bir kanun çalışması yapılması gereğini ortaya koymuştur[5]. Nitekim, özel hayat kavramını 'yalnız bırakılma hakkı' olarak tanımlamak, bilginin saniyeler içinde dünya yolculuğu yaptığı günümüzde yeterli olmamaktadır.

İletişimin denetlenmesi tedbirinin tarihsel gelişim sürecinin anlaşılabilmesi bakımından, tarihsel süreç içindeki önemli yargı kararları ve konu ile ilgili kanun çalışmalarının incelenmesi gerekmektedir. Bu bağlamda, ABD hukukunda, 1967 tarihli Berger ve Katz kararları bir dönüm noktası olarak algılandığı için, bu kararların öncesindeki durum anlatılmış, sonrasında da, ABD'nin iletişimin denetlenmesi ile ilgili mevzuatı açıklanmıştır.

---

[4] BERMAN, Jerry/BRUENING, Paula, ,"Is privacy still possible in the twenty first century?", Center for Democracy and Tecnology, 6 November 2006, http,//www.cdt.org/publications/privacystill.shtml (İET: 12. 11.2007)

[5] WARREN, D.Samuel/BRANDEİS, Louis D., "The right to privacy", Harvard Law Review, Vol.IV December 15, 1890 No.5, www.lawrence.edu/fast/boardmaw/ Privacy_brand_ warr2.html (İET: 15.5.2006)

1.1.1.1967 Öncesi Durum

İletişimin devlet tarafından denetlenmesi ABD'de uzun tarihsel arka planı olan bir meseledir. Kanun uygulayıcıları, 1844 yılından bu yana telle dinleme (wiretapping), 1890 yılından bu yana da telefon dinlemesi yapmaktadırlar[6].

Kanun dışı dinlemeyi yasaklayan eyalet kanunlarının tarihi ise 1862 yılına dek uzanmaktadır. Bununla birlikte, federal kanunlar konu hakkında uzun bir süre sessiz kalmıştır. 1928 yılında, ABD Yüksek Mahkemesi Olmstead[7] kararında federal ajanlarca wiretapping yöntemiyle iletişimin denetlenmesinin ABD Anayasası'nın 4. maddesi (Fourth Amendment)[8] anlamında bir arama veya elkoyma anlamına gelmediğine karar vermiştir[9]. Mahkeme böylece; insanların bedenlerini, mallarını, belgelerini, elkoyma ve arama kararlarına karşı koruma altına almış, soyut nitelikte olan telefon konuşmaları için aynı korumayı öngörmemiştir[10].

Olmstead kararının hatırlanmasını sağlayan en önemli yönü, Hakim Brandeis ve Holmes tarafından yazılan karşı oy yazılarındaki görüşlerdir. Bahse konu hakimlerin, Anayasa'nın 4. maddesi kapsamında fiziksel arama ve elkoyma ile ilgili hükümlerin

---

[6] WONG, Thomas:"Regulation Of Interception Of Communications In Selected Jurisdictions", Research and Library Services Division Legislative Council Secretariat, 3.1.1., http://www.legco.gov.hk/yr04-05/english/sec/library/0405rp02e.pdf,(İET:7.8.2007).

[7] Washington'daki federal ajanlarca 'Milli İçki Yasağı Kanunu'nu ihlal ettiği iddiasıyla ve de telefonları dinlenerek elde edilen deliller sonucunda tutuklanan Olmstead, ABD Yüksek Mahkemesi tarafından 4'e karşı 5 oyla mahkum edilmiştir. Mahkeme'nin aldığı bu kararla, telefon görüşmelerinin Anayasa'nın 4. maddesi korumasına dahil olmadığı tespiti yapılmıştır. OLMSTEAD-ABD, 277 U.S. 438 (1928), http://supreme.justia.com/us/277/438/index.html, (İET:10.11.2007).

[8] The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized. http://www.lectlaw.com/def/f081.htm) (İET:8.8.2007).

[9]ÖZDOĞAN, Ali: Teknik Dinlemeye Dair, "Gizli Dinleme Kanunlarına ve Uygulamalarına Dair Bir Araştırma", Emniyet Genel Müdürlüğü İDB yayınları No. 92, Ankara 2004,(2004), s.7;WONG, 3.1.2; DONOHUE, Laura K.: "Criminal law: Anglo-American Privacy and Surveillance", Northwestern School of Law, Journal of Criminal Law & Criminology, 2006, 96 j. Crim. L. & criminology 1059, Online, Lexis-Nexis, (İET: 1.11.2007), s.3; AN OVERVIEW OF ELECTRONİC SURVEILLANCE: History and Current Status, D.2. http//swiss.csail.mit.edu/6805/articles/crypto/nrc-report/nrc0d.txt, Cryptography's Role in Securing the Information Society, Prepublication, May 30, 1996, Appendices. (İET:15.10.2007); U.S. CONSTITUTION: FOURTH AMENDMENT, ELECTRONIC SURVEILLANCE AND THE FOURTH AMENDMENT,http://supreme.lp.findlaw.com/constitution/amendment04/05.html#1 (İET:7.8.2007); KHAN, Zmarak: "The National Security Agency(NSA) Eavesdropping on Americans, A Programme that is Neither legal Nor Necessary",Utrecht Law Review, Volume 2, Issue 2(December)- 2006 http://www. Utrecht lawreview.org/ , s.63.

[10] WONG, 3.1.2; ÖZDOĞAN, (2004), s.7.

iletişimin denetlenmesi bakımından uygulanamayacağına ilişkin görüşleri, iletişimin denetlenmesi hususunda önemli bir altyapı oluşturmuştur[11].

Mahkeme, Olmstead kararıyla iletişimin denetlenmesiyle ilgili olarak Kongre'ye bazı tavsiyelerde bulunmuştur. Bu bağlamda, özel hayat hakkı ve iletişimin denetlenmesi yoluyla elde edilen delillerin mahkemede kullanılması hususlarında düzenleme yapılması tavsiye edilmiştir. Olmstead kararı, Katz kararına kadar iletişimin denetlenmesinin hukuksal temelinin belirlenmesinde önemli bir rol oynamıştır[12]. Kongre de, 1934'te Federal Haberleşme Kanunu'nun 605. maddesini çıkararak, Mahkeme'nin tavsiyesi hakkında kısmen de olsa adım atmıştır. Bu madde sadece iletişimin denetlenmesi ile elde edilen delillerin zanlı aleyhinde kullanılmasını düzenlememiş, bunun yanı sıra, eyaletler arası telefon görüşmelerine ait dinleme kayıt ve bantlarının üçüncü kişilere verilmesini yasaklayan bir hüküm getirmiştir[13].

Yüksek Mahkeme 605. madde'yi, teknik dinleme ile elde edilen delillerin her ne şekilde olursa olsun mahkemelerde delil olarak kullanılmasının yasak olduğu şeklinde yorumlayarak, bu konuya yeni bir perspektif getirmiş, bu bağlamda, 1939 tarihli Weiss-

---

[11] Hakim Brandeis bu karardaki karşıoy yazısında, bugün bile hala atıfta bulunulan meşhur satırlara yer vermiştir. Brandeis, yalnız bırakılma hakkı (the right to be let alone) olarak nitelediği mahremiyet (özel hayat) hakkını medeni insanlar tarafından en değerli bulunan, en kapsamlı hak olarak nitelemiştir. Bu hakkın korunması bakımından, hükümet tarafından yapılan her gayrimeşru müdahale, kullanılan araç ne olursa olsun, Amerikan Anayasasının 4. maddesinin (Fourth Amendment) bir ihlali olarak değerlendirilmelidir. Keza, böyle bir müdahale ile elde edilen her türlü bilgi ve belge de bu maddenin ihlali anlamına gelmelidir. Bk. OLMSTEAD-ABD., 277 U.S. 438 (1928), http://supreme. justia. com/ us/ 277/ 438/index.html,(İET:10. 11. 2007); Bu kararda karşıoy yazanlardan biri de Hakim Rudkin idi. Hakim Rudkin ikna edici bir dille, verilen kararın yanlışlığını ifade etmiştir. Ona göre, bir mektup vasıtasıyla gönderilen mesajla bir telefon veya telefon marifetiyle iletilen mesaj arasında bir fark yoktur. Bunlardan ilkinin görünür(visible), somut(tangible) ve kapalı(sealed) olduğu, ikincisinin ise bu özellikleri taşımadığı doğrudur. Ancak, başkasıyla telefon görüşmesi yapan kişi bunu dış dünyaya yaymamaktadır. Bu mesajı ileten vasıtanın izin verdiği ölçüde içerik gizlidir ve hiçbir federal görevlinin mesajı kablolardan alıp, kişi aleyhine kullanma hakkı yoktur. Böyle durum, en basit ifadesiyle üzücü ve tolere edilemeyecek bir davranışın ifadesidir. ADMISSIBILITY OF EVIDENCE OBTAINED BY TAPPING TELEPHONE WIRES*,* New York Law Review, Volume VI, Mart 1928, Sayı 3, sayfa 81, Hein Online—6 N.Y.L. Review 80, 1928, (İET: 13.10.2007).

[12]OLMSTEAD-ABD, 277 U.S. 438 (1928).

[13]Kanunla ilk defa göndericinin (sender) rızası olmadan iletişimin denetlenmesi ve açıklanması (divulgence) yasaklanmıştır. Bu kanunun getirdiği diğer bir önemli reform ise; iletişimin denetlenmesi yoluyla elde edilmiş materyallerin geçerli delil olarak kullanılmasının sınırlandırılması olmuştur. Bununla birlikte, kanunun çıkarılmasını takip eden 30 yıl içinde, federal görevlilerin getirilen bu hükmü hiçe sayarak hareket ettikleri ve iletişimi keyfi olarak dinledikleri bilinen bir vakıadır. Bu durum özellikle, milli güvenlik aleyhindeki suçlara karıştığı iddia edilen yabancı ajanlar hakkında geçerli olmuştur. Federal yetkililer Başkanın milli güvenliği korumaya ilişkin anayasal yetkisi gölgesinde mahkeme kararı olmaksızın iletişime müdahale etmeye devam etmişlerdir. Bu yasadışı müdahaleler, eyaletlerin kanunları izin verdiği müddetçe hayata geçirilebiliyordu. Bu çerçevedeki faaliyetler daha sonra 1978 tarihinde FISA hükümleri uyarınca düzenlendi. (AN OVERVIEW OF ELECTRONIC SURVEILLANCE: History and Current Status, D.2.).

ABD kararında eyalet içi telefon görüşmelerinin dinlenilmesi ve dinlemeden elde edilen delillerin mahkemede kullanılması yasaklanmıştır[14].

1942 tarihli Goldman kararı, açılımların devam ettiği yeni bir halka olmuş, 'telefon görüşmesi yapan kişinin, evinin sınırları dışına gönderdiği seslerin başkaları tarafından dinlenmesi riskini taşıdığını bilmesi gerekir' şeklinde yeni bir görüş ortaya konulmuştur[15]. Devletin özel hayata müdahalesinin meşru olduğu görüşünün temelini hazırlayan düşüncelerden biri olan bu karara göre; duvar arkasından kişinin ikametini dinlemek, fiziki bir girişi tazammum etmediği için[16], Anayasa'nın 4. maddesini ihlali sayılmamaktadır[17].

Daha sonraki 1961 tarihli Silverman davasında ise mahkeme, merkezi kalorifer sistemi kullanılarak yerleştirilen verici ile dinlenilen konuşmaların haneye fiziki müdahale anlamına geldiğine ve Anayasa'nın 4. maddesinin ihlal edildiğine karar vermiştir[18].

Bazen özel hayatın kısıtlanması, bazen de genişletilmesi düşüncesine hizmet eden bu süreç esnasında genelde hakim olan kanaat, Anayasa'nın 4. maddesinin; kişinin sadece bedenine, hanesine ve evraklarına yöneltilmiş fiziki müdahalelere taalluk ettiği, bunlara karşı koruma sağladığı şeklindedir. 1967 yılına kadar süren bu dönemde verilen mahkeme kararları ile, Federal Haberleşme Kanunu müteaddit defalar delinmiş, iletişime müdahaleler eyalet Başsavcılarının inisiyatifleri ile yapılmıştır[19].

1.1.2.1967 Tarihli Berger ve Katz Davalarıyla Başlayan Süreç

1928 tarihli Olmstead kararı, iletişimin denetlenmesi hususunda yarım asra yakın bir süre Amerikan hukuk sistemini etkisi altına almıştır. 1967 tarihli Berger ve Katz kararları bu bağlamda bir dönüm noktası olmuş ve Yüksek Mahkeme, Anayasa'nın 4. maddesinin özel hayat kavramına bakışına yeni bir yorum getirmiştir. Bu dönemde yürürlükte olan Federal Haberleşme Kanunu gibi kanunlar, kolluk kuvvetleri tarafından

---

[14] WEİSS-ABD, (http://supreme.justia.com/us/308/321/ (İET:9.8.2007).

[15] GOLDMAN-ABD, 316 u.s.129 1942, http://supreme.justia.com/us/316/129/case.html , (İET:9.8.2007)

[16] STEVENS, Gina ve Doyle, Charles, "Privacy: An Overview of Federal Statutes Governing Wiretapping and Electronic Eavesdropping", CRS Report for Congress, Order Code 98-326., s. 4; AN OVERVIEW OF ELECTRONIC SURVEILLANCE: History and Current Status, D.2.

[17] GOLDMAN-ABD, 316 u.s.129 1942, http://supreme.justia.com/us/316/129/case.html , (İET:9.8.2007).

[18] SİLVERMAN-ABD, 365 u.s. 505 (1961), http://supreme.justia.com/us/365/505/ (İET:9.8.2007).

[19] ÖZDOĞAN, (2004), s.7; http://www.lectlaw.com/def/f081.htm (İET:8.8.2007).

uygulanmayan ancak bireylerin başvurduğu müdahelelere ilişkin hükümler içermekteydiler[20].

1967 tarihinde verilen Berger[21] kararında Mahkeme, gelişigüzel yapılan iletişimin denetlenmesini eleştirerek kabul edilemez bulmuş, Osborn[22] kararına da atıf yaparak bu tür uygulamaların Anayasa'nın 4. ve 5. maddeleri ile tanınan hakların ağır bir ihlali anlamına geldiğini vurgulamıştır[23]. Mahkeme, uzun ve sürekli olarak devam eden (bir günde 24 saat) bu tedbirle, iletişim kapsamına bir şekilde giren herkesin rastgele ve takibat konusu suçla olan ilgisine bakılmaksızın dinlenebilmesini eleştirmiştir[24]. Mahkeme, Berger kararında makul sebep ilkesiyle ilgili önemli bir tespit yapmıştır. Mahkemeye göre, Anayasa'nın 4. maddesinde belirlenen makul sebep ilkesi muhik neden olmadıkça Anayasa ile muhafaza altına alınan alandan devletin el çekmesini öngörmektedir[25].

New York Eyaleti Alkollü İçecekler Kurumu (The New York State Liquor Authority) Başkanına rüşvet verdiği iddiasıyla hakkında takibat başlatılan Berger hakkında Eyalet Yüksek Mahkemesi hakiminin, New York Eyaleti Ceza Usul Kanunu'nun 813. maddesi uyarınca verdiği izin çerçevesinde yerleştirilen cihaz vasıtasıyla 60 günlük bir süre için dinleme yapılmış, bu dinlemeden elde edilen delillerle de ikinci bir dinleme cihazı yerleştirilmesi yapılmış, iki haftalık dinleme sonrasında likör lisanslarının çıkarılması ile ilgili bir şebeke ortaya çıkarılmıştır. Telefonlarının dinlenmesinin özel hayatının masuniyetini ihlal ettiğini iddia eden Berger hakkındaki davada, Yüksek Mahkeme, önceki kararlarından farklı bir yaklaşımı benimsemiş, konuşmaların Anayasa'nın 4.maddesi kapsamında olduğuna ve bu nedenle de teknik imkanlarla elde edilen

---

[20] AN OVERVIEW OF ELECTRONIC SURVEILLANCE: History and Current Status, D.2.

[21] BERGER-NEW YORK, 388 u.s. 41 (1967)http://supreme.justia.com/us/388/41/case.html (İET:9.8.2007).

[22] OSBORN-ABD, 385 U.S. 323 (1966), http://supreme.justia. com/us/ 385/323/ case. html#T7 (İET :26.11. 2007).

[23] ELECTRONİC SURVEİLLANCE AND THE FOURTH AMENDMENT. Bu davada Hakim Black ve Hakim White karara muhalif kalmışlardır. Bu hakimlere göre, Berger kararı Anayasa'nın dördüncü maddesini çok sıkı yorumlamış ve bu konudaki Anayasal eşiği oldukça yüksek tutmuştur. Bu azınlık görüşü daha sonra verilen Katz kararında dikkate alınmış kanunla düzenlenmek kaydıyla iletişimin denetlenmesine imkan tanınmasının gerekli olduğu kabul edilmiştir. Bk. BERGER-NEW YORK, 388.

[24] BERGER-NEW YORK, 388, 59; DEMPSEY, James X. : "Communications Privacy In The Digital Age: Revitalizing The Federal Wiretap Laws To Enhance Privacy", Originally published in the Albany Law Journal of Science & Technology, Volume 8, Number 1, 1997, http://www.cdt.org/publications/ lawreview/1997 albany.shtml#t33 (İET:25.9.2007).

[25] ELECTRONIC SURVEILLANCE AND THE FOURTH AMENDMENT. The purpose of the probable-cause requirement of the Fourth Amendment to keep the state out of constitutionally protected areas until it has reason to believe that a specific crime has been or is being committed is thereby wholly aborted. (ELECTRONİC SURVEILLANCE AND THE FOURTH AMENDMENT).

konuşma içeriklerinin arama ve elkoyma hükümlerine tabi olması gerektiğine karar vermiştir[26]. Yüksek Mahkeme, New York Eyaleti Ceza Usul Kanunu'nun 813. maddesinin anayasal koruma altında olan alana müdahale edecek kadar geniş bir alana girdiğini bu nedenle Anayasa'nın 4 ve 14. Ek maddelerinin ihlaline neden olduğuna karar vermiştir[27]. Mahkemenin dile getirdiği eksiklikler şunlardır[28]:

1. İletişiminin denetlenmesi tedbirine konu olacak yere ve suça ilişkin[29], ayrıca suçun işlendiğini veya işlenmekte olduğunu gösterecek yeterli açıklama bulunmamaktadır.[30]

2. Aramayı genel olmaktan çıkaracak sınırlandırmalar bulunmamaktadır ve iletişimin ne kadar bir süre zarfında denetleneceği, tedbirin bitiş tarihi belirtilmemiştir, tedbirin bitirilmesi kolluk görevlisine bırakılmıştır[31].

3. Mahkeme kararının bir an önce yerine getirilmesi öngörülmüş değildir[32].

4. Mahkeme kararınına ilişkin sürenin uzatılması için sadece 'kamu yararı' yeterli sayılmış, tedbirin uzatılması için makul sebeplerin bulunduğu izah edilmemiş, kanunda iletişimin denetlenmesi tedbirinin kullanılabileceği suç tipi için "yeterli sebep" şartı belirtilmemiştir[33].

5. Tedbirin ilgiliye bildirimine ilişkin bir düzenleme bulunmadığı gibi, birtakım zorlayıcı sebeplerin (exigent circumstances) varlığı nedeniyle bu kurumun hayata geçirilmediği hususu da belirtilmemiştir[34].

---

[26] BERGER-NEW YORK, 388, 41.

[27] STEVENS, Gina/ CHARLES Doyle;, "Privacy: An Overview of Federal Statutes Governing Wiretapping and Electronic Eavesdropping", CRS Report for Congress, Order Code 98-326. s.6; DONOHUE, s. 8; BERGER-NEW YORK, 388 u.s. 41-42, 1967, P. 51. http:// supreme.justia.com/us/388/41/case.html (İET:9.8.2007).

[28] STEVENS/DOYLE, s.6.

[29] Denetlemenin sadece suça taalluk eden durumlara ilişkin olabileceğini öngören hususilik prensibi (particularity principle) belirtilmemiştir.; ÖZDOĞAN,(2004), s.11.

[30] BERGER-NEW YORK, 388, 55-58.

[31] BERGER-NEW YORK, 388, 59.

[32] BERGER-NEW YORK, 388, 59.

[33] BERGER-NEW YORK, 388, 59.

[34] BERGER-NEW YORK, 388, 60; Şüpheliye, dinleme sonrasında telefonunun dinlendigi bilgisinin verilmemesi, sanığın mahkemede kendi aleyhine delil olarak kullanılacak bilgilerden haberdar olamaması gibi bir sonuç doğurmaktadır ki, bu durum, iddia ve savunma taraflarının eşit imkanlara sahip olması (equality of arms) prensibini, dolayısıyla adil yargılanma ilkesini ihlal etmektedir.(ÖZDOĞAN, (2004), s.11.

6. Gizlilik gerekçesiyle bildirimin öngörülmediği hallerde de, bu eksiklik zorlayıcı nedenlerin belirtilmesi suretiyle bertaraf edilmemiştir[35].

7. Denetleme süreci ve sonuçları hakkında yargıya rapor verme zorunluluğu bulunmamaktadır.

8. Kişinin, mahkeme kararında belirtilmeyen suçları için de, aynı Mahkeme kararı ile dinleme yapılabilmektedir. Diğer bir ifadeyle, mahkeme kararında belirtilmeyen durumlar bakımından bu mahkeme kararı kullanılarak dinleme yapılabilmektedir[36].

Berger davasının en önemli özelliği, iletişimin denetlenmesinin Anayasa'nın 4. maddesi kapsamına girdiğine hükmedilmesidir. Fiziksel arama ve elkoyma sınırlarını belirleyen bu maddeye, iletişimin denetlenmesinin sokulması yeni bir yaklaşımın ürünüdür. Katz davasıyla da, haberleşme hürriyetinin Anayasa'nın 4. maddesiyle korunduğu tescil edilmiştir[37].

Berger kararından sonra verilen Katz kararı[38] da, Amerikan Yüksek Mahkemesinin telefon iletişimini Anayasa'nın 4. maddesindeki mahremiyet alanı içinde[39] kabul ederek koruma altına aldığı çok önemli bir karardır[40]. 1960'lı yıllarda Yüksek Mahkeme, iletişimin denetlenmesine dayandırılarak yapılan, aşırı ve gayri makul (unreasonable) olarak nitelendirilebilecek soruşturmalar çerçevesinde verilmiş arama ve elkoyma kararlarından bireyleri korumayı amaçlamıştır. Bu konuda dönüm noktası olarak kabul edilen Katz kararıyla, mahkeme kararı olmaksızın yapılan telefon dinlemesinin Anayasa'nın 4. maddesine aykırı olduğuna karar verilerek mahremiyet alanını genişleten bir karar alınmıştır. Böylece, 1928 tarihli Olmstead ve Goldman kararlarından farklı bir yaklaşım benimsenmiş[41] ve iletişim anayasal korumaya

---

[35] BERGER-NEW YORK, 388, 60.

[36] ÖZDOĞAN,(2004), s.11.

[37] ÖZDOĞAN,(2004), s.13.

[38] Loto sonuçları, piyango numaraları gibi kumar bilgilerini eyaletler arası telefon hatları üzerinden göndermeye ilişkin yasağı ihlal eden Katz, bir telefon kulübesini kullanarak kumar bilgilerini başka eyaletlere göndermekteydi. Federal Sorusturma Bürosu (FBI) ajanları tarafından, Katz'ın kullandığı telefon kulübesine dinleme ve kaydedici cihaz yerleştirildiğini öğrenen Katz, özel hayatının ihlal edildigi gerekçesi ile mahkemeye başvurmuştur. KATZ-ABD, 389.

[39] STEVENS/DOYLE, s.6.

[40] JUDGE Michael P./KALUNIAN, Robert Kathy Quant: "Brief Overwiev of the Wiretap Law",http:// pd.co. la.ca.us/overv.htm,(İET:26.9.2007); DEMPSEY, "Communications Privacy In The Digital Age: Revitalizing The Federal Wiretap Laws To Enhance Privacy" ; KHAN, s. 65.

[41] AN OVERVIEW OF ELECTRONIC SURVEILLANCE,D.2.

alınmıştır[42]. Deprem etkisi oluşturan bu kararıyla Mahkeme, Anayasa'nın 4. maddesi ile korunan şeyin mekanlar olmadığını, insan olduğunu ifade ederek özel hayat bakımından çok önemli bir karar almıştır[43]. Çoğunluk görüşüne katılan Hakim Stewart[44], insanların ev veya işyerleri gibi kendi özel alanlarında kamuya açıkladıkları, açığa vurdukları şeylerin 4. madde kapsamına girmediğini ancak kendilerine saklayıp kamuya açıklamadığı şeylerin özel hayat kapsamında sayılması gerektiğini ifade etmiştir. Bu bağlamda, kişinin mahrem alanda tuttuğu şey, kamuya açık bir alanda bile olsa, Anayasal koruma altındadır. Makul mahremiyet beklentisi (reasonable expectation of privacy) doktrini, Hakim Harlan'ın yazdığı çoğunluk görüşünde irdelenerek ikili bir teste tabi tutulmuş ve öncelikle bir mahremiyet beklentisinin var olup olmadığının, ikinci olarak da bu beklentinin makul olup olmadığının araştırılması gerektiği vurgulanmıştır[45].

Katz davasında ise mahkeme, iki noktayı değerlendirmeye almıştır. Bunlardan ilkine göre; herkesin kullanımına açık bir telefon kulübesinden yapılan konuşma da kişinin mahremiyet beklentisi kapsamındadır[46]. Mahkemece tartışılan ikinci nokta ise, 4. madde kapsamında arama ve el koyma işleminin vaki olması için, fiziksel müdahalenin gerekliliği sorunudur. Bu konuda mahkeme, Anayasa'nın 4. maddesi bağlamındaki arama ve elkoyma için müdahaleye gerek olmadığını, çünkü (haksız arama ve el koymaya karşı olan) 4. maddenin "fiziksel alana ilişkin değil, şahsın kendisine ilişkin bir koruma getirdiği sonucuna varmıştır. ABD Kanun koyucunun amacı haksız polisiye uygulamalara karşı vatandaşın korunmasıdır[47].

Bu kararla, haksız uygulamaların meydana gelmiş sayılması için fiziksel müdahalenin şart olmadığı vurgulanmıştır. Bu kararı desteklemekle birlikte farklı bir gerekçeye dayanan Hakim Harlan'ın muhakemesi, yani makul mahremiyet beklentisi doktrini (reasonable expectation of privacy) bugün bile geçerliliğini korumaktadır. Bu değerlendirmeye göre, mahremiyetin ihlal edilmesi için iki şartın varlığı aranmaktadır. Bunlardan ilki, şüphelinin mahremiyet beklentisinin bulunmasıdır. İkinci şart ise, bu

---

[42] DONOHUE, s., 6; WONG, 3.1.4.

[43] DONOHUE, s., 6; AN OVERVIEW OF ELECTRONIC SURVEILLANCE,D.2.

[44]KATZ-ABD, 389 U.S. 347 (1967), 389 U.S. 347, http://supreme.justia.com/us/389/347/case.html, (İET:10.11.2007) Konuyla ilgili olarak Bk. LEWİS-ABD, 385 U.S. 206, 210; LEE -ABD., 274 U.S. 559, 563. kararları.

[45] DONOHUE, s.,6 ;STEVENS /DOYLE, s. ,Dp.15.

[46] Bk. KATZ-ABD.

[47] ÖZDOĞAN, (2004),s.12-13.

beklentinin genel bir kabulle kabullenilmiş olmasıdır. Bu ikili şart 'sübjektif mahremiyet beklentisinin objektif ölçülere göre makul olması' şeklinde ifade edilmektedir. Bir radyo ya da televizyon programına katılan bir insanın, yaptığı konuşmaların başka medya organlarında yayınlanması halinde özel hayat iddiasında bulunamaması bu duruma örnek verilebilir. Harlan'a göre, bu unsurlardan ilki, ilgilinin bir alanı mahrem olarak görerek bunu dışa vurmasıdır. Ayrıca, bu mahremiyetin toplum tarafından kabul edilebilecek bir nitelikte olması, diğer bir ifadeyle makul olması gerekmektedir[48]. Katz kararıyla, Mahkeme, kısa süreli, dar bir alana odaklanmış ve sadece bazı iletişimleri kapsamına alan denetlemelerin, bir hakim tarafından tasdik edilmek ve özel ve muhik nedenler olmak kaydıyla Anayasa açısından kabul edilebilir olduğuna hükmetmiştir[49].

1.1.3.1968 Tarihli Teknik Dinleme Kanunu

ABD Kongre'si, 1968 yılında Teknik Dinleme Kanunu'nu (Wiretap and Electronic Surveillence Act) çıkarmıştır. Çok Yönlü Suçla Mücadele ve Güvenli Sokaklar Kanunu'nun 3. Bölümü olarak kanunlaştırıldığı için Bölüm III (Title III) olarak da adlandırılan bu kanun, adli amaçlı iletişimin denetlenmesi hususunda hükümler getiren temel kanundur. Bu kanun detaylı bir şekilde aşağıda anlatılacaktır.

1.1.4.1978 Tarihli Dış Güvenlik İstihbarat Kanunu

1978 yılında çıkarılan Dış Güvenlik İstihbarat Kanunu (Foreign Intelligence Surveillence Act-FISA) ABD'de önleme amaçlı iletişimin denetlenmesi tedbirini düzenleyen temel kanundur. Bu kanun aşağıda detaylı bir şekilde anlatılacaktır.

1.1.5. 1986 Tarihli Elektronik Haberleşme Mahremiyeti Kanunu

Kongre, 1986 yılında iletişimin denetlenmesi hususunda yeni bir kanun çıkarmak zorunda kalmıştır. 1968 Kanunu'nu güncellemek amacıyla atılan bu adımın arkasında birkaç neden bulunmaktadır. Değişik tarihlerde verilen mahkeme kararlarıyla Teknik Dinleme Kanunu'nun iyice delinmesi, telekomunikasyon teknolojisindeki başdöndüren gelişme ve telekomünikasyon sektörü tarafından yeni bir kanun çıkarılması yönünde yapılan baskı da Kongre'nin bu kanunu çıkarmasına neden olan faktörlerdendir.

---

[48] DONOHUE, s., 6 ; STEVENS/DOYLE, Dp.15 ;ÖZDOĞAN, (2004), s. 13

[49] "…under sufficiently 'precise and discriminate circumstances' a federal court may empower government agents to employ a concealed electronic device 'for the narrow and particularized purpose of ascertaining the truth of the…allegations…" (KATZ -ABD, 347, 355); DEMPSEY, "Communications Privacy In The Digital Age: Revitalizing The Federal Wiretap Laws To Enhance Privacy".

ECPA olarak da adlandırılan bu (The Electronic Communication Privacy Act) kanun öncesinde devlet görevlileri, Teknik Dinleme Kanunu'nun tanıdığı yetkiler bağlamında kablosuz, dijital, modem ve optik haberleşmeleri dinleme yetkisine sahip olamamaktan şikayetçi idiler. Bu ortamda kanunlaştırılan ECPA, teknolojik gelişmeler doğrultusunda, devlet görevlilerinin vatandaşın özel hayatını korumak kaydıyla, iletişimin denetlenmesi tedbirine başvurabilmesi için gerekli hukuki altyapıyı güncellemeyi amaçlamıştır. Denilebilir ki ECPA, üç ana hedefi gerçekleştirmek için çıkarılmıştır. Bunlar; kolluk kuvvetlerinin işini kolaylaştırmak, mahremiyeti korumak ve teknolojinin gelişimini ve kullanımını desteklemektir[50].

Bu niyetle kamuoyuna sunulan ECPA, Teknik Dinleme Kanunu'ndan daha geniş yetkiler tanımış, başka bir ifadeyle kolluk kuvvetlerinin teknik dinleme kabiliyetlerini artırmıştır. Teknik Dinleme Kanununda kullanılan "kablolu veya sözlü haberleşme (wire or oral communication) tabiri "kablolu, oral veya elektronik haberleşme ile foto-elektronik veya foto-optik sistemlerle yapılan haberleşme" olarak genişletilmiştir. 'Interception'"(müdahale-denetleme) tabiri, 'intercept or other acquisition' yani müdahale / denetleme veya diğer metotlarla elde etme" olarak değiştirilmiştir. Teknik Dinleme Kanun'unda geçen "kablolu haberleşme" tabiri "kablolu haberleşme veya iki kablosuz telefon arasındaki haberleşme veya bir kablosuz ile bir kablolu telefon arasındaki haberleşme" olarak değiştirilmiştir. Böylece, kablosuz telefonlarla yapılan haberleşmenin de dinlenebilmesi için gerekli kanuni altyapı meydana getirilmiştir[51].

ECPA'nın, mahremiyeti koruma hakkında yaptığı en önemli katkı, elektronik işlem ve depolama bilgilerini de özel hayat kapsamına dahil etmesidir[52]. Teknik Dinleme Kanunu'nda, özel haberleşme şebekeleri üzerinden yapılan iletişimin mahremiyet kapsamına girip girmediği hususu muğlak bulunduğundan, ECPA bu konuya açıklık getirmiş ve özel şebekeler üzerinden yapılan haberleşmelerin de anayasal koruma altına alınması gerektiğini vurgulamıştır[53].

[50] ÖZDOĞAN, (2004), s.22.

[51] ÖZDOĞAN, (2004), s.22-24.

[52] AN OVERVIEW OF ELECTRONIC SURVEILLANCE, D.1.2.

[53] ÖZDOĞAN, (2004), s. 24.

ECPA'nın açıklığa kavuşturduğu diğer bir husus da, iletişimin denetlenmesi ile elde edilen bilgilerin hangi durumlarda kimlere açıklanabileceğinin net olarak ortaya konulmuş olmasıdır[54].

1.1.6.1986 Tarihli Numara ve Rota Tespit Kanunu

İletişimin tespiti konusunda düzenleme getiren Numara ve Rota Tespiti Kanunu, 1986 yılında çıkarılmıştır. Bu kanun detaylı bir şekilde aşağıda açıklanacaktır.

1.1.7.1994 Tarihli Telekomünikasyon Şirketlerinin Kolluk Kuvvetlerine Yardımı Kanunu

Teknolojinin gelişmesiyle, hem iletişimin denetlenmesi alanındaki teknik ve yasal zorluklar, hem de bu teknolojilerin uygulanması ile özel hayatın ihlali tehlikesi artmıştı[55]. Yetersiz hat kapasitesi, çevrilen numaranın tespit edilemeyişi, telefon servis sağlayıcılarının teknik yetersizlikleri yüzünden şehirler ve milletlerarası görüşmelerin güvenlik güçleri tarafından dinlenemeyişi, hızlı arama, sesle arama, çağrı bekletme, çağrı yönlendirme, sesli mesaj gibi yeni iletişim vasıtalarının ortaya çıkmış olması ve telekomünikasyon sektöründe monopolinin sona ermesi gerek eyalet, gerekse federal kolluk kuvvetlerinin başarısızlığına neden olmaktaydı[56].

Bahse konu problemlerin aşılması amacıyla 1994'te kanunlaştırılan bu kanun (Communications Assistance for Law Enforcement Act-CALEA)[57], önceki tecrübelerden yararlanılmak suretiyle bazı asgari standartların ülke çapında yerleştirilmesini şart koşmuş[58] ve üç unsur arasında denge kurmayı hedeflemiştir. Bunlar, suçla mücadelede güvenlik güçlerinin teknik dinleme imkanlarından yeterince yararlandırılması, yeni teknolojilerle birlikte artan mahremiyetin ihlaline yönelik risklerin en aza indirilmesi ve sayılan bu iki hedefin gerçekleştirilmesi esnasında yeni haberleşme servisleri ve teknolojilerinin engellenmemesi olarak sayılabilir[59].

---

[54] 18 U.S.C. § 2517.

[55] STEVENS/DOYLE, s. 54; ÖZDOĞAN, (2004), s. 44-45. ; DEMPSEY, "Communications Privacy In The Digital Age: Revitalizing The Federal Wiretap Laws To Enhance Privacy".

[56] ÖZDOĞAN, (2004), s.44-48.

[57] 18 U.S.C. § 2522, Communications Assistance for Law Enforcement Act, http://www4.law.cornell. edu/ uscode/search/display.html?terms=2522&url=/uscode/html/uscode18/usc_sec_18_00002522----000-.html (İET:3.11.2007).

[58] DEMPSEY, "Communications Privacy In The Digital Age: Revitalizing The Federal Wiretap Laws To Enhance Privacy".

[59] ÖZDOĞAN, (2004), s. 54-55; DEMPSEY, "Communications Privacy In The Digital Age: Revitalizing The Federal Wiretap Laws To Enhance Privacy".

CALEA ile telekomünikasyon servis ve transmisyon sağlayıcıları, sistemlerini yetkisiz ve uygun olmayan gizli dinlemelere karşı koruyacak tedbirleri almakla yükümlü kılınmışlar[60], bu kanundaki kabiliyet ve kapasite yükümlülüklerini (Madde 103 ve 104) yerine getirmek için birbirlerine danışmanlık yapmak ve işbirliğine gitmek zorunda bırakılmışlardır[61]. Adalet Bakanlığı da, Kanun çerçevesinde, güvenlik güçleri ile işbirliği halinde, standart belirleyici organizasyonlara, telekomünikasyon şirketleri birliklerine, telekomünikasyon aletleri tüketici temsilcilerine ve ilgili diğer kuruluşlara danışmanlık yapmakla yükümlü kılınmıştır[62].

Kanun'un 102. maddesi uyarınca her türlü telekomünikasyon servis ve transmisyon sağlayıcıları, Kanun'u yürütmekle yükümlü kılınmıştır[63]. Bu bağlamda, telekomünikasyon sektörü tarafından hizmete sokulan yeni teknolojiler, kolluk güçlerinin teknik dinleme yeteneklerini sınırlandırmamalıdır[64]. 104. maddede sayılan yükümlülükler çerçevesinde; servis sağlayıcılar, acil durumlarda, güvenlik güçlerine şirketlerinin binalarını kullanarak dinleme yapmalarına imkan tanımak ve teknik dinleme konusu mobil hedefin kendi servis bölgelerine giriş çıkışları hakkındaki bilgileri güvenlik güçlerine vermek zorunda bırakılmışlardır. Bununla birlikte, güvenlik güçleri, telekomünikasyon şirketlerine, herhangi bir aletin kullanılıp kullanılmaması konusunda baskı yapamayacaklardır[65].

Özel hayatın korunması amacıyla CALEA tarafından atılan adımlar önemlidir. CALEA'nın 202. ve 203. maddeleri ile, ECPA'nın radyo haberleşmesi ve kablosuz telefon görüşmeleri hakkındaki mahremiyeti korumaya ilişkin hükümlerinin kapsamı genişletilmiştir[66]. Numara ve rota tespit cihazlarının kullanımı da CALEA ile

---

[60] CALEA 105. madde.

[61] CALEA 106. madde.

[62] CALEA 107. madde.

[63] ÖZDOĞAN, (2004), s.55.

[64] DEMPSEY, "Communications Privacy In The Digital Age: Revitalizing The Federal Wiretap Laws To Enhance Privacy"; Kullanılan teknolojiler içinde, teknik dinlemeye engel olacak durumlar içeren sistemler elden geçirilerek, bu sistemler dinlemeye müsait hale getirilmelidir. Kanun'un 103. maddesi uyarınca servis ve transmisyon sağlayıcıları, çağrının kapsamını izole etmeli, çağrı tanımlama detaylarını (arayan ve aranan numaralar, arama süresi, aramanın zamanı, vs.) güvenlik güçlerine vermelidirler. Coğrafi yer bilgisi, arayan ve aranan numaralarla tespit edilen bir bilgi olmadığı müddetçe, çağrı tanımlama bilgisi kapsamına girmemektedir. Çağrı içerik ve tanımlama bilgileri, servis saglayıcının hizmet verdigi alan içerisinde güvenlik güçlerinin göstereceği bir yere, uygun formatta iletilmelidir. Görüşmelere müdahale edildiği hususunun fark ettirilmemesi için azami tedbirler alınmalıdır. (ÖZDOĞAN, (2004), s.55).

[65] ÖZDOĞAN,(2004), s.56-57;

[66] 206. madde hükmüne göre yetki olmaksızın ve telekomünikasyon servislerine erişim maksadıyla degişikliğe uğratılmış telekomünikasyon cihazı, yazılım, donanım ve radyo frekans tarama cihazları kullanılması yasaklanmıstır. Kanun; radyo frekans tarama cihazları dahil, hücresel telefonların (cep

kısıtlanmıştır[67]. Telekomünikasyon servis ve transmisyon sağlayıcıları, hakkında denetleme kararı verilmemiş görüşmelerin mahremiyetinin ve güvenliğinin korunması için gerekli tedbirleri almalıdırlar[68]. Telekomünikasyon sistemlerinin tasarım aşamalarındaki değişiklikleri de kapsayan bu hüküm, güvenlik güçlerinin ihtiyacı olan dinlemeye karşı bir denge oluşturmaktadır. Her hangi bir kişi ya da kuruluş teknik dinleme kabiliyetlerinin yeniden değerlendirilmesi için Federal İletişim Komisyonu'na başvurma hakkına sahiptir[69].

İletişimin denetlenmesi talebi doğrultusunda yetkili hakim, ilgili üçüncü kişilerden bilgi vermelerini, teknik yardım sağlamalarını isteyebilir. Hakimin bu yöndeki bir kararında, CALEA Kanunu hükümleri çerçevesinde hareket edilmesi, diğer bir ifadeyle iletişimin denetlenmesi kabiliyet yükümlülüklerinin yerine getirilmesi istenebilir. CALEA hükümlerine göre, bu üçüncü kişilerin yaptıkları yardım esnasında uğradıkları zararlar tazmin edilir[70].

1.1.8. 2001 Tarihli Patriot Act (Vatansever Kanunu)

1.1.8.1.Genel Olarak

Tam adı, 'Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001' olan ve USA PATRİOT Act ya da USAPA olarak kullanılan Patriot Kanunu, her şeyden önce adından dolayı eleştirilen bir kanun olarak kamuoyuna sunulmuştur. Bu uzun cümlenin kelimelerinin baş harfleri alınarak diğer bir ifadeyle, akrostiş[71] yapılarak ismi konulan bu kanun, kolluk kuvvetlerinin teknik takip ve soruşturma kabiliyetlerini artıran bir formatta

---

telefonu vs.) kopyalanması için kullanılan kopyalama aletlerinin bulundurulmasını da yasak kapsamına almıştır. Bu maddede belirtilen hükümlere uymayanlar hakkında, 15 yıla kadar varan hapis ile en az 50 bin dolar para cezası veya telefon kopyalama suçu ile elde ettigi maddi kârın iki katı kadar para cezası öngörülmüştür. (ÖZDOĞAN, (2004), s.59-60).

[67] CALEA 207. madde

[68] CALEA 103.mad.

[69] DEMPSEY, "Communications Privacy In The Digital Age: Revitalizing The Federal Wiretap Laws To Enhance Privacy"; CALEA 107. madde; ÖZDOĞAN, (2004), s. 57.; 107. maddeye göre, CALEA yükümlülüklerinin yerine getirilmesini denetlemekle ve bu kanun hakkındaki soruları cevaplandırmakla yükümlü kurum Federal İletişim Komisyonu'dur. (FCC-Federal Communications Commission).

[70] WONG, 3.3.9.

[71] Akrostiş/İlkleme, bir şiirde dizelerin ilk harflerinin yukarıdan aşağıya doğru sıralandığında anlamlı bir sözcük meydana getirmesidir. http://tr.wikipedia.org/wiki/Akrosti%C5%9F (İET:24.11.2007) (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act,(USA PATRIOT Act).

hazırlanmıştır[72]. Bu yasanın, yürütme gücü ile sivil haklar arasındaki dengeyi yürütme lehine bozduğu iddia edilmektedir[73].

11 Eylül 2001 saldırısının gerçekleşmesinden birkaç gün sonra kanun çalışmaları hazırlanmış ve Başkan Bush tarafından 26 Ekim 2001 tarihinde imzalanmıştır. 15'ten fazla önemli kanunda ciddi değişiklik yapan 322 sayfalık[74] bu kanun acele olarak hazırlanmış ve Kongre ve Senato'da yeterli bir düzeyde tartışılmamış, hatta birçok milletvekili tarafından okunmamış[75] bir metin olarak eleştiri almaktadır[76]. Terörizmle mücadele amacı taşıyan çok fazla hüküm içeren, kolluk kuvvetlerine iletişime müdahale etmek, kişisel verilere ulaşma hususlarında genişletilmiş yetkiler veren ve Terörizmle Mücadele Kanunu'nun[77] biraz yumuşatılarak kaleme alınmış hali olan Patriot Kanunu, iletişimin engellenmesi hususunda geçici hükümler (sunset provision) içermekteydi. Kolluk güçlerine aşırı yetkiler verdiği, ancak mahkemelere verilmiş olan denge ve fren yetkisini[78] (checks and balances) ortadan kaldırdığı için eleştirilen[79] Patriot Kanunu'yla, sivil hakları özellikle de yabancıların ve de göçmenlerin[80] sivil haklarını doğrudan etkileyen birçok önemli kanunda[81] değişiklik yapılmıştır[82].

---

[72] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act, (USA Patriot Act), Calendar No. 198, 107th Congress, 1st Session H. R. 2975, http://www.govtrack.us/data/us/bills.text/107/h/h2975.pdf ,(İET:28.11.2007).

[73] Electronic Privacy Information Center, The USA PATRIOT Act, http://www.epic.org/privacy/terrorism/usapatriot/default.html 19.11.2007 (THE USA PATRIOT ACT, EPIC Report).

[74] EFF Analysis Of The Provisions Of The USA PATRIOT Act, That Relate To Online Activities(October 31, 2001) Last updated October 27, 2003, http://w2.eff.org/ Privacy/ Surveillance/ Terrorism/ 20011031_eff_usa_patriot_analysis.php (EFF ANALYSIS OF PATRIOT ACT)(İET: 17.9.2007)

[75] DONOHUE, s. 16-18.

[76] Amerikan Sivil Haklar Birliği (ACLU) birçok milletvekilinin metnini okumadan lehte oy kullandığını, terörle mücadele sloganı ile bu kanunun büyük bir acelecilikle ve gizlice çıkarıldığını iddia etmektedir. Bk. AMERICAN CIVIL LIBERTIES UNION, "The Usa Patriot Act And Government Actions That Threaten Civil Our Liberties", http://www.aclu.org/FilesPDFs/patriot%20act%20flyer.pdf , (İET:24.11.2007).

[77] Anti-Terrorism Act of 2001 .

[78] Mahkemelerin denge ve fren sistemini uygulamasıyla, kolluk güçlerinin yetkilerini aşarak hürriyetleri kısıtladığını gösteren birçok gizli olay açığa çıkarılmıştır. Bu örneklerden biri, 1974 yılında, aralarında Martin Luther King'in de bulunduğu 10000 Amerikan vatandaşı hakkında gizli olarak teknik dinleme yapıldığının ortaya çıkarılmasıdır. (EFF ANALYSIS OF PATRIOT ACT).

[79] EFF ANALYSIS OF PATRIOT ACT; Bk. DONOHUE, s. 16-22.

[80] Kanuna karşı çıkan tek senatör olan Russ Feingold, bu kanunun özellikle göçmenlerin sivil hürriyetleri açısından bir tehdit olacağını savunmuştur. Senatöre göre, İrlanda, Haiti ya da Afrika'dan gelen göçmenlerin bu kanunun olumsuz etkilerine maruz kalmayacaklarını, bu kanunun özellikle Arap, Müslüman ve Güney Asya ülkelerinden gelen insanları kötü yönde etkileyeceğini ifade etmiştir.(THE USA PATRIOT ACT, EPIC Report).

[81] Wiretap Statute (Teknik Dinleme Kanunu)(Title III), Electronic Communications Privacy Act (ECPA), Computer Fraud and Abuse Act (Bilgisayar sahteciliği ve suistimali kanunu, Foreign Intelligence Surveillance Act (FISA), Family Education Rights and Privacy Act (Aile Eğitim Hakları ve Mahremiyet Kanunu), Pen Register and Trap and Trace Statute (Numara ve Rota Tespit Kanunu), Money Laundering

Patriot Kanunu'nun, birçok hükmü aslında 11 Eylül olaylarından önce kanunlaştırılmaya çalışılmış, ancak Kongre'de ciddi tartışmalara neden olmuştu. Beyaz Saray Personelinin 1998-2001 yılları arasında şefliğini yapan John Podesta bu hususu gündeme getirerek, bu yasal değişikliğin yapılmasını meşrulaştıran bir neden bulunmadığını ifade etmektedir. Podesta'ya göre yapılan bu değişiklikler, ABD'yi, Anayasa'nın birinci maddesi ile teminat altına alınan haklarını kullanan insanların takip edilerek taciz edildiği istihbarat toplumu günlerine geri götürmektedir ve de 11 Eylül olayları sonrasında böyle bir döneme geri dönmeyi meşrulaştıran hiçbir neden yoktur[83].

1.1.8.2.Patriot Act İle Yapılan Değişiklikler

Patriot Kanunu ile 11 Eylül olayları sonrasında bazı kanunlarda birtakım değişiklikler yapılmıştır. Bunlardan en önemlisi FISA Kanunu kapsamında verilecek elektronik takip ve arama yetkisi ile ilgilidir. Bir diğer önemli husus da, cezai ve istihbari soruşturmacılar arasında bilgi değişiminin mümkün hale gelmesidir. Daha önceden, FISA kapsamında, denetlemenin istihbari amaçlı olduğunun sadece üst düzey idari yetkililerce teyit edilmesi sonrasında elektronik takip ve aramanın yapılması mümkündü. Bu teyit, mahkemeler ve Adalet Bakanlığı tarafından ilk hedef testi olarak adlandırılıyordu. Patriot Kanunu (218. madde) ile, istihbarat toplayabilmek için önemli hedef (significant purpose)[84] kriteri getirilmiş[85] ve FISA'nın kapsamı genişletilmiş oldu. 'Önemli' (significant) kelimesinin anlamının tanımlanmamış olmasından kaynaklanan belirsizlik tutarsızlıklara ve yeknesak olmayan uygulamalara neden olabilmektedir. Yabancı istihbarat toplama gerekçesiyle, cezai soruşturmalarla iç içe geçmiş konularda, FISA hükümleri uygulanmaktadır. Hak ve hürriyetlerin korunması hususunda Teknik Dinleme Kanunu'na göre çok daha gevşek hükümler içeren FISA uygulanarak bir nevi hile yöntemiyle cezai soruşturmalarda delil elde edilmektedir[86].

Act (Kara Para Aklama Kanunu), Immigration and Nationality Act (Göç ve Milliyet Kanunu), Money Laundering Control Act (Kara Para Aklanmasının Önlenmesi Kanunu), Bank Secrecy Act (Banka Gizliliği Kanunu), Right to Financial Privacy Act (Finansal Mahremiyet Hakkı Kanunu), Fair Credit Reporting Act (Adil Kredi Bildirimi Kanunu).

[82] THE USA PATRIOT ACT, EPIC Report.

[83] THE USA PATRIOT ACT, EPIC Report; PODESTA, John:" USA Patriot Act, , The Good, the Bad, and the Sunset American Human Rights", Association Human Rights Magazine, 2002, http://www. abanet. org/ irr/hr/winter02/podesta.html, (İET:19.11.2007).

[84] US Code, 1804(a)(7)(B maddesinde yer alan ifade aşağıdaki gibidir: " … iletişimin tespitinin önemli hedefi yabancı istihbarat elde etmektir."

[85] In Re Sealed Case 310 F.3d 717 Foreign Int. Surv. Ct. Rev. 2002, http://www. prosecutingterrorists. com/inresealedcase.pdf).

[86] THE USA PATRIOT ACT, EPIC Report.

FISA kapsamındaki takip ve aramalarla ilgili olarak istihbaratçılar ile kolluk görevlileri arasında tam bir paylaşım öngörülmesi Patriot Kanunu ile getirilen değişikliklerdendir. 203. madde ile 18 U.S.C. 2517[87] nolu madde değiştirilmiş, iletişimin denetlenmesinden elde edilen bilgilerin açıklanması ve kullanılması hususlarını düzenleyen maddeye yapılan ekleme ile yabancı istihbarat ve karşı istihbarat bilgilerinin (foreign intelligence or counterintelligence) herhangi bir federal kolluk görevlisine ya da istihbarat, göçmen, milli güvenlik görevlisine bu kişinin görev alanı ile ilgili olmak kaydıyla açıklanabilmesi kabul edilmiştir[88]. Kolluk görevlileri ile istihbarat görevlileri arasındaki bilgi 'duvar'ını yıkmayı başka bir ifadeyle bilgi boşluklarını ortadan kaldırmayı (connect the dots) amaçlayan bu kanun ile artık dış istihbarat, karşı casusluk (counterespionage) ve bir ceza soruşturması (criminal investigation) kapsamında elde edilmiş yabancı istihbarat bilgilerinin kolluk görevlileri ve federal görevliler arasında milli güvenliğin korunması amacıyla paylaşılması mümkün hale gelmiştir[89].

6 Mart 2002 tarihinde Genel Savcı John Ashcroft Patriot Kanunu'ndan kaynaklanan bilgi paylaşma prosedürünü hayata geçirdi[90]. Ancak FISA Mahkemesi, 17 Mayıs 2002 tarihinde bu yeni politikayı reddetti. Bu kararla; kolluğun, hedeflerini gerçekleştirmek için FISA usullerini uygulamak suretiyle bir soruşturmayı yönlendirip kontrol edemeyeceğine, bir cezai soruşturmayı derinleştirmek için FISA usullerini kullanamayacağına, ayrıca FISA kapsamındaki arama ve takiplerin başlatılması, genişletilmesi ve devam ettirilmesi amacıyla istihbarat görevlilerine tavsiyelerde bulunamayacağına karar verildi. FISA mahkemesinin bu kararına itiraz edilmesiyle, bu mahkemenin kararı tarihinde ilk kez itiraza konu oldu. İtiraz üzerine FISA İtiraz Mahkemesi (FISA Court of Review), FISA'nın, yabancı istihbarat bilgisinin belli türdeki cezai soruşturmalarda hükümet tarafından kullanılmasını sınırlandırmadığına karar verdi[91]. Mahkemenin bu kararıyla, FISA'nın Patriot Kanunu ile değiştirilmiş hükmünün[92]

---

[87] 18 U.S.C. § 2517(6); THE USA PATRIOT ACT, EPIC Report.

[88] Aslında 203. madde ile getirilen bu değişiklik, daha önceden Anti Terör Kanunu ile getirilmek istenmişti. Patriot Kanunu'nun, Anti Terör Kanunu ile getirilmek istenen hükme göre daha az hak sınırlayıcı olduğu söylenebilir. Nitekim, bu bilgiler ancak usulsüz bir soruşturma çerçevesinde kullanılabilmekte, bu bilginin usulsuz kullanılması ve açıklanması birtakım müeyyidelere bağlanmaktadır THE USA PATRIOT ACT, EPIC Report.

[89] PATRIOT ACT FACT SHEET; BULZOMI, MICHAEL J.: Foreign Intelligence Surveillance Act, Before and After the USA PATRIOT Act, The FBI Law Enforcement Bulletin, http://www.fbi.gov/ publications/ leb/ 2003/june2003/june03leb.htm#page_26,(İET:27.8.2007) (BULZOMI, "Foreign Intelligence Surveillance Act").

[90] BULZOMI,"Foreign Intelligence Surveillance Act".

[91] Mahkeme yabancı istihbarat suçlarını FISA Kanunu'nda belirtilen suçlar olarak tanımlamıştır. Casusluk, uluslararası terörizm, yasadışı gizli istihbari faaliyetler, sabotaj, yabancı bir güç için veya bu güç adına işlenen kimlik sahteciliği suçları ve bu suçlara yardım ve yataklık suçları bu suçlar arasındadır. Öte

Anayasa'nın 4. maddesine aykırı olmadığına hükmedilmiş oldu[93]. Böylece istihbaratçılar ile diğer kolluk görevlileri arasındaki bilgi duvarını yıkmayı hedefleyen Patriot Kanunu'nun bu hükmü yargının da onay vermesiyle perçinlenmiş oldu.

FISA İtiraz Mahkemesi tarafından verilen bu karar, Kongrenin ve Genel Savcı Ashcroft'un intikamını onlar adına almak anlamına gelmektedir. Bu bağlamda, casus ve teröristlerin soruşturulması, aranması ve yakalanmaları amacıyla istihbarat elemanları ile kolluk görevlileri arasında bir işbirliğine izin verilmiş olmaktadır[94].

Patriot Kanunu'nun 201[95] ve 202. maddeleriyle, Teknik Dinleme Kanununda belirlenen suçların kapsamı artırılmış ve yeni suçlar eklenmiştir. Bu hükümlerle, Teknik Dinleme Kanununda sayılan öncü suçların (predicate offenses) kapsamı bazı suçları içine alacak şekilde genişletilmiştir. Bu bağlamda, kimyasal suçlar[96], terörizm suçları[97] bilgisayar sahteciliği ve suiistimali suçu[98] da bu kapsama alınmıştır. Daha sonraki eklemelerle, kamuya açık yerlerin, hükümet binalarının, kamu taşıma sistemlerinin ve bunlara ilişkin altyapı sistemlerinin bombalanması[99] ve terörizmin finansmanı suçu[100] da dahil edilmiştir[101].

---

yandan, yabancı bir istihbarat faaliyetini ile iç içe geçmiş bir adi suç da bu kapsamdadır. Terör eylemlerini finanse etmek için banka soymak veya bir casusun kimliğini saklamak için kredi kartı sahteciliği yapmak bu suçlara örnek verilebilir. Mahkemeye göre, Patriot Kanunu ceza kolluk görevlileri ile istihbarat ve karşı istihbarat görevlileri arasındaki 'duvar'ı ortadan kaldırmıştır. Kongre, Patriot Kanunuyla FISA'ya bir ek yapmakla bu konudaki niyetini açıkça ortaya koymuştur.(BULZOMI,"Foreign Intelligence Surveillance Act").

[92] Ceza kolluk görevlileri ile istihbarat ve karşı istihbarat görevlileri arasındaki 'duvar'ı ortadan kaldıran yeni FISA maddesi aşağıdaki gibidir: 'Bu başlığın altında yabancı istihbarat elde etmek için elektronik takip yapan federal görevliler, yabancı bir gücün veya bu gücün bir ajanının mevcut veya potansiyel veya başka türden bir düşmanca faaliyetlerini, yabancı bir gücün veya bu gücün bir ajanının gerçekleştirdiği bir sabotaj veya terörizm faaliyetini, bir istihbarat servisinin veya yabancı bir gücün veya bu gücün bir ajanının yürüttüğü gizli istihbarat faaliyetini soruşturmak veya bunlara karşı korunma amaçlı olarak federal kolluk görevlileri ile işbirliğine gidebilirler'(50 U.S.C. § 1806(k)).

[93] BULZOMI,"Foreign Intelligence Surveillance Act".

[94] BULZOMI,"Foreign Intelligence Surveillance Act". Aslında hükümet, FISA marifetiyle şüpheli teröristleri dinlemek hakkına sahipti. Ancak FISA ile ABD vatandaşları hakkında iletişimin denetlenmesi tedbirine başvurulması mümkün olmadığından Patriot Kanunu'nun 201. maddesi ile yapılan bu değişiklik, hükümete bir Amerikan vatandaşının da ülke içi terörizm suçlaması nedeniyle bu kapsama sokulması sonucunu doğurmuştur.(BULZOMI,"Foreign Intelligence Surveillance Act").

[95] 10 Mart 2005 tarihi itibariyle, 201. maddeye iki ayrı soruşturmada toplam 4 defa başvurulmuştur. Bu davalardan birtanesi, kürtaj kliniklerini bombalamak için patlayıcı madde edinmek suçundan mahkum olan Ku Klux Klan örgütünün milli lideri (Imperial Wizard) hakkında idi. FACT SHEET: USA PATRIOT ACT PROVISIONS SET FOR REAUTHORIZATION, http://www.lifeandliberty.gov/agpatriotactrevision.htm (İET: 24.11.2007) (PATRİOT ACT FACT SHEET).

[96] 18 U.S.C. § 229.

[97] 18 U.S.C. § 2332, 2332a, 2332b, 2332d, 2339A, 2339B.

[98] 18 U.S.C. § 1030.

[99] 18 U.S.C. § 2232f.

Patriot Kanunu'yla ile getirilen bir diğer önemli yenilik de, gezici takip (roving tap) olarak adlandırılan yöntemdir[102]. FISA gezici takip yöntemini, Teknik Dinleme Kanunu'nda sayılan şartların varlığı halinde hayata geçirebilmektedir[103]. Bu madde ile, hedef kişinin (intelligence target) kullandığı bir cihazın takibe alınması yerine, FISA Mahkemesinin vereceği bir karar marifetiyle, ilgili kişinin kullanabileceği tüm cihazların denetlenmesine imkan tanınmaktadır. Teröristlerin, kullandıkları iletişim araçlarını çabucak ve ustalıkla değiştirebildikleri ve bu konuda eğitim aldıkları gerçeğinden hareket edilerek çıkarılan bu hüküm gelişmiş yöntemleri kullanan teröristlerin daha kolay takibini sağlaması bakımından hükümetin elini güçlendirmiştir. Teknik Dinleme Kanunu çerçevesinde uyuşturucu suçları gibi eylemler hakkında başlatılmış cezai soruşturmalar kapsamında uzun bir süreden beri başvurulagelen bu uygulama, FISA kapsamındaki suçlar hakkında da böylelikle uygulanmaya başlamıştır[104]. Böylece, takipten kaçmak için değişik yöntemlere başvuran kişiler hakkında, gerekli şartların varlığı halinde gezici takip denilen bir takip türü çıkarılmaktadır. FISA, gezici takip yöntemini Teknik Dinleme Kanununda sayılan şartların varlığı halinde hayata geçirebilmektedir[105].

Bu genel uygulama ile masum kişilerin özel hayatlarının ihlal edileceği yönünde kamuoyunda ciddi endişeler ortaya çıkmıştır. Örneğin, hedef kişi tarafından kullanılacağı istihbar edilen ve bu bilgi sonrasında FBI tarafından takibe alınan bir internet kafedeki tüm kişilerin iletişimleri takibe maruz kalmış olacaktır. Takibe alınan yerin bir kütüphane olduğu varsayımı bu endişenin boyutlarını artırmaktadır. Kütüphane yetkililerinin, böyle bir takibin yapıldığını kullanıcılara açıklamaktan menedildiği hallerde durum kuşkusuz daha da ağırlaşmış olacaktır. Genel nitelikli bir gezici takip emrinin ciddi anayasa ihlalleri oluşturduğu ve Anayasa'nın 4. maddesinin ihlali anlamına geldiği, EPIC gibi bazı sivil toplum kuruluşları tarafından iddia edilmektedir. Nitekim, iletişimin denetlenmesine imkan tanıyan mahkeme kararı takibe alınacak yeri kesin

---

[100] 18 U.S.C. § 2339C.

[101] MUELLER, Robert S.: "Congressional Testimony, Federal Bureau of Investigation Before the United States Senate Committee on the Judiciary Sunset Provisions of THE USA PATRIOT ACT" April 5, 2005, http://www.fbi.gov/congress/congress05/mueller040505.htm (İET:17.11.2007); PATRIOT ACT FACT SHEET.

[102] Patriot Act 206. Madde.

[103] WONG, 3.4.6; EFF ANALYSIS OF PATRIOT ACT.; THE USA PATRIOT ACT, EPIC Report; PATRIOT ACT FACT SHEET.

[104] PATRIOT ACT FACT SHEET; Özellikle uluslararası terörizm suçları ve casusluk suçlarında etkin olarak kullanılmıştır. Bu maddeye, 30 Mart 2005 tarihi itibariyle 49 defa başvurulmuştur.

[105] WONG, 3.4.6; EFF ANALYSIS OF PATRIOT ACT; THE USA PATRIOT ACT, EPIC REPORT .

olarak belirtmemektedir. Kanunlara bağlı Amerikan vatandaşlarının da bu tür takiplere takılması ihtimali endişe ile karşılanmaktadır[106].

Patriot Kanunu'nun 207. maddesi ile, FISA kapsamında verilmiş iletişimin denetlenmesi süresi 90 günden 120 güne çıkarılmaktadır. Bu süre, yine mahkeme kararıyla bir yıla kadar uzatılabilir[107].

Patriot Kanunu'nun 212. maddesiyle Amerikan Adalet Bakanlığının savunduğu bir uygulama hayata geçirilmiştir. Bu madde ile, elektronik servis sağlayıcıları vasıtasıyla, acil durumlarda müşteri kayıtları ve abonelerin iletişimlerinin içerikleri elde edilebilmektedir[108].

219. maddeyle Federal Rules of Criminal Procedure (Federal Usul Yasası) hükümleri değiştirilmiş ve bir mahkeme tarafından iç ve uluslararası terörizm suçlarıyla ilgili olarak verilen bir iletişimin denetlenmesi kararının o mahkemenin yargı yetkisi dışında da geçerli olması sağlanmıştır. Bu uygulama servis sağlayıcılar nezdinde sıkıntılara neden olmuştur[109]. Patriot Kanunu öncesinde hem Teknik Dinleme Kanunu hem de Numara ve Rota Tespit Kanunu çerçevesinde alınmış kararlar, sadece ilgili mahkemenin coğrafi alanıyla sınırlıydı. Yapılan değişiklikle, iletişimin denetlenmesi amacıyla verilen karar çerçevesinde ABD'nin herhangi bir yerinde cihaz kurulmasını mümkün kılan bir düzenleme yapıldı[110]. İletişimin denetlenmesine ilişkin olarak tüm ülkede geçerli olan mahkeme kararlarının verilmesi, bu kararlara maddi hukuk veya usul hukuku boyutu itibariyle itiraz edecek olan servis sağlayıcılarının işlerini zorlaştırmıştır. Gerçekten de, çok büyük bir ülke olan ABD'de, örneğin, doğudaki bir eyalet mahkemesinin verdiği karara karşı batıdaki bir servis sağlayıcının itiraz etmesi oldukça güçleşmiştir. Gerçekten de, servis sağlayıcıların, kararı veren mahkemeden abonelerinin özel

---

[106] THE USA PATRIOT ACT, EPIC Report.

[107] PATRIOT ACT FACT SHEET.

[108] PATRIOT ACT FACT SHEET.ABD Adalet Bakanlığı yetkilileri, 212. maddenin insan hayatını tehdit eden bazı ciddi suçlarda etkinlikle kullanıldığını ifade etmektedirler. Bu açıklamaya göre, El Paso'daki Islamic Center isimli dini kuruluşa üye kişileri tehdit ettiği iddiasıyla hakkında kovuşturma sürdürülen Jared Bjarnason isimli kişinin iletişimi denetlenmiş ve çok ciddi sonuçlar doğurabilecek bir tehdit engellenmiştir. FBI yetkililerine göre, bu yetkinin kullanılmaması durumunda işletilecek hukuki prosedürün 30 günden fazla bir süre alacak olması nedeniyle, ivedilik arzeden bu durumda gerekli tedbirlerin alınamayacağı ve masum insanların hayatlarının kurtarılamayacağı iddia edilmiştir. (PATRIOT ACT FACT SHEET).

[109] THE USA PATRIOT ACT, EPIC Report.

[110] THE USA PATRIOT ACT, EPIC Report.

hayatlarının hukuk dışı ihlalini doğuracak bir uygulamaya neden olmamak kaygısıyla açıklama (clarification) talebinde bulundukları bilinmektedir[111].

Kanunla yapılan bir başka değişiklikle de, FISA İtiraz Mahkemesi hakimlerinin sayısı 7'den 11'e çıkarılmıştır[112].

1.2.ABD'de İletişimin Denetlenmesi Mevzuatı

1.2.1.Teknik Dinleme Kanununa Göre Adli Amaçlı İletişimin Denetlenmesi

1.2.1.1.Genel Olarak

Adli amaçlı iletişimin denetlenmesi ile ilgili ilk düzenli kanun olan Teknik Dinleme Kanunu, sosyal, politik ve ekonomik parametrelerin tabii bir sonucu olarak ortaya çıkmıştır. Kanunun çıktığı dönemden önceki günlerde Vietnam'da savaşa saplanmış olan ABD'nin ekonomisi kötü yönde etkilenmiş ve ABD'inin barış karşıtı bir ülke olduğu iddiaları güçlenmiştir. Bu iddiaların da etkisiyle, Güney Amerika'dan Kuzey Avrupa'ya ve ülkemize kadar birçok üniversite, ögrenci olayları ile sarsılmıştır. Sadece ABD'de 70'li yıllara girerken 500'e yakın üniversitede, ögrenci hareketleri neden gösterilerek devlet tarafından eğitime ara verilmiştir. Başkan Kennedy'nin öldürülmesi, suçlusunun bulunamaması kamuoyunda tansiyonu artırmış, insanlar güvensiz bir toplumda yaşadıklarına inanmaya ya da inandırılmaya başlamışlardır[113].

Berger ve Katz davalarının görüldüğü günlerde yaklaşık 70 milyon telefon hattına sahip olan ABD'de[114], Kongre, 1968 yılında Wiretap and Electronic Surveillence Act olarak adlandırılan ancak, Çok Yönlü Suçla Mücadele ve Güvenli Sokaklar Kanunu'nun 3. Bölümü olarak kanunlaştırıldığı için Teknik Dinleme Kanunu (Bölüm III) olarak bilinen

[111] THE USA PATRIOT ACT, EPIC Report.

[112] 50 U.S.C. & 1803(a) bu madde ile Patriot Kanunu'nun 208. maddesiyle değiştirilmiştir. Bk. KHAN, s.70.

[113] ÖZDOĞAN, (2004), s. 27-28.

[114] DONOHUE, s. 5.

yasayı çıkarmıştır[115]. Bu Kanun, Suçlar ve Cezai Usul (Crimes and Criminal Procedure) isimli 18 nolu başlık[116] altında düzenlenmiştir[117].

Teknik Dinleme Kanunu, ABD Anayasa'sının 4. bölümünde arama ve elkoyma tedbirleri için öngörülenlerden daha ağır şartlar koymuştur. Bunlar neticesinde birtakım cezai ve sivil yaptırımlar öngörülmüş, bunun yanı sıra bu kurallara riayet edilmeden elde edilen bilgilerin delil sayılmaması gibi birtakım hukuki sonuçlar da ortaya konulmuştur. Böylece, aslında Anayasa'nın 4. maddesinde sayılan şartları taşıyan bir usuli işlemden elde edilen bilgiler, 1968 Kanunu'ndaki şartları karşılamadığı için geçersiz sayılmıştır[118].

1.2.1.2. Tanım ve Kapsam

ABD'deki ilk geniş kapsamlı iletişimin denetlenmesi kanunu olarak kabul edilen[119] ve Berger davasında Yüksek Mahkemenin eksiklik olarak belirlediği durumlar ile yaptığı tespitlerden yola çıkılarak hazırlanmış bir metin[120] olan Teknik Dinleme Kanunu'nun

---

[115] Omnibus Crime Control And Safe Streets Act, Public Law 90-351; 82 Stat. 197 [H. R. 5037], June 19 P.L. 90-351. İET: 16.11.2007, http://www.fcc.gov/Bureaus/OSEC/library/legislative_histories/1615.pdf Kanun başlığının altında 'An Act to assist State and local governments in reducing the incidence of crime, to increase the effectiveness, fairness, and coordination of law enforcement and criminal justice systems at all levels of government, and for other purposes' (Eyalet ve yerel yönetim yetkililerine suçların azaltılması; hükümetin tüm merciilerinde kolluğun ve ceza sisteminin koordinasyonun, adaletinin ve etkinliğinin artırılması ve diğer amaçlar için akdedilmiş bir kanun) ifadesine yer verilmiştir; DEMPSEY, "Communications Privacy In The Digital Age: Revitalizing The Federal Wiretap Laws To Enhance Privacy".

[116] Bu 51 başlığa ((http://www.law.cornell.edu/uscode/ adresi marifetiyle ulaşılabilmektedir. Başlıklar şunlardır: Title 1 General Provisions, Title 2 The Congress, Title 3 The President, Title 4 Flag and Seal, Seat Of Government,and the States, Title 5 Government Organization and Employees, Appendix to Title 5 , Title 6 Domestic Security, Title 7 Agriculture, Title 8 Aliens and Nationality, Title 9 Arbitration, Title 10 Armed Forces, Appendix to Title 10 (Rules of Court of Appeals for the Armed Forces), Title 11 Bankruptcy, Appendix to Title 11, Title 12 Banks and Banking, Title 13 Census, Title 14 Coast Guard, Title 15 Commerce and Trade, Title 16 Conservation, Title 17 Copyrights, Title 18 Crimes and Criminal Procedure, Appendix to Title 18, Title 19 Customs Duties, Title 20 Education, Title 21 Food and Drugs, Title 22 Foreign Relations and Intercourse, Title 23 Highways, Title 24 Hospitals and Asylums, Title 25 Indians, Title 26 Internal Revenue Code, Appendix to Title 26, Title 27 Intoxicating Liquors, Title 28 Judiciary and Judicial Procedure, Appendix to Title 28, Title 29 Labor, Title 30 Mineral Lands and Mining, Title 31 Money and Finance, Title 32 National Guard, Title 33 Navigation and Navigable Waters, Title 34 Navy (repealed), Title 35 Patents, Title 36 Patriotic Societies and Observances, Title 37 Pay and Allowances Of the Uniformed Services, Title 38 Veterans' Benefits, Appendix to Title 38 (Rules of Court of Appeals for Veterans Claims(), Title 39 Postal Service, Title 40 Public Buildings, Property, and Works, Title 41 Public Contracts, Title 42 The Public Health and Welfare, Title 43 Public Lands, Title 44 Public Printing and Documents, Title 45 Railroads, Title 46 Shipping, Appendix to Title 46, Title 47 Telegraphs, Telephones, and Radiotelegraphs, Title 48 Territories and Insular Possessions, Title 49 Transportation, Title 50 War and National Defense, Appendix to Title 50 .

[117] Title 18 > Part I > Chapter 119, (Wire And Electronic Communications Interception And Interception Of Oral Communications), 2510-2522. maddeleri arasında düzenlenmiştir. http://www4.law. cornell.edu/ uscode/html/uscode18/usc_sup_01_18_10_I_20_119.html (16.8.2007).

[118] AN OVERVIEW OF ELECTRONIC SURVEILLANCE: History and Current Status.

[119] ÖZDOĞAN, (2004), s. 14.

[120] Bk. STEVENS/DOYLE, s.6.

(Bölüm III) çıkarılmasındaki temel gaye, gerek telli gerekse telsiz (dogrudan ağızdan çıkan konuşmaların) mahremiyetini korumak ve bu konuşmaların devlet tarafından dinlenmesi hususunu ülke genelinde belli standartlara bağlamaktır[121].

Teknik Dinleme Kanunu'nun çatısı, Berger davasına konu olan New York Eyaleti Ceza Usul Kanunu'nun 813. maddesine yönelik eleştirilerden yararlanılarak kurulmuştur. Yüksek Mahkeme, anılan kararda, iletişiminin denetlenmesi tedbirine konu olacak yere ve suça[122] ilişkin, ayrıca suçun işlendiğini veya işlenmekte olduğunu gösterecek yeterli açıklama[123] olmadığı ve aramayı genel olmaktan çıkaracak sınırlandırmaların bulunmadığı eleştirisini getirmektedir. Mahkemeye göre, bunun yanı sıra, iletişimin ne kadar bir süre zarfında denetleneceği ve tedbirin bitiş tarihi belirtilmemiş, tedbirin bitirilmesi kolluk görevlisine bırakılmış[124], mahkeme kararının bir an önce yerine getirilmesi öngörülmemiş[125], mahkeme kararına ilişkin sürenin uzatılması için sadece 'kamu yararı' yeterli sayılmış, tedbirin uzatılması için makul sebeplerin olup olmadığı hususu izah edilmemiş[126], tedbirin ilgiliye bildirimine ilişkin bir düzenleme bulunmadığı gibi, gizlilik gibi birtakım zorlayıcı nedenlerin (exigent circumstances) varlığı nedeniyle bildirimin yapılmadığı gibi bir gerekçe belirtilmemiş[127], denetleme süreci ve sonuçları hakkında yargıya rapor verme zorunluluğu getirilmemiş, böylece yargının iletişimin denetlenmesi tedbirine ilişkin kontrolü yeterince yapması sağlanmamıştır[128]. Mahkeme, iletişimin denetlenmesi tedbirinin kullanılabilecegi suç tipi için "yeterli sebep" şartının da belirtilmediğini ve aynı şüphelinin mahkeme kararında belirtilmeyen suçları için de yine aynı Mahkeme kararı ile dinleme yapılabildiğini göz önüne sermekte, yani mahkeme kararında belirtilmeyen durumlar için de, bu mahkeme kararı kullanılarak dinleme yapılabildiğini vurgulamaktadır[129].

---

[121] KHAN, s. 66; ÖZDOĞAN, (2004), s. 14.

[122] Mahkemenin 'suça ilişkin açıklama' ile kastı, hususilik prensibinin (particularity principle) yani, denetlemenin sadece suça taalluk eden durumlara ilişkin olabileceği hususunun öngörülmemiş olmasıdır. 18 U.S.C. § 2516.

[123] BERGER-NEW YORK, 388, Pr. 55-58.

[124] BERGER -NEW YORK, 388, Pr.59.

[125] BERGER-NEW YORK, 388, Pr.59.

[126] BERGER-NEW YORK, 388, Pr. 59.

[127] BERGER-NEW YORK, 388, Pr.60; Şüpheliye, dinleme sonrasında telefonunun dinlendiği bilgisinin verilmemesi, sanığın mahkemede kendi aleyhine delil olarak kullanılacak bilgilerden haberdar olamaması gibi bir sonuç doğurmaktadır ki bu durum iddia ve savunma taraflarının eşit imkanlara sahip olması (equality of arms) prensibini, dolayısıyla adil yargılanma ilkesini ihlal etmektedir. (ÖZDOĞAN(2004),s. 11.

[128] ÖZDOĞAN(2004),s. 12.

[129] ÖZDOĞAN (2004),s. 11.

Söz konusu karardaki eleştiriler dikkate alınarak hazırlanan Teknik Dinleme Kanunu'nda yer alan temel prensipler bugün de güncel kanunlarda yer alan ilkelere ışık tutar niteliktedir. Bu ilkelerden bazıları şunlardır[130].

1. Sadece kanunla belirlenmiş suçlar hakkında yapılacak soruşturmalarda, bu tedbire başvurulabilir[131]. (Hususilik ilkesi-Particularity requirement).

2. Kullanılabilecek başka soruşturma yöntemlerinin varlığı halinde iletişimin denetlenmesi yöntemlerine başvurulmamalıdır[132]. (Son çare ilkesi-Exhaustion requirement).

3. İletişimin denetlenebilmesi tedbirine başvurulabilmesi için yeterli ve makul sebeplerin varlığı olmazsa olmaz bir şarttır[133]. (Makul sebep ilkesi-Probable cause requirement).

4. İletişime mahkeme kararı olmadan yapılan müdahale kanun dışıdır[134].

5. Anayasa hükmü uyarınca, hakkında iletişimin denetlenmesi kararı verilmiş kişinin suç unsuru ihtiva etmeyen konuşmalarının kayda alınması en aza indirgenmelidir. (En aza indirgeme ilkesi-Minimization requirement).

6. İletişimin denetlenmesi sonrasında, tedbire başvurulduğu keyfiyeti şüpheliye bildirilmelidir.

7. Yeterli sebeplerle desteklenmemiş mahkeme onayı ile veya mahkeme onayı olmaksızın yapılan dinlemelerden elde edilen deliller yargı sürecinde kullanılamaz[135].(Delil Yasağı ilkesi-Exclusion principle)

Teknik Dinleme Kanunu, iletişimin yasal olarak denetlenmesine (intercept)[136] imkan tanıyan, bireylerin iletişime müdahalelerini yasaklarken kolluk kuvvetlerinin anayasal

---

[130] DEMPSEY, "Communications Privacy In The Digital Age: Revitalizing The Federal Wiretap Laws To Enhance Privacy"; ÖZDOĞAN, (2004), s. 14-15.

[131] 18 U.S.C. § 2516.

[132] 18 U.S.C. § 2518(3).

[133] 18 U.S.C. § 2518(3)(b).

[134] 18 U.S.C. § 2518(4).

[135] 18 U.S.C. §2518(10).

[136] 18 U.S.C. § 2510(4)'te 'Intercept' ifadesi içeriğin elde edilmesi (acquisition of the contents) olarak tanımlanmıştır. Bk. http://www4.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00002510----000-.html#FN-1#FN-1.

denetimine yetki veren[137] ve iletişimin yasal denetlenmesi dışındaki tüm diğer müdahaleleri yasadışı ilan eden ilk spesifik kanundur. Bu kanun çıkarıldığı tarihe kadar yasadışı yöntemlerle yapılan iletişime müdahaleyi yasal bir zemine oturtmuş ve anayasal kontrol mekanizmalarını harekete geçirerek keyfiliğin sona erdirilmesi sürecini tetiklemiştir[138].

Özel hayatın korunması ile kolluk görevinin ifası arasında bir denge kurmayı amaçlayan Kanun[139]; iletişimin mahremiyetinin korunmasını sağlarken, iletişimin denetlenmesine ilişkin yeknesak şartların ve durumların belirlenmesini sağlamaya da çalışmıştır[140]. Polis gücü karşısında bireysel mahremiyetin önemini vurgulayan bir düzenleme olan bu hukuksal metin, hem federal hem de eyalet bazında önemli bir düzenleme olarak kabul edilmektedir. Federal düzeyde, teknolojik gelişmelerin tehdit ettiği mahremiyete ilişkin olarak anayasal koruma ötesinde bir koruma getirmiştir. Eyalet bazında ise, en aza indirgenme (minimisation) şartını ortaya koymuştur[141].

Kanunda yer alan 'intercept' ifadesi ile kastedilen 'elektronik, mekanik veya başka bir cihaz marifetiyle kablolu, elektronik veya sözlü iletişime ilişkin içeriğin dinlenmesi veya başka bir süretle elde edilmesidir[142]. Katz ve Berger kararlarıyla çizilen hedefin ötesine geçen ve iletişimin güncel içeriklerine ilişkin düzenleme getiren kanunun[143] temas ettiği 'içerik' terimi, 'iletişim taraflarının kimliklerine veya iletişimin varlığına, özüne, amacına veya anlamına ilişkin herhangi bir bilgi'[144] anlamında kullanılmıştır. Diğer bir ifadeyle, 'intercept' ifadesi, gerçek zamanlı denetlemeler için geçerli olup, depolanmış kablolu veya elektronik iletişime teşmil edilemez[145].

---

[137] 9-7.000, Electronic Surveillance, (USDOJ Electronic Surveillence) (İET:11.9.2007), http://www.Usdoj .gov/ usao/eousa/foia_reading_room/usam/title9/7mcrm.htm.

[138] AN OVERVIEW OF ELECTRONIC SURVEILLANCE: History and Current Status.

[139] STEVENS/DOYLE, s.7.

[140] DEMPSEY, "Communications Privacy In The Digital Age: Revitalizing The Federal Wiretap Laws To Enhance Privacy".

[141] MADDOX, Laurie M.; "Criminal Procedure, Search and Seizure- Interception of Cordless Telephone Communication Does Not Violate Title III of Omnibus Crime Control Act of 1968", Missisipi Law Journal, Heinonline, -- 54 Mss.339,:1984, s.348.

[142] Elektronik iletişim 1986 tarihli ECPA Kanunu çerçevesinde bu kanun kapsamına alınmıştır. (WONG, 3.2.5.)

[143] DONOHUE, s. 8; DEPARTMENT OF JUSTICE.

[144] 'any information concerning the identity of the parties to such communication of the parties to such communication or the existence, substance, purport, or meaning of that communication'(18 U.S.C. §2510(8)); SCHWARTZ: The Pen Register Act, The Statute.

[145] DEPARTMENT OF JUSTICE: Report of the U.S. Department Of Justice, Office of Legislative Affairs, 26.7.2002, http://www.lifeandliberty.gov/subs/congress/hjcpatriotactcombinedresponses3. ; SCHWARTZ,

Adresleme bilgisi ile içerik bilgisinin[146] tespiti hakkında uygulanacak kanunlar farklıdır. Teknik Dinleme Kanunu, hükümet görevlilerine gerçek zamanlı olan ve depo edilmemiş kablolu ya da elektronik iletişim içeriğini denetleme imkanı tanımakta iken, Numara ve Rota Tespit Kanunu[147] ise bu tür haberleşmelerde gerçek zamanlı olmak kaydıyla adresleme bilgilerini ve içeriğe ilişkin olmayan bilgileri tespit etme ile ilgili hükümler ihtiva etmektedir[148]. Bu bağlamda, numara ve rota tespit cihazlarının[149] kullanılması Teknik Dinleme Kanunu anlamında yaptırıma bağlanmış değildir[150].

Teknik Dinleme Kanunu, sözlü, elektronik ve kablolu iletişimin tanımlarını da içermektedir. Sözlü iletişim[151], müdahale edilmeyeceğine ilişkin bir inanç ile bir kimseden sadır olan her türlü sözlü haberleşmeye denir. Elektronik iletişim[152] ise; her türlü işaret, sinyal, yazı, ses, veri, görüntü veya bilginin kablo, radyo, elektomanyetik, fotoelektronik ya da fotooptik bir sistem vasıtasıyla iletilmesidir[153].

Kablolu iletişim, insan sesinin kablo veya kablo benzeri iletim materyalleri ile aktarılmasıdır. Fiber optik de bu kapsamdadır. Tanıma bakıldığında öne çıkan en önemli unsur, iletişimin içeriğinin insan sesi içermesidir. Nitekim, işitsel transfer (aural

---

Paul M.: 2007, 2.The Statistics; "Reviving Telecommunications Surveillance Law", University Chicago Law School Surveillance Symposium (June 2007), http://www. law.uchicago. edu/Lawecon/ events/schwartz.pdf , (iET:16.11.2007); 18 U.S.C. § 2510 maddesinde yer alan "electronic communications" aktrarmayı (transfer) kapsama almışken, depolanmış bilgileri(storage) kanunun haricinde tutmuştur.Diğer bir ifadeyle içerik gerçek zamanlı başka bir ifadeyle iletimi ile eşzamanlı(contemporaneous with its transmission) olmalıdır. Bk. SCHWARTZ, Dp. 11.

[146] Adresleme bilgisi ile içerik bilgisi arasındaki fark net bir şekilde ortaya konabilmektedir. Bir telefon görüşmesinde adresleme bilgisi, aranan numara ile gelen numarasına (çağrı numarası) ilişkin bilgilerdir. İçerik bilgisi ile kastedilen ise, taraflar arasında gerçekleşen haberleşmenin bizatihi kendisidir. Adresleme bilgisi ve içerik bilgisi arasındaki fark İnternet haberleşmelerinde ve elektronik postada da benzer bir şekilde tespit edilmektedir. (DEPARTMENT OF JUSTICE; Content and Address Information).

[147] Ayrıntılı bilgli için bk. Numara ve Rota Tespit Kanunu ile ilgili Altbölüm.

[148]DEPARTMENT OF JUSTICE; MADDOX, Dp. 44.

[149] Telefon numarası tespit cihazlarının Teknik Dinleme Kanunu kapsamına giren cihazlardan farkını gösteren mahkeme kararları: United States Telecom Ass'n-FCC, 227 F.3d 450, 454 (D.C. Cir. 2000) ile Brown v. Waddell, 50 F.3d 285, 289-94 (4th Cir. 1995) Bk.DEPARTMENT OF JUSTICE.

[150] 18 U.S.C. § 2511(h)(i).

[151] 18 U.S.C. § 2510 (2) "oral communication" means any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication.

[152] 18 U.S.C. § 2510(12). "electronic communication" means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system.

[153] Sözlü iletişim konuşulan kelimelerin ses dalgaları ve hava vasıtasıyla iletimine denir. Sözlü iletişimin elektronik takibi böcek(bug) olarak tabir edilen cihazlar vasıtasıyla yapılmaktadır. Elektronik ortamda iletilen veri, metin, ses ve video da dahil olmak üzere her türlü haberleşmeye elektronik iletişim denilmektedir. ECPA ses içeren radyo iletişimini elektronik olarak nitelemektedir. Ancak iletişim kısmen radyo kısmen de mobil telefon gibi kablolu cihazlarla iletilmişse bu halde bu iletişim kablolu olarak addedilmektedir(AN OVERVIEW OF ELECTRONIC SURVEILLANCE: History and Current Status).

transfer) kavramı, kanunda 'insan sesi ihtiva eden transfer'[154] olarak tanımlanmıştır. Bu bağlamda, insan sesi içermeyen iletişim, gerek tekil olsun gerekse bir gruba ait olsun kablolu iletişim olarak tanımlanamayacaktır[155]. Tanımdaki ikinci önemli unsur, kablo veya diğer benzeri bağlantılar marifetiyle orjin ile kabul eden noktalar arasında gidip gelen sinyallerin varlığıdır. Bu bağlamda, uydu sinyalleri içeren telefon görüşmeleri gibi kablosuz görüşmeler[156] ve cep telefon görüşmeleri kablolu iletişim olarak değerlendirilmektedir[157].

1.2.1.3. Denetlemeye Konu Katalog Suçlar

Teknik Dinleme Kanunu'nun kaleme alınmasının asıl nedeni, organize suçlarla mücadele etmek düşüncesidir[158]. Bu amaca yönelik olarak, Teknik Dinleme Kanunu'nun orijinal metninde teknik dinlemenin bir soruşturma yöntemi olarak kullanılmasına imkan tanıyan 26 suç türü, genellikle organize suç ve ulusal güvenliği ilgilendiren ağır[159] federal[160] suçlar idi[161]. Ancak bu suçların sayısı, kanuna yapılan eklemelerle 100 civarına ulaşmıstır. Bahse konu suçların yanında, en az 1 yıl hapsi gerektiren suçlar ile ölüm cezasını müstelzim suçların da soruşturulmasında teknik dinleme kullanılabilir[162].

---

[154] 18 U.S.C. § 2510(18).

[155] DEPARTMENT OF JUSTICE, Wire Communication.

[156] Yapılan yasal değişiklik öncesinde verilmiş State-Delaurier (1985) kararında, Rhode Island Eyaleti Yüksek Mahkemesi, kablosuz telefon ile yapılan telefon görüşmelerinde "makul mahremiyet beklentisi"nin (Reasonable expectation of privacy) olamayacağı şeklinde bir sonuca varmıştır. Mahkeme bu şekilde bir yargıya varmasının nedenini ilginç bir noktaya dayandırmıştır. Mahkemeye göre, bu telefonlarla yapılan görüşmelerde mahremiyetin korunmasının garanti edilmediği hususu, tüm kablosuz telefonların beraberinde tüketiciye verilen broşürde açıkça belirtilmiştir. Gerçekten de, kablosuz telefonlarla birlikte tüketiciye sunulan kullanım kılavuzunda, 'bu telefonla yapılan görüşmelerin mahremiyetinin korunduğu garanti edilemez' ibaresinin bulunması yasal bir zorunluluktur. Bu ibarenin bulunmaması ürünün satışa sunulamaması gibi bir sonucu doğurmaktadır (ÖZDOĞAN, (2004), s. 17.

[157] DEPARTMENT OF JUSTICE, Intercept; Sözlü iletişim konuşulan kelimelerin ses dalgaları ve hava vasıtasıyla iletimine denir. Sözlü iletişimin elektronik takibi böcek(bug) olarak tabir edilen cihazlar vasıtasıyla yapılmaktadır. Kablolu iletişim insan sesinin kablo veya kablo benzeri iletim materyalleri ile aktarılmasıdır. Fiber optik de bu kapsamdadır. Elektronik ortamda iletilen veri, metin, ses ve video da dahil olmak üzere her türlü haberleşmeye elektronik iletişim denilmektedir. ECPA ses içeren radyo iletişimini elektronik olarak nitelemektedir. Ancak iletişim kısmen radyo kısmen de mobil telefon gibi kablolu cihazlarla iletilmişse bu halde bu iletişim kablolu olarak addedilmektedir. (AN OVERVIEW OF ELECTRONIC SURVEILLANCE: History and Current Status.).

[158] ÖZDOĞAN, (2004), s.30.

[159] AN OVERVIEW OF ELECTRONIC SURVEILLANCE: History and Current Status, D.1.1; DEMPSEY, "Communications Privacy In The Digital Age: Revitalizing The Federal Wiretap Laws To Enhance Privacy".

[160] STEVENS/DOYLE, s. 37.

[161] Bk. KHAN, s.69.

[162] DONOHUE, s. 8.

ABD kanun külliyatında 18 nolu başlık altında düzenlenen 2516 nolu bölümde iletişimin denetlenmesi tedbirine konu olabilecek suçlar sayılmıştır. 1968 tarihinde belirlenen suç sayısının çok arttığı ve hemen her suçun bu önemli tedbir kapsamına alındığı görülmektedir.

Bu suçlar aşağıdaki gibidir[163]:

a) 42 no'lu başlığın 2122 no'lu bölümü(section) ile 2274-2277 no'lu bölümlerinde düzenlenen ve ölüm cezasını veya bir yıldan fazla hapsi gerektiren suçlar: 1954 tarihli Atom Enerjisi Kanununa muhalefet suçları (42 no'lu başlık), Nükleer veya Petrol Tesislerine sabotaj suçları, (42 no'lu başlık),

42 no'lu başlık altında düzenlenen;

Casusluk suçları (Chapter 37), adam kaçırma suçları (chapter 55), ticari sırların korunması (chapter 90), sabotaj suçları (chapter 105), vatana ihanet suçları (chapter 115), isyan (chapter 102), başkasının malına zarar verme (chapter 65), gemilerin tahribi (chapter 111), mahremiyeti ihlal (chapter 81) suçları;

(b) 29. no'lu başlıkta düzenlenen işçi örgütlerinin ödemelerini sınırlandırma suçları ile yine bu başlık altında düzenlenen ve cinayet, adam kaçırma, gasp veya haraç içeren suçlar,

c) 18 no'lu başlıkta düzenlenen, section 201 (kamu görevlilerine ve tanıklara rüşvet), section 215 (banka görevlilerine rüşvet), section 224 (spor müsabakalarında rüşvet), section 844 (yasadışı patlayıcı kullanımı), section 1032 (vergi kaçakçılığına matuf mal gizleme), section 1084 (bahis bilgilerinin iletimi), section 751 (firar), section 1014 (alacak ve borç başvuruları ile bunların yenilenmesi ve tenzilatı ilgili suçlar), sections 1503, 1512, and 1513 (kamu görevlisini, jüri üyesini veya tanığı etkileme ve mutazarrır etme), section 1510 (ceza soruşturmasını engelleme), section 1511 (Eyalet veya yerel yönetim görevlisini engelleme), section 1591 (çocukların zorla, şiddetle veya hile ile seks trafiğine zorlanması), section 1751 (Başkan veya başkanlık görevlilerine yönelik suikast, adam kaçırma ve saldırı), section 1951 (tehdit ve şiddet marifetiyle ticarete müdahale), section 1952 (şirketlere şantaj amacıyla eyaletlerarası ve yabancı seyahat ile transport), section 1958 (kiralık katil sözleşmesi kapsamında eyaletlerarası ticareti

[163] Bk. 18 U.S.C. § 2516 http://www.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00002516----000-.html (İET:2.12.2007) (Maddenin numaralandırma stili aynen alınmış, maddeler asıllarına bağlı kalınarak tercüme edilmiştir.).

kullanma), section 1959 (şantajla bağlantılı şiddet içeren suçlar), section 1954 (işçi yararına -employee benefit plan- gerçekleştirilen operasyonları nüfuz amaçlı teklif, Kabul ve aracılık), section 1955 (kumar işletmelerinin yasaklanması), section 1956 (kara para aklama), section 1957 (belli yasadışı faaliyetlerden elde edilmiş mallarla ilgili parasal işlemlerde bulunmak), section 659 (eyaletlerarası kargo hırsızlığı), section 664 (emekli aylığı ve sosyal fonlara ilişkin zimmet), section 1343 (kablolu cihazlar, radyo ve televizyon marifetiyle dolandırıcılık), section 1344 (banka dolandırıcılığı), sections 2251 and 2252 (çocukların cinsel sömürüsü), section 2251A (çocuk ticareti), section 2252A (çocuk pornografisi içeren materyallere ilişkin suçlar), section 1466A (çocuk müstehcenliğine ilişkin suçlar), section 2260 (küçüklerin cinsel görüntülerinin ABD'ye ithal amacıyla üretimi), sections 2421, 2422, 2423, and 2425 (yasadışı cinsel faaliyetler ve ilgili suçlarla ilgili taşımacılık), sections 2312, 2313, 2314, and 2315 (eyaletlararası çalıntı mal taşımacılığı), section 2321 (belli motor araçlarının ve parçalarının kaçakçılığı), section 1203 (rehin alma suçları), section 1029 (erişim cihazları (access devices) dolandırıcılığı ve bağlantılı faaliyetler), section 3146 (mahkemede hazır bulunmama), section 3521 (b)(3) (tanık transferi ve yardımı), section 32 (uçak ve uçak tesislerinin tahribi), section 38 (uçak parçası sahteciliği -aircraft parts fraud-), section 1963 (şantaja maruz ve yolsuz örgütlere ilişkin ihlaller- violations with respect to racketeer influenced and corrupt organizations-), section 115 (bir federal görevli aleyhine tehdit ya da misilleme), section 1341 (posta dolandırıcılığı), section 1030 (bilgisayar sahteciliği ve suiistimali), section 351 (Kongre, Kabine ve Yüksek mahkeme üyelerine yönelik suikast, adam kaçırma ve saldırı), section 831 (nükleer madde içeren yasaklanmış işlemlerle ilişkili suçlar), section 33 (motorlu taşıtlar ve bunlara ilişkin tesislerin tahribi), section 175 (biyolojik silahlarla ilgili suçlar), section 175c (çiçek hastalığı virüsü ile ilgili suçlar), section 1992 (trenlerin tahribi ile ilgili suçlar), section 1028 (kimlik sahteciliğine ilişkin belge tanzimi), section 1425 (yasadışı olarak vatandaşlığa alma), section 1426 (vatandaşlık belgelerinin çoğaltılması -reproduction of naturalization or citizenship papers-), section 1427 (vatandaşlık belgelerinin satılması), section 1541 (yetkisiz pasaport tanzimi), section 1542 (pasaport başvurularında sahte beyanda bulunmak), section 1543 (pasaport sahteciliği), section 1544 (pasaport kullanımında suiistimal), or section 1546 (visa, izin belgesi ve diğer belgelerde suiistimal ve sahtecilik);

(d) kalpazanlık içeren suçlar (section 471, 472, or 473); (18 nolu başlık)

(e) 11 no'lu başlık kapsamındaki sahtecilik içeren suçlar ile narkotik maddeler, marihuana ve ABD'de suç sayılan diğer maddelerin üretimi, ithali, alımı, saklanması, satılması veya başka tür alışverişi;

(f) fahiş borç işlemleri içeren suçlar (sections 892, 893, or 894) (18 nolu başlık);

(g) parasal işlemlerin bildirilmesi (section 5322) (31 nolu başlık)

(h) belirli haberleşmelere müdahale ile bunların açıklanması, (sections 2511 and 2512) (18 nolu başlık)

(i) müstehcenlik (chapter 71) (18 nolu başlık)

(j) doğal gaz boruhatlarının tahribine ilişkin suçlar (section 60123) ile hava korsanlığı suçları(section 46502) (49 nolu başlık)

(k) Silah İhracatı Kontrol Kanununa muhalefet suçları (section 2778 of title 22)

(l) 2516 nolu bölümde sayılan suçlarla ilgili kanun kaçaklarının barındırılması -the location of any fugitive from justice from an offense described in this section-;

(m) Göçmenlik ve Vatandaşlık Kanununa muhalefet suçları (section 274, 277, or 278) (8 U.S.C. 1324, 1327, or 1328)(göçmen kaçakçılığı ile ilgili suçlar)

(n) ateşli silahlara ilişkin suçlar (sections 922 and 924) (18 nolu başlık);

(o) 1986 tarihli İç Gelir Kanunu'nun ihlali (ateşli silahlarla ilgili)(section 5861);

(p) sahte kimlik tanzimine ilişkin suçlar (section 1028), pasaport başvurularında sahte beyanda bulunmak (section 1542) viza, izin belgesi (permit) ve diğer belgelerde sahtecilik ve suiistimal suçları (section 1546) (18 nolu başlık) ile Göçmenlik ve Patriot Kanunu hükümlerinin ihlali (göçmen kaçakçılığı ile ilgili) (section 274, 277, or 278)

(q) kimyasal silahlarla ilgili suçlar (section 229) ile yine 18 nolu başlıkta düzenlenen terörizm suçları (section 2332, 2332a, 2332b, 2332d, 2332f, 2332g, 2332h, 2339A, 2339B, or 2339C)

(r) Bu paragrafta sayılan suçlardan herhangi birini işlemek amacıyla kurulmuş suç anlaşmasına (conspiracy) ilişkin suçlar

Resmi rakamlara göre, iletişimin denetlenmesi tedbirine en çok başvurulan suçların başında, uyuşturucu suçları gelmektedir. 2006 yılında, gerek eyalet gerekse federal düzeyde yapılan başvuruların yüzde 80'i uyuşturucu suçuyla ilgilidir. İkinci önemli

kategori ise, organize suçlar ile öldürme/saldırı suçlarıdır. Bu suçlar başvuruların yaklaşık yüzde 11'ine tekabül etmektedir[164].

1.2.1.4. Adli Amaçlı İletişimin Denetlenmesi Tedbirine Başvurmanın Koşulları

1.2.1.4.1. Makul Sebep

'Kablolu, Sözlü ve Elektronik İletişimin Denetlenmesi Usulu' (Procedure for interception of wire, oral, or electronic communications) başlıklı 2518 sayılı maddeye göre, iletişime müdahale edilebilmesi için Madde 2518(3)'e göre makul sebebin (Probable cause) varlığı şarttır[165].

Hakim, başvuruda belirtilen olgulara ilişkin bir değerlendirme yaparken iletişimin denetlenmesi tedbirini uygulamak amacıyla gerekli şartların varolup olmadığını anlayabilmek için aşağıdaki sorulara cevap arar:[166]

- İletişimi denetlenecek kişinin 2516 sayılı maddede belirtilen suçlardan birini işlediğini, işlemekte olduğunu veya işlemek üzere olduğunu gösteren makul sebepler var mıdır?[167]

- Bu tedbir marifetiyle soruşturma konusu suçlar hakkında belli delillerin elde edileceğine ilişkin makul sebepler bulunmakta mıdır?[168]

- Diğer soruşturma yöntemlerine başvurulmuş mudur? Bu yöntemlerin kullanıldığını ancak sonuç alınamadığını veya bu yöntemler kullanılmamış olmakla birlikte kullanılsa dahi sonuç alınamayacağını veya kullanılmasının çok tehlikeli olduğunu gösteren haller mevcut mudur[169]?

- Denetlenmeye konu olacak olan yerin bir suç bağlamında kullanıldığını, kullanılmakta olduğunu ve kullanılmak üzere olduğunu gösteren veya bu yerin iletişimi

---

[164] SCHWARTZ, The Statistics.2.

[165] DONOHUE, s. 8; DEPARTMENT OF JUSTICE, Interception Authorized by a Title III Order; AN OVERVİEW OF ELECTRONİC SURVEİLLANCE: History and Current Status, D.1.2; SCHWARTZ , A.1; EFF ANALYSIS OF PATRIOT ACT; DEMPSEY, "Communications Privacy In The Digital Age: Revitalizing The Federal Wiretap Laws To Enhance Privacy".

[166] ÖZDOĞAN, (2004), s. 33; SCHWARTZ, A.1; STEVENS/DOYLE, s. 39; EHRLICH, Tim: "Case study on Lawful Intercept, (Presented to: Harward Law School Cyber Law and The Global Economy", http:// cyber. law.harvard.edu/globaleconomy/lawful_intercept.pdf , (İET: 8.11.2007), s. 7-8; DONOHUE, s.8.

[167] 18 U.S.C. § (2518(3)(a)).

[168] 18 U.S.C. § 2518(3)(b).

[169] 18 U.S.C. § 2518(3)(c).

denetlenecek kişi tarafından kiralandığını, bu kişi adına kayıtlı olduğunu ya da bu kişi tarafından kullanıldılğını gösteren makul sebepler var mıdır[170]?

Hakim tarafından yukarıda belirtilen hususlarda yapılacak değerlendirme sonucunda denetlemeye ilişkin karar verilir.

1.2.1.4.2.Son Çare Prensibi

Son çare prensibinin (exhaustion requirement) uygulanması ile elde edilmek istenen amaç, dinlemenin kullanılacağı dava sayısını azaltmak ve özel hayata yönelik riskleri minimize etmektir. 2518(3) no'lu kanun maddesi, iletişimin denetlenmesi tedbirine başvurulabilmesi aşağıda sayılan şartların varlığını aramaktadır[171]:

1. İletişimin denetlenmesi dışındaki soruşturma yöntemleri kullanılmış ancak bu yöntemler başarısız olmuştur. Diğer bir ifadeyle bu yöntemlerden fayda elde etmek mümkün olamamıştır.

2. İletişimin denetlenmesi dışındaki yöntemlerin kullanılması durumunda başarı elde edilemeyeceğine ilişkin bir kanaat vardır.

3. İletişimin denetlenmesi dışındaki yöntemlerin kullanılması çok tehlikelidir.

Son çare ilkesinin uygulanması için aranacak şartların varlığı ve bu şartların oluştuğunun göstergesi olan makul sebebin tespiti, ortam ve amaca göre değişir. Bununla birlikte, bulunması gereken -olmazsa olmaz- koşul, şartların oluşması hakkındaki kanaatlerin makul temellere bina edilmesidir. Gerçekten de, Teknik Dinleme Kanunu'nda, makul desteğe dayanmayan kanaatlerin son çare prensibinin uygulanması için yeterli bulunmadığı vurgulanmıştır. Kolluk güçleri, bir soruşturma kapsamında elde ettikleri bilginin daha fazlasına ihtiyaç duyduklarında, bunu elde etmek için iletişimin denetlenmesine ihtiyaç duymaktadırlar. Yani aslında, başka yöntemlerle elde edilmiş bilgi ve belgelerin yeterli bulunmadığı şartlarda iletişimin denetlenmesine ihtiyaç duyulabilir[172].

---

[170] 18 U.S.C. § 2518(3)(d)).

[171] 18 U.S.C. § 2518(3); DONOHUE, s.8; AN OVERVIEW OF ELECTRONIC SURVEILLANCE: History and Current Status, D.1.2; ÖZDOĞAN, (2004),s. 33 ; EHRLICH, s. 8; DEMPSEY, "Communications Privacy In The Digital Age: Revitalizing The Federal Wiretap Laws To Enhance Privacy".

[172] ÖZDOĞAN, (2004), s. 35; DEMPSEY, "Communications Privacy In The Digital Age: Revitalizing The Federal Wiretap Laws To Enhance Privacy" .

Bu itibarla, öncelikli olarak, klasik soruşturma yöntemlerine başvurulmama gerekçeleri açıklanmalıdır. Giordiano[173] davasında, iletişimin denetlenmesi talebinde bulunan kolluk kuvvetleri, diğer soruşturma yöntemlerine niçin başvurulmadığını ve bu yöntemlerin kullanılmamasının nedenlerini açıklamak zorunda bırakılmıştır. Alternatif soruşturma yöntemleri, Teknik Dinleme Kanunu'nun kanunlaştırılması öncesindeki Kongre tartışma kayıtlarında ifade edilmiştir. Kongre'nin, iletişimin denetlenmesi dışında kabul ettiği alternatif soruşturma yöntemleri; fiziki takip, sorgulama, mülakat, arama, ve gizli polis veya ajan kullanmak suretiyle sızma olarak sıralanabilir. İletişimin denetlenmesi gerektiği iddiasıyla mahkemeye başvuran kolluk görevlisi, alternatif yöntemler yerine iletişimin denetlenmesi yöntemine başvurma gerekçesini mahkemeye izah etmek durumundadır. Bu açıklamayı yapılırken; kolluk güçlerinin, iletişimin denetlenmesi dışındaki soruşturma yöntemlerinin kullanıldığını ancak bu yöntemlerin başarısız olduğunu bildirmesi, ya da, bu yöntemlerin tehlikeli olduğu ya da kullanılması durumunda başarı elde edilemeyeceği hususlarında mahkemeyi ikna etmesi gerekmektedir[174].

Kanun koyucu, 'normal soruşturma usullerini' sayarken bunların arasına iletişimin denetlenmesini koymamıştır. Yüksek yargı da, bu tedbiri normal soruşturma usullerinden biri olarak görmemektedir. Nitekim, Giordano kararında, Yüksek Mahkeme, iletişimin dinlenmesini olağanüstü bir son çare olarak tanımlamıştır. Mahkemeye göre, iletişimin denetlenmesi şartlarına sıkı sıkıya bağlı kalınmalıdır ve gerekli olan bu şartlar olgunlaşmadan yapılan bir müdahale bir yaptırıma tabi tutulmalıdır. Bu yaptırım da, bu şekilde elde edilen delillerin imha edilmesidir[175]. Bununla birlikte, iletişimin denetlenmesine gelinceye kadar tüm diğer çareler denenmemiş olsa bile, iletişimin denetlenmesine ilişkin karar verilebilmektedir. Örneğin ABD-Garcia, kararında Mahkeme, elektronik takip için diğer tüm normal yolların tüketilmiş olmasının gerekli olmadığına karar vermiştir. Mahkeme, son çare prensibini, diğer geleneksel yollarda karşılaşılan güçlüklerin bildirilmesi olarak yorumlamıştır[176].

1.2.1.4.3.Kanunda Belirlenen Kişilerin Mahkeme Kararı için Başvurusu

---

[173] GIORDANO-ABD, 416 u.s. 505 (1974), 527-528, http://supreme.justia.com/us/416/505/case.html.

[174] ÖZDOĞAN, (2004), s. 33-35 ;DONOHUE, s.8.

[175] JUDGE/KALUNIAN/QUANT "Brief Overwiev of the WiretapLaw".

[176] DEMPSEY, "Communications Privacy In The Digital Age: Revitalizing The Federal Wiretap Laws To Enhance Privacy".

Teknik Dinleme Kanunu, federal düzeyde[177] iletişimin denetlenmesi kararı çıkarılabilmesi için, Adalet Bakanı (Attorney General[178]) veya emrindeki üst düzey görevlilerin[179] başvuru yapabileceklerini öngörmüştür[180].

Eyaletlerde ise, ilgili eyalet kanunlarının bu kişileri belirlemesi zorunluluğu getirilmiştir[181]. Bu bağlamda, eyalet Başsavcısı veya yetkilendirdiği kişiler başvuru yapabilirler[182]. Böylece farklı uygulamaların olması engellenebilecek ve uygulamada yeknesaklık sağlanacaktır. Bunun yanı sıra, bu kurumun ihdasıyla, yetkinin kötüye kullanılmasından doğacak sorumluluğu bir hiyerarşi zincirinin tepesinde olan kişinin yüklenmesi mümkün hale gelmiştir. Kongre, bu hükmün getirilmesiyle, görevin kötüye kullanılmasının engelleneceğine olan inancını ifade etmiştir. Yüksek Mahkeme, Giordano kararında, kanunla belirlenmiş yüksek görevlinin onayı olmaksızın yapılan bir başvuruyla elde edilen delillerin imha edilmesi gerektiğine karar vermiştir[183].

Teknik Dinleme Kanunu'nun en kısıtlayıcı hükümlerinden bir tanesi, federal soruşturma ajanslarının, iletişimin denetlenmesine ilişkin talebi, gözden geçirilmesi ve mahkemeye

---

[177] STEVENS/DOYLE, s. 37.

[178] Federal hükümette görev alan Genel Savcı (Attorney General) sıfatlı kişi, Senatonun onayıyla Başkan tarafından atanan ve bir kabine üyesi olan Adalet Bakanıdır. (28 U.S.C. § 503, http://www.law. cornell. edu/uscode/28/503.html İET:3.12.2007) Federal hükümetin taraf olduğu, federal mevzuatın yetki verdiği olaylarda federal soruşturmalar yapmanın yanı sıra, ülkedeki savcıları denetlemek fonksiyonunu da üstlenen Adalet Bakanı aynı zamanda FBI (Federal Bureau of Investigation) ve Adalet Bakanlığının diğer infaz operasyonları (law enforcement) üzerinde de bir denetim yetkisine sahiptir. Eyalet Genel Savcıları (State Attorney General) da benzer yetkilerle donatılmıştır. Başkan tarafından atanan Adalet Bakanından farklı olarak seçimle göreve gelen bu kişiler, eyalet düzeyindeki kovuşturmalar üzerindeki denetim yetkilerini, büyük çaplı kötü yönetim sergilenmediği takdirde pek kullanmazlar. Değişik kanunlarla, eyalet genel savcılarına çeşitli yetkiler verilmiştir. Bunların arasında, tüketicinin korunması, çevre hukukuna dair sorunlar, vakıfların ve kar amacı gütmeyen kuruluşların denetimi ve vatandaşların korunması bağlamında eyalet kanunlarının verdiği diğer yetkiler de vardır. 1789 tarihli 'The Judiciary Act' (ch. 20, sec. 35, 1 Stat. 73, 92-93) ile ihdas edilen Adalet Bakanlığı'nın 'Office of the Attorney General' görevleri arasında ise; Yüksek Mahkeme önündeki tüm davaların kovuşturulması ve davalara müdahil olunması, mahkeme başkanı tarafından sorulan sorular bağlamında başkan ve diğer kabine üyeleri (heads of departments) tarafından kanun hakkında ya da kendi alanları ile ilgili olarak sorulan sorular hakkında bilgi ve tavsiye vermek vardır. İşyükü her geçen gün daha arttığı için Adalet Bakanı adına çalışmakla görevlendirilmiş yardımcı sıfatlı kişilerin görevlendirilmesi gerekmiştir. http://www.usdoj.gov/02organizations/, Statutory Authority.

[179] Bu görevliler kanunda '…Deputy Attorney General, Associate Attorney General or any Assistant Attorney General, any acting Assistant Attorney General, or any Deputy Assistant Attorney General or acting Deputy Assistant Attorney General in the Criminal Division specially designated by the Attorney General' olarak sayılmıştır. Anglo Sakson sistemini benimsemiş bir ülke olan ABD'deki bu görevlerin tam karşılığı Ülkemizde bulunmadığı için tercüme edilmeden orjinal hali yazılmıştır. (18 U.S.C. § 2516(1)).

[180] DEPARTMENT OF JUSTICE, Interception Authorized by a Title III Order; AN OVERVIEW OF ELECTRONIC SURVEILLANCE: History and Current Status, D.1.2.

[181] 18 U.S.C. § 2516(2); 18 U.S.C. § 2511(2)(a)(ii)(B)).

[182] STEVENS/DOYLE, s. 38.

[183] GIORDANO-ABD, 416 u.s. 505 (1974), 527-528, http://supreme.justia.com/us/416/505/case.html .

sunulması hususunda onay verilmesi için Adalet Bakanlığına sunmasıdır[184]. Kanun[185], bu gözden geçirme ve onay verme yetkisini Adalet Bakanına vermiştir. Bakan da, bu yetkiyi sınırlı sayıdaki yetkiliye aktarmaktadır[186]. Gezici takip (roving tap) yetkisinin talep edileceği hallerde, Adalet Bakanı Yardımcısı veya Cezai Bölümden Sorumlu Adalet Bakan Yardımcısı Vekili (Acting Assistant Attorney General for the Criminal Division) bu gözden geçirme ve onay verme görevini kullanabilirler. Usulune uygun olmayan ya da yasadışı bir iletişimin denetlenmesi uygulamasından elde edilmiş delillerin kullanılması ve açıklanması, cezai, hukuksal ve idari yaptırımları ve ayrıca bilgilerin delil sıfatını kaybetmesini gündeme getireceğinden, Federal Savcıların ve kolluk görevlilerinin Adalet Bakanlığı onayının ne zaman ve nasıl işlediği konusunda yeterli bilgi sahibi olmaları şarttır[187].

1.2.1.4.4.Adli Amaçlı İletişimin Denetlenmesine İlişkin Mahkeme Kararı

İletişimin denetlenmesi tedbirine başvurulması, kişi hak ve hürriyetleri açısından ciddi riskleri barındırdığı için Teknik Dinleme Kanunu, dinlenilecek şüpheli hakkında makul sebeplerin oluştuğuna[188] ve bu tedbire başvurulmasının son çare olduğuna bir hakim tarafından karar verilmesini şart koşmuştur[189]. Kanunda belirtilen şartları taşıyan başvuru dilekçesi sonrasında, yetkili mahkeme; kablolu, sözlü ya da elektronik bir iletişimin denetlenmesine ilişkin kararını[190] verir. İletişimin denetlenmesi kararını verebilecek yetkili merci, federal mahkeme[191] ya da eyalet mahkemesi[192] hakimidir[193]. Teknik Dinleme Kanunu, iletişimin denetlenmesine ilişkin karar verebilecek yetkili

---

[184] USDOJ ELECTRONIC SURVEILLENCE, 9-7.100; EHRLICH, s.8.

[185] 18 U.S.C. § 2516(1).

[186] USDOJ ELECTRONIC SURVEILLENCE, 9-7.100.

[187] USDOJ ELECTRONIC SURVEILLENCE, 9-7.100.

[188] AN OVERVIEW OF ELECTRONIC SURVEILLANCE: History and Current Status, D.1.2.

[189] DONOHUE, s. 8 ; WONG, 3.3.2; Bk. STEVENS/DOYLE, s. 6.

[190] Teknik Dinleme Kanunu kapsamında verilen iletişimin denetlenmesi kararı 1997 yılında 1186 iken, bu rakam, 2006 yılında 1839'a yükselmiştir. Bu da, yüzde 55 civarında bir yükselme anlamına gelmektedir. Geçen onyıl içinde eyalet mahkemelerinden daha çok federal düzeyde verilen kararlarda bir artış meydana gelmiştir. "Intercept Orders Issued by Judges During Calendar Year 1997", http://www.uscourts. gov/ wiretap/table2.pdf (İET:10.10.2007) ; MECHAM, Leonidas Ralph: "Report of the Administrative Office of the United States Courts on Applications for Orders Authorizing or Approving the Interception of Wire, Oral, or Electronic ommunications", http://www.uscourts. gov/wiretap 06/Table22006.pdf (İET:10.10.2007).

[191] 18 U.S.C. § 2516(1).

[192] 18 U.S.C. § 2516(2).

[193] WONG, 3.2.2;

mahkemeyi 'Eyalet kanunlarının yetkili kıldığı genel ceza mahkemesi'[194] olarak tanımlamıştır[195].

Hakim, iletişimin denetlenmesine ilişkin karar verdiğinde iki ayrı belge düzenlemektedir. Bunlardan ilki, kolluk görevlisine iletişimin denetlenmesi yetkisi veren karar[196], diğeri de ilgili telekomünikasyon yetkilisinin kolluk görevlisine gerektiğinde yardım yapması için gerekli emir belgesidir[197].

Madde 2518(4)'te bir kararda olması gerekli olan bilgiler belirtilmiştir. Bu bilgiler şunlardır[198]:

- İlgililerin bilgisi dahilinde ise, iletişimin denetlenmesi tedbirine konu kişi(lerin) kimlik bilgi(leri)[199],
- İletişimin denetlenmesi tedbirine konu yerin adresi[200],
- Tedbire konu iletişim ve ilgili suç hakkında açıklama[201],
- Ne kadar süreyle dinleme yapılmak istendiği ve iletişime ilişkin tespit ve dinleme yapıldıktan sonra tedbirin kendiliğinden sona erip ermeyeceği hakkında bir açıklama[202],
- İletişimin denetlenmesi tedbirini uygulamaya yetkili kılınan organın ve başvuruya izin veren kişinin kimliği[203].

---

[194] 18 U.S.C. § 2510(9)(b).

[195] JUDGE/KALUNIAN/QUANT "Brief Overwiev of the WiretapLaw"; Federal Bölge Mahkemeleri (Federal District Courts) ve istinaf mahkemeleri (Courts Of Appeals) bu konuda karar almaya yetkilidirler. Halbuki arama kararları, daha alt düzeydeki mahkemeler olan 'federal magistrates' tarafından verilebilmektedir. Eyaletler, iletişimin denetlenmesine ilişkin kanunlarında eyalet yetkililerini belirlemek zorundadır. Teknik Dinleme Kanunu'nun yanı sıra, FBI ve çoğu eyalet ajansı, bu konuda görevlilerinin takip edeceği usulleri açıklayan iç yönergeleri belirlemişlerdir. (AN OVERVIEW OF ELECTRONIC SURVEILLANCE: History and Current Status, D.1.2).

[196] Federal düzeyde ve eyalet düzeyinde yapılan istatistikler sonucu, iletişimin denetlenmesine ilişkin olarak verilen kararların ülke genelinde bir homojenlik göstermediği görülmektedir. Örneğin 2006 rakamlarına göre, verilen kararların yüzde 59'u 4 eyalet mahkemesince verilmiştir.Kalifornia (430 karar), New York (377 karar), New Jersey (189 karar), and Florida (98 karar). Bk. 2006 REPORT OF THE DIRECTOR OF THE ADMINISTRATIVE OFFICE OF THE UNITED STATES COURTS ON APPLICATIONS FOR ORDERS AUTHORIZING OR APPROVING THE INTERCEPTION OF WIRE, ORAL, OR ELECTRONIC COMMUNICATIONS, 2007, http://www.uscourts.gov/wiretap06/2006WT.pdf (2006 REPORT OF THE DIRECTOR OF THE ADMINISTRATIVE OFFICE)(İET: 23.11.2007).

[197] ÖZDOĞAN, (2004), s.37.

[198] ÖZDOĞAN, (2004), s.37.

[199] 18 U.S.C. § 2518(4)(a) .

[200] 18 U.S.C. § 2518(4)(b).

[201] 18 U.S.C. § 2518(4)(c).

[202] 18 U.S.C. § 2518(4)(e).

Hakim, ABD sınırları içinde olmak kaydıyla mobil bir iletişim aracının da dinlenmesine karar verebilir. Yukarıda da ifade edildiği gibi, hakim, başvuruda belirtilen olgulara ilişkin bir değerlendirme yaparak[204], iletişimi denetlenecek kişinin 2516 sayılı maddede belirtilen suçlardan birini işlediğini, işlemekte olduğunu veya işlemek üzere olduğunu gösteren makul sebeplerin olup olmadığını[205], bu yöntemle delil elde edilebileceğine ilişkin yeterli sebeplerin bulunup bulunmadığını[206], bu tedbirin en son çare olarak kullanılıp kullanılmadığını[207] ve iletişim konusu cihazın ya da cihazın bulunduğu yerin suç bağlamında kullanıldığını, kullanılmakta olduğunu ve kullanılmak üzere olduğunu gösteren makul sebeplerin var olup olmadığını [208] değerlendirerek nihai kararını verir. İletişimin içeriğinin denetlenmesine ilişkin taleplerde, hakim taleple bağlı değildir. Başka bir anlatımla, hakim, kabul ya da red şeklinde karar verebilir[209]. Öte yandan, hakim kararıyla birden fazla telefon numarasının denetlenmesine karar verilebilir[210].

1.2.1.4.4.1. Mahkeme Kararı için Yapılacak Başvurunun Niteliği

İletişimin denetlenmesini talep eden kolluk görevlisi tarafından, yetkili hakime yazılı olarak ve yemin ya da yemin yerine geçen söz tahtında (affirmation) başvuru yapılması gerekmektedir[211]. 2518(1) no'lu maddeye göre, başvuru evrakında yer alması gerekli olan bilgiler şunlardır[212]:

- Soruşturmayı yapan kolluk görevlisinin ismi[213],
- Talepte bulunan görevlinin dayandığı ve bu tedbire başvurulmasının gerekli olduğunu gösteren eksiksiz bir açıklama.

Bu açıklamada bulunması gerekli olan detaylar ise şunlardır[214];

---

[203] 18 U.S.C. § 2518(4)(d).

[204] AN OVERVIEW OF ELECTRONIC SURVEILLANCE: History and Current Status.

[205] 18 U.S.C. § 2518(3)(a).

[206] 18 U.S.C. § 2518(3)(b).

[207] 18 U.S.C. § 2518(3)(c).

[208] 18 U.S.C. § 2518(3)(d)).

[209] AN OVERVIEW OF ELECTRONIC SURVEILLANCE: History and Current Status; Oysa ki, numara ve rota tespiti hakkında yapılan bir başvuru hakkında, kanunda belirtilen şartları taşımak kaydıyla, hakim olumlu karar vermek zorundadır.

[210] SCHWARTZ,The Statistics.2.

[211] 18 U.S.C. § 2518(1) ; DEPARTMENT OF JUSTICE, Interception Authorized by a Title III Order.

[212] Bk. AN OVERVİEW OF ELECTRONİC SURVEİLLANCE: History and Current Status, D.1.2.; STEVENS/DOYLE, s. 38-39.

[213] 18 U.S.C. § 2518(1)(a).

1. Denetime konu suçun işlendiğini, işlenmekte olduğunu veya işleneceğini gösteren ayrıntılar[215],

2. İletişimin denetleneceği yer veya cihaza ilişkin açıklama[216], denetime konu olacak iletişimin türüne ilişkin açıklama, (cep telefonu, sabit telefon, faks, modem, vs.),

3. Denetime konu olan şahıs(ların) kimlik bilgi(leri)[217].

4. Diğer soruşturma yöntemlerine başvurulup başvurulmadığına ya da diğer yöntemlerin kullanılıp da başarısız olunduğuna ilişkin bilgi. Bunun yanısıra, bu yöntemler kullanılmamış olmakla birlikte kullanılsa dahi sonuç alınamayacağını veya bu yöntemlerin kullanılmasının çok tehlikeli olduğunu gösteren bilgi[218].

5. İletişimin denetlenmesine ilişkin süre, denetlemenin ne kadar bir süre zarfında yapılacağı[219],

6. Denetlenmesi istenen yer veya kişi hakkında daha önceden vuku bulmuş bir talep bulunup bulunmadığı ve varsa bu hususta hakim tarafından verilen karar[220],

7. Süre uzatımına ilişkin bir başvurunun varlığı halinde, iletişimin denetlenmesi tedbirinden o tarihe kadar alınan sonuçlar veya o tarihe kadar sonuç alınamamasını haklı gösteren makul bir açıklama[221].

Hakim gerektiğinde, başvuruyu destekleyecek mahiyette birtakım ek belgelerin ibraz edilmesini de başvurandan talep edebilir[222].

1.2.1.4.4.2.Teknik Dinleme Kanunu Kapsamında Mahkeme Kararı Olmaksızın İletişimin Denetlenmesi

---

[214] 18 U.S.C. § 2518(1)(b).

[215] 18 U.S.C. § 2518(1)(b)(i).

[216] 18 U.S.C. § 2518(1)(b)(ii).

[217] 18 U.S.C. § 2518(1)(b)(iv).

[218] 18 U.S.C. § 2518(1)(c).

[219] 18 U.S.C. § 2518(1)(d).

[220] 18 U.S.C. § 2518(1)(e).

[221] 18 U.S.C. § 2518(1)(f).

[222] WONG, 3.3.4.

Devlet görevlilerinin bazı durumlarda mahkeme kararı olmaksızın dinleme yapmasına izin verilmiştir[223]. Bu haller, genellikle, dinlenilecek sahısların meşru ve makul olarak mahremiyet beklentilerinin olamayacağı durumlardır.

Bir kişiye yönelik hayati tehlikeyi veya ciddi fiziksel yaralanmayı**[224]**,

Milli güvenlik çıkarlarını tehdit eden bir komployu**[225]**,

Organize suçlarla ilgili bir komployu**[226]**,

içeren ve kablolu, sözlü veya elektronik iletişimin dinlenmesini gerektiren acil bir durumun varlığı halinde, mahkeme izni olmaksızın dinleme yapılabilir[227]. Bu uygulamanın Adalet Bakanı, Bakan Yardımcısı ve kanunda sayılan diğer kişiler tarafından devreye konulabilmesi için 2518 no'lu maddede sayılan şartların varlığı gerekmektedir**[228]**. Bu yetkinin kullanılabilmesi için iletişime yapılan müdahaleden itibaren 48 saat içinde mahkeme kararına ilişkin talebin yapılması gerekmektedir. Mahkeme kararının yokluğunda yapılan dinleme, hedeflenen dinleme içeriği elde edildiğinde veya mahkeme kararı için yapılan başvuru reddedildiğinde biter. Bu hallerden hangisi önce gerçekleşirse dinleme o zaman sona ermiş sayılır. Mahkemece onay verilmemesi veya mahkeme kararı elde edilmeden dinlemenin sona ermesi hallerinde, dinlemeyle elde edilen materyaller yasadışı olarak elde edilmiş sayılacaktır**[229]**. Mahkemeye 48 saat içinde iletilen ve başvuruyu destekler nitelikteki yeminli ve yazılı ifadede (affidavit); Adalet Bakanı veya yetkilendirilmiş kişilerin tedbir

---

[223] TITLE 50, CHAPTER 36,SUBCHAPTER I, § 1802, http://www4.law.cornell.edu /uscode/ html/ uscode 50/usc_sec_50_00001802----000-.html (İET:11.9.2007).

[224] 18 U.S.C. § 2518(7)(a)(i).

[225] 18 U.S.C. § 2518(7)(a)(ii).

[226] 18 U.S.C. § 2518(7)(a)(iii).

[227] Yakın nitelikte hayati tehlike, adam kaldırma, rehin alma vs. gibi haller, sayılan bu durumlar içerisinde acil bir denetleme kararını en çok gerektirecek hallerdir. USDOJ ELECTRONIC SURVEILLENCE, 9-7.112.

[228] Maddede ismi geçen yetkililer orijinal metinde '…any investigative or law enforcement officer, specially designated by the Attorney General, the Deputy Attorney General, the Associate Attorney General, or by the principal prosecuting attorney of any State or subdivision thereof acting pursuant to a statute of that State' olarak belirtilmiştir. Bu kavramların bazıları sistem farklılığı nedeniyle ülkemizde bulunmadığından tercüme edilmemiştir. 2518(7)(b).

[229] 18 U.S.C. § 2518(7) '… In the absence of an order, such interception shall immediately terminate when the communication sought is obtained or when the application for the order is denied, whichever is earlier. In the event such application for approval is denied, or in any other case where the interception is terminated without an order having been issued, the contents of any wire, oral, or electronic communication intercepted shall be treated as having been obtained in violation of this chapter, and an inventory shall be served as provided for in subsection (d) of this section on the person named in the application.'; ÖZDOĞAN, (2004), s. 42-43; USDOJ ELECTRONIC SURVEILLENCE, 9-7.112.

talebine konu olan olayla ilgili olarak bildiği hususlar ve durumun aciliyetini anlatan olgular izah edilir[230].

1.2.1.4.5.İletişim Aracı Belirtilmeksizin Bir Kişi Adına Çıkarılan Hakim Kararı

Teknik Dinleme Kanunu kapsamında, uyuşturucu ticareti gibi suçlar hakkında başlatılmış cezai soruşturmalar çerçevesinde uzun bir süreden beri başvurula gelen[231] gezici takip(roving tap) yöntemi, hakkında takibat yapılan ancak takipten kurtulmak için değişik yöntemlere başvuran kişiler hakkında gerekli şartların varlığı halinde uygulanmaktadır[232].

Bu tür bir kararın çıkarılması için, kanunda belirlenen kişiler[233] tarafından yapılmış bir talep bulunması önşarttır[234]. Gezici takip yönteminde, iletişimin denetlenmesi tedbiri bir ya da birden çok telefon numarası hakkında değil bir kişi hakkında verilmektedir[235]. Hakkında takip çıkarılan kişi tarafından kullanılan sabit telefon, cep telefonu ya da İnternet hesabı hakkında böyle bir karar çıkarılabilmesi için, bahse konu kişinin bir suç işlediği hakkında bir kanaat olması ve bunun başvuruda ifade edilmesi gerekmektedir. Aranan bir diğer şart ise, gezici takibe konu olacak kişinin belli bir cihazdan (facility) yapılacak denetlemeyi önlemeye yönelik iradesinin ve niyetinin bulunduğu hususunda makul ve yeterli sebepler bulunmasıdır[236].

Bu tür taleplerde önemli olan bir başka unsur da, hakkında gezici takip çıkarılacak kişinin, takip altına alınacak cihazın yakınında olduğunu gösteren belirtilerin bulunmasıdır. Bu hususlar anlaşıldığında, ilgili hakkında bu takibin çıkarılması mümkün olmaktadır[237].

---

[230] USDOJ ELECTRONIC SURVEILLENCE, 9-7.112.

[231] PATRIOT ACT FACT SHEET; 30 Mart 2005 tarihi itibariyle bu maddeye 49 defa başvurulmuş ve bu madde, özellikle uluslararası terörizm suçları ve casusluk suçlarında etkin olarak kullanılmıştır. (PATRIOT ACT FACT SHEET).

[232] WONG, 3.3.7; SCHWARTZ, The Statistics.2.

[233] The Attorney General, the Deputy Attorney General, the Associate Attorney General, an Assistant Attorney General, or an acting Assistant Attorney General. 18 U.S.C. § 2518(11)(a)(i) ve (b)(i).

[234] USDOJ ELECTRONIC SURVEILLENCE, 9-7.111.

[235] SCHWARTZ:,The Statistics. 2.

[236] 18 U.S.C. § 2518(11) (b)(ii); USDOJ ELECTRONIC SURVEILLENCE, 9-7.111.

[237] 18 U.S.C. § 2518(11) (b)(iv).

1.2.1.5. Süre

Mahkeme kararı ile verilebilecek tedbirin süresi en fazla 30 gündür. 2518(5) no'lu madde hükmüne göre, hedeflenen amacın elde edilmesine yeterli olacak süreden fazla bir zaman dilimi için bu tedbir öngörülemez ve bu tedbir hiçbir halde 30 günü geçemez[238]. Bu süre, tedbiri uygulayacak olan kolluk görevlisinin tedbiri başlattığı tarihten ya da her halükarda 10. günden itibaren başlar[239]. 2518(5) no'lu madde hükmü uyarınca mahkeme kararında belirtilen dinleme süresinin bitiminde denetleme sona erer. Denetlemenin uzatılması talep edildiği takdirde, 2518(3)'de belirlenen hallerin varlığı halinde ve 2518(1)no'lu maddeye göre hazırlanan yeni başvuru evrakıyla mahkemeye yeniden başvurulması gerekmektedir. Yetkili hakimin, başvuruyu kabul edilebilir bulması halinde dinleme süresi her başvuruda 30'ar gün uzatılır[240]. Her dinleme veya uzatma kararı mümkün olan en kısa süre içinde infaz edilmeli ve tedbirle elde edilmek istenen hedefe ulaşılmasıyla bitirilmelidir. Bu süre hiçbir halde 30 günü geçemez[241].

Denetlemeye konu olan iletişimin şifreli veya yabancı bir dilde olması halinde süreye ilişkin bir istisna uygulanır. Bu durumda, tedbir için öngörülen zaman zarfında bu şifreyi çözebilecek ya da yabancı dili bilen bir kişi olmaması halinde, dinlemenin en aza indirgenmesi prensibi çerçevesinde, olabilecek en kısa zaman diliminde[242] bu çözümleme yapılır. Bu bölüm tahtında yapılacak bir denetleme, bir hükümet görevlisinin denetimi altındaki bir sözleşmeli personel tarafından gerçekleştirilmelidir[243].

1.2.1.6. Denetlemenin En Aza İndirgenme Zorunluluğu

İletişimin denetlenmesi, fiziksel arama ve elkoymaya kıyasla özel hayatı daha fazla tehdit eden bir nitelik arz etmektedir. Gerçekten de, diğer tedbirler daha kısa bir zaman

---

[238] WONG, 3.3.10; EFF ANALYSIS OF PATRIOT ACT; EHRLICH, s. 8.

[239] Telefon numara tespit ve rota tespit cihazları için mahkeme kararı ile verilecek süre en fazla 60 gündür. Her müracaatta bu süre 60'ar günlük dilimlerle uzatılabilir.

[240] Mahkeme kararları sonucunda verilen iletişimin denetlenmesi kararları çerçevesinde yapılan dinlemeler artış eğilimi göstermektedir. Gerçekten de, 1980 yılında ortalama dinleme süresi 21 gün iken, bu rakam 1996 yılında 38 güne çıkmıştır. 1997 itibariyle en uzun süreli denetleme 420 gün sürmüştür. Günlük olarak denetlenen iletişim sayısı da 1058'den (1980) 1969'a (1996) çıkmıştır. DEMPSEY, "Communications Privacy In The Digital Age: Revitalizing The Federal Wiretap Laws To Enhance Privacy".

[241] 18 U.S.C. § 2518(5), ÖZDOĞAN, (2004), s. 37; EFF ANALYSIS OF PATRIOT ACT.

[242] 18 U.S.C. § 2518(5) '...In the event the intercepted communication is in a code or foreign language, and an expert in that foreign language or code is not reasonably available during the interception period, minimization may be accomplished as soon as practicable after such interception.'

[243] 18 U.S.C. § 2518(5).

diliminde gerçekleştirilmekte iken, iletişimin denetlenmesi doğası itibariyle belli bir zamana yayılmaktadır. Ortaya çıkması muhtemel diğer bir sakınca ise, müdahale esnasında denetlemenin amacıyla ilgisi olmayan konuların da takibe takılabilmesidir. Bu nedenle, Teknik Dinleme Kanunu müdahalenin en aza indirgenmesi (minimisation) prensibini benimsemiştir[244]. Eyaletlere[245], teknik dinleme ile ilgili kısıtlamalar yapma imkanı da sunulmuştur. Bu bağlamda, birçok eyalet kendi kanunlarını[246] federal kanunun öngördüğü sıkı şartlara bağlamıştır[247]. Teknik dinlemenin en aza indirgenmesi kuralına uyulmaması, elde edilen bilgilerin delil sıfatını kazanamaması gibi bir handikap doğurabileceğinden dolayı önemlidir[248].

İletişimin dinlenmesinin en aza indirilmesi prensibinde hedeflenen temel amaç, özel hayata müdahale riskini en aza indirmektir[249]. Bu husus son çare ilkesinde de geçerlidir. Madde 2518(5) uyarınca, iletişimin dinlenmesi esnasında mahkeme kararında belirtilen sınırların dışına çıkılmaması bakımından elden gelen gayret gösterilmelidir. Mahkeme kararında belirtilen sınırlar ifadesi kullanılırken kastedilen iki şey vardır. Bunlar[250] :

- Mahkeme kararında ismi geçmeyen kişilerin, mümkün olabildiği ölçüde denetleme kapsamına alınmamasına riayet edilmesi,

- Mahkeme kararında isimleri belirtilen kişilerin iletişimlerinin, sadece karar konusu suçlardan dolayı denetlenmelerinin sağlanması. (Bu kişilerin kararda belirtilmeyen suçları işlemeleri durumunda, kararda değinilmeyen suçlardan dolayı denetlemeye alınmalarının önlenmesi.)

Bununla birlikte, bahsedilen sınırlar içinde kalmak mevcut teknolojilerle pek mümkün değildir. Başka bir ifadeyle, en aza indirgenme prensibi, olması gereken ölçüde sıkı

---

[244]AN OVERVIEW OF ELECTRONIC SURVEILLANCE: History and Current Status, D.1.2; SCHWARTZ, A.1.

[245]2006 yılı itibariyle iletişimin denetlenmesi ile ilgili eyalet kanunlarını gösteren tablo için Bk. "Jurisdictions With Statutes Authorizing the Interception of Wire, Oral, or Electronic Communications Effective During the Period January 1 Through December 31 2006", http://www.uscourts.gov/wiretap06/Table1.pdf .

[246] 18 U.S.C. § 2516(2).

[247] DEMPSEY, "Communications Privacy In The Digital Age: Revitalizing The Federal Wiretap Laws To Enhance Privacy" (25 nolu sonnot).

[248] AN OVERVIEW OF ELECTRONIC SURVEILLANCE: History and Current Status, D.1.2.

[249] AN OVERVIEW OF ELECTRONIC SURVEILLANCE: History and Current Status, D.1.2.; EHRLICH, s. 8.

[250] ÖZDOĞAN, (2004), s. 38.

uygulanabilmiş değildir[251]. Nitekim, iletişimin denetlenmesi esnasında denetleme amacıyla ilgisi olmayan bilgilerin de ilgililerin bilgisi kapsamına girmesi muhtemeldir. Örneğin, hakkında dinleme kararı alınan bir kişinin konuşmalarından sadece suç unsuru bulunanlarının dinlenmesi, diğerlerinin ise ayıklanması sonucunu verecek bir filtrelemenin yapılması teknolojik olarak pek mümkün değildir. Bu hususta uygulayıcıların yaşadığı zorlukları hafifletmek amacıyla Yüksek Mahkeme, en aza indirme prensibini uygulamak hususunda dinlemeyi yapan memurun değerlendirmesine atıf yapmıştır. Bu bağlamda, dinlemeyi yapan memur, dinledikleri arasında suç unsuru olmayan konuşmaları kayıttan çıkarırsa veya yazılı metin haline getirmezse veyahut kimseye bildirmezse bu prensibi hayata geçirmiş olur denilmektedir[252].

Bazı davalarda, en aza indirgenme prensibi bir süreliğine ertelenebilir. Bu bağlamda, kayda alınan bilgilerin yabancı bir dilde olmasından dolayı tercüman getirtilmesi nedeniyle yaşanan bekleme ya da kripto (encrypted) metinler çözümlenmesi için beklenmesi bu duruma örnek verilebilir[253].

---

[251] DEMPSEY, "Communications Privacy In The Digital Age: Revitalizing The Federal Wiretap Laws To Enhance Privacy", SCOTT-ABD kararında Yüksek mahkeme konuşmaların tümünü dinleyip kayda alan kolluk görevlilerinin bu eylemlerini yasadışı bulmamıştır. Bu kararın verilmesinde etken olan hususlardan biri de bazen çok kısa süren konuşmalar esnasında bile kullanılan kodlu ifadelerdir. Scott davasının etkisi ABD-OZAR davasında da görülmüştür. Bu davada mahkeme, Adalet Bakanlığı görevlilerince uygulanan ve 'iki dakika dinleme, bir dakika mola' olarak da ifade edilebilecek "two minutes up/one minute down" tekniğine onay vermiştir. Bu olayda FBI, her üç dakikalık konuşmalardan iki dakikasını dinlemiştir. Toplam olarak denetlemeye takılan 8126 dakikanın 223 dakikasi yani % 2.75'i suçlamalarla ilgili bulunmuştur. İstinaf mahkemesi de, bu kararda bir hukuka aykırılık bulmamıştır. Mahkeme, Scott kararınından farklı olarak Ozar davasındaki konuşmaların uzun ve karmaşık olmasını gerekçe göstermiştir.(DEMPSEY, "Communications Privacy In The Digital Age: Revitalizing The Federal Wiretap Laws To Enhance Privacy").

[252] ÖZDOĞAN, (2004), s. 19,38; AN OVERVIEW OF ELECTRONIC SURVEILLANCE: History and Current Status, D.1.2; 1978'deki Scott-ABD davasında mahkeme, Teknik Dinleme Kanunu'nun temel taşlarından biri olan en aza indirgenme prensibini, dinlemeyi yapan devlet görevlisinin takdirine bırakmıştır. Gerçekten de, telefon dinlenmesi suretiyle elde edilen deliller doğrultusunda mahkum edilen Frank Scott, dinlenilen telefon görüsmelerinin sadece % 40'ının suç içerigi taşıdığını, geri kalanının ise normal ve meşru yasamıyla ilgili olduğunu vurgulamış, bu bağlamda dinlemenin en aza indirilmesi için gereken gayretin gösterilmediğini iddia etmiştir. Mahkeme, Scott'un iddiasını reddetmistir. Mahkemeye göre, dinlemenin en aza indirilmesi prensibi, dinlemeyi yapan devlet görevlisinin görevi esnasındaki "iyi niyeti" ile ilgilidir ve dava konusu olayda dinleme yapan görevlinin iyi niyet göstermedigine dair hiçbir emare bulunmamaktadır. (SCOTT-ABD, 436 U.S. 128 (1978), 142-143, http://supreme. justia.com/us/ 436 /128/ case.html)(İET: 27.11.2007).

[253] AN OVERVIEW OF ELECTRONIC SURVEILLANCE: History and Current Status, D.1.2; Elektronik iletişim de tıpkı sözlü ve kablolu iletişim gibi en aza indirgenme prensibi kapsamında değerlendirilir. Bununla birlikte, uygulamada bazı farklılıklar ortaya çıkabilir. Mesela, bir sözlü iletişimde denetlenmenin amacına uygun olmayan diyaloglar esnasında 'şartel kapatma' mümkünken, metinlerle yapılan iletişimde (text communication) bütün ekranı kaplayan bir metin için kapatma ve sonra tekrar açma sözkonusu olamaz. Bu gibi durumlar için uygulanacak yöntem, metnin ilgisiz bölümlerinin silinmesi diğerlerinin de denetlenme amacı doğrultusunda kullanılmasıdır. (AN OVERVIEW OF ELECTRONIC SURVEILLANCE).

İletişimin denetlenmesi fiziksel aramaya kıyasla özel hayat bakımından daha ciddi riskler ortaya çıkarmaktadır[254]. Doğası itibariyle gelişigüzel (inherently indiscriminate) bir tedbir olarak nitelendirilen iletişimin denetlenmesinin sağlanması amacıyla kullanılan cihazlara titizlikle ve ayırt edici koşullar altında başvurulması gerektiği ABD Yüksek Mahkemesi kararlarında vurgulanmıştır. Bu hususa dikkat edilmesi, hususilik prensibi (particularity principle) denilen, tedbirin, sadece suç unsuru taşıyan hususlara hasredilmesi ilkesinin gereğidir[255]. Çünkü, iletişimin denetlenmesi tedbiri, iletişimin içeriğinin soruşturma ile ilgili olup olmadığına bakmadan, kolluk görevlilerine hedef kişinin tüm iletişimini denetleme imkanı vermektedir. Bu da, kişi hakkında çıkarılmış genel bir arama kararının risklerini barındırmaktadır[256]. Bu tedbir doğası itibariyle müdahaleden bağışık olması gerekli olan bir alanda sürekli bir müdahale anlamına gelmektedir. Bu özellik de, fiziksel aramadan daha riskli bir noktaya temas etmektedir. Günlerce, bazen aylarca süren iletişimin denetlenmesi tedbiri özel hayatın sürekli bir ihlaline yol açabilmektedir[257].

Dinlemeye konu olan iletişimin şifreli veya yabancı bir dilde olması ve de dinleme için öngörülen zaman zarfında bu şifreyi çözebilecek ya da yabancı dili bilen bir kişi olmaması halinde, olabilecek en kısa zaman diliminde bu çözümleme yapılır[258].

İletişimin denetlenmesini en aza indirgemeyi amaçlayan bir diğer madde olan 2518(3)(d)'ye göre, iletişimin denetlenmesi tedbirine konu olacak yer veya cihaz aşağıdaki şartları haiz olmalıdır[259]:

- Hakkında karar verilen kişi tarafından sürekli veya genellikle kullanılmaktadır,
- Hakkında karar verilen kişi tarafından kiralanmıştır,
- Hakkında karar verilen kişinin adına kayıtlıdır.

---

[254] BERGER-NEW YORK kararında, Mahkeme, iletişimin denetlenmesi amacıyla gelişigüzel kullanılan cihazlar, ABD Anayasa'sının dördüncü ve beşinci maddelerinin ağır bir şekilde ihlali anlamına gelmektedir. Bk. BERGER-NEW YORK, 388 u.s. 41-56 http://supreme.justia. com/ us/ 388/ 41/ case .html .

[255] LOPEZ-ABD, 373 U.S. 427, 463 (1963), http://supreme.justia.com/us/373/427/case.html; (26.11.2007); OSBORN-ABD, 385 U.S. 323 (1966), http://supreme.justia.com/us/385/323/case.html#T7 (iET: 26. 11. 2007).

[257] DEMPSEY, "Communications Privacy In The Digital Age: Revitalizing The Federal Wiretap Laws To Enhance Privacy".

[258] 18 U.S.C. § 2518(5).

[259] 18 U.S.C. § 2518(3)d .

1.2.1.7. İletişime Müdahalenin Meşru Sayıldığı Haller

Teknik Dinleme Kanunu, kasta dayanan ve iletişime müdahale ile elde edilen bilgi ve belgelerin kullanılması ve açıklanmasını yasaklamaktadır. Genel olarak, devlet de dahil olmak üzere, 3. kişiler tarafından gerçekleştirilen müdahaleler bu yasaklamalar kapsamına girmekle birlikte, bazı haller bu kurala istisna teşkil etmektedir. Bu hallerden biri olan mahkeme kararı ile iletişimin denetlenmesi geniş bir şekilde anlatıldığı için, bu kısımda diğer hallere değinilecektir:

1.2.1.7.1.İletişimin Taraflarından Birinin Rızası

İletişimin taraflarından birinin iletişimin denetlenmesine rızası bulunduğu takdirde, yapılan müdahale meşrudur[260]. Bu hüküm özellikle devletin gizli ajan (undercover agent) kullanması halinde bu görevlinin yaptığı görüşmeleri denetlemek bakımından önem arzetmektedir. Gerçekten de, gizli ajanın kaydettiği telefon görüşmesinin, Teknik Dinleme Kanunu kapsamı dışına çıkarılması için bu kişinin rızasının varlığı yeterlidir. Aynı şekilde, sivil bir kişinin de, tarafı olduğu bir görüşmeyi kaydetmesi halinde bu kişinin rızasının varlığı, bu iletişime müdahale edilmesi için yeterlidir. Bununla birlikte, bir cürüm veya haksız bir fiilin bu iletişimin engellenmesi için belirleyici bir neden olmaması gerekmektedir[261]. Mahkeme kararı zorunluluğuna getirilen bu istisna, daha çok gizli narkotik polislerinin uyuşturucu satıcıları ile temasa geçtiği ve hayati tehlike barındıran hallerde, olaya diğer polislerin hemen müdahale ederek gizli polisin hayatını kurtarmak amacı ile oluşturulmuştur. Suçlularla temasa giren gizli polis, mahkeme kararı olmaksızın üzerine gizli verici yerleştirir ve bu verici marifetiyle, satıcı ile arasında geçen konuşmaların uzaktaki polis ekibine iletilmesini sağlar. Konuşmaları dinleyen uzaktaki polis ekibi, gizli polisin herhangi bir şekilde deşifre olması durumunda olaya çabucak müdahale edebilir[262].

Teknik Dinleme Kanunu'nun aradığı rıza açık olabileceği gibi, dolaylı bir rıza da geçerlidir[263]. Dolaylı rızanın (implied consent) varolduğu nasıl anlaşılacaktır? Taraflardan birinin aslında izlemeden haberi olduğunu şartlar gösteriyorsa, o halde 'rıza'dan bahsetmek mümkündür[264]. İletişime taraf olan kişileri kuşatan şartların genel

---

[260] 18 U.S.C. § 2511(2)(c).

[261] DEPARTMENT OF JUSTICE, Consent of a Party to Communication; ÖZDOĞAN, (2004), s. 42-43.

[262] ÖZDOĞAN, (2004), s. 42-43.

[263] Bk. AMEN-ABD, 831 F.2d 373, 378 (2d Cir. 1987).

[264] Bk. WORKMAN-ABD, 80 F.3d 688, 693 (2d Cir. 1996)

bir değerlendirmeye tabi tutulması suretiyle, taraflardan birinin bilerek takibe onay verdiği anlaşılıyorsa rıza vardır. Bir çok olayda, kişi takibe maruz kaldığına ilişkin ikazı almakta ve bu ikaza rağmen takip edilen sistemi kullanmaya devam etmektedir. (Berry-Funk, 146 F.3d 1003, 1011 (D.C. Cir. 1998). İkaza ilişkin delil, rızası olduğu iddia edilen tarafın bu takibi bildiği önermesini desteklemektedir. Delil yokluğu halinde ise, ilgili tarafın bu takibi bildiğini hükümetin ispatlaması gerekmektedir.(ABD-Lanoue, 71 F.3d 966, 981 (1st Cir. 1995))[265].

Gerek polis, gerekse sivil bir kişinin, tarafı olduğu kablolu ya da elektronik bir iletişime müdahalesinde federal kanunlar bakımından bir sakınca bulunmamakla birlikte bazı eyaletler, sadece tarafların hepsinin rızası olduğu hallerde iletişime müdahaleye izin vermektedirler[266]. Amerikan Barolar Birliği, çeyrek asır kadar önce, karşı tarafın bilgisi ya da rızası olmaksızın bir görüşmeyi gizlice dinleme ya da kaydetmenin etik kurallara uygun olmadığına karar vermiştir. Bu örgüt, kolluk güçlerinin yaptığı dinleme ve kaydın bu kapsamda olmadığını vurgulamıştır[267].

Kişinin kendisi ve görüşmeyi yaptığı kişi, iletişimin tarafları olup, bu iki taraftan biri bahse konu iletişimi dinlemeye alabilirler. Bu durum, taraflardan birinin yapılan iletişim öncesinde dinlemeye rıza gösterdiğini beyan etmiş olması halinde de geçerlidir[268]. Bununla birlikte, dinlemenin bir suç işlemek veya haksız fiil irtikap etmek için yapılmaması gerekmektedir[269].

ABD-White kararında Mahkeme, makul mahremiyet beklentisi (reasonable expectation of privacy) olmayan kişi ile gerçekleştirilen diyalog, bu kişinin rızası hilafına kaydedilse bile kişinin Anayasa'dan ya da Teknik Dinleme Kanunundan kaynaklanan hakları haleldar olmaz hükmüne varmıştır. Sırrını açıkladığı kişinin, bu sırrı açıklamayacağına ilişkin yanlış inancı Anayasa'nın 4. maddesi kapsamında kabul edilemez[270].

---

[265] DEPARTMENT OF JUSTICE, Consent of a Party to Communication.

[266] STEVENS/DOYLE, s. 13.

[267] STEVENS/DOYLE, s. 20 Uygulamada bazıları, Amerikan Barolar Birliğinin bu görüşünü kabul ya da reddetmek şeklinde tutum izlerken, bazıları da etik sınırlar içinde bu tür dinleme ve kayda alımaların daha geniş bir alanda meşru kabul edilmesi gerektiğini iddia etmektedirler.(STEVENS/DOYLE, s. 20).

[268] 18 U.S.C. § 2511 (2)(c).

[269] 18 U.S.C. § 2511 (2)(d).

[270] MADDOX, Dp. 46.

1.2.1.7.2.Servis Sağlayıcılarının İletişime Müdahalesi

1.2.1.7.2.1.Genel Olarak

Servis sağlayıcıları veya bunların çalışanları, servis sağlayıcının haklarını ve mülkiyetini korumak amacıyla iletişimi dinleyebilir veya açıklayabilirler. Maddede geçen, 'servis sağlayıcılarının haklarını ve mülkiyetini koruma'[271] ifadesi sahtecilik ve servis hırsızlığına karşı mücadeleye imkan tanımak için verilmiştir[272]. Örneğin, bir cep telefonu şirketi yasadışı olarak klonlanmış olan bir cep telefonunun kaynağını tespit etmek amacıyla iletişime müdahale edebilir (Pervaz-ABD, 118 F.3d 1, 5 (1st Cir. 1997)). Bu istisna ile servis sağlayıcıları, sistemin, tahribattan, hırsızlıktan ya da mahremiyet tecavüzlerinden korunması amacıyla iletişime müdahale edebilirler. Burada vurgulanması gerekli olan bir husus da, bu servis sağlayıcılarına tanınan bu iznin sınırsız takip olarak algılanamayacağı gerçeğidir. ABD-Auler, 539 F.2d 642, 646 (7th Cir. 1976) kararında Mahkeme, 'telefon şirketinin dinleme ve açıklama yetkisi sınırsız değildir' demekle bu hususun altını çizmiştir. Madde metninde[273] geçen hizmetin gereği (rendition of service) ve servis sağlayıcısının haklarının korunması ifadesi önemlidir. Burada yapılması gereken, servis sağlayıcılarının haklarının korunması ile hizmeti alan abonelerin mahremiyet haklarının korunması arasındaki dengenin muhafaza edilmesidir[274]. Servis sağlayıcı adına işgören bir tamircinin iletişime müdahil olması da bazen kaçınılmazdır ve bu istisna kapsamındadır[275].

Servis sağlayıcılar kendi sistemlerini izinsiz olarak kullanan kişilerin araştırılması hususunda geniş yetkilerle donatılmıştır. Bu yetkiler izleme ve elde edilen bilgileri açıklama olarak sayılabilir. Bununla birlikte, servis sağlayıcıları, gerek izleme gerekse elde edilen bilgileri açıklama hususunda yetkilerini en dar çerçevede kullanmak ve böylece iletişime müdahaleyi ve mahremiyete tecavüzü en aza indirmekle yükümlüdürler. Servis sağlayıcıları, hak ve mülkiyetlerini korumak amacıyla kendilerine

---

[271] 18 U.S.C. § 2511(2)(a)(i).

[272] 18 U.S.C. § 2511 (2)(a)(i), Bk. Villanueva-ABD, 32 F. Supp. 2d 635, 639 (S.D.N.Y. 1998).

[273] 2511(2)(a)(i).

[274] HARVEY-ABD, 540 F.2d 1345, 1350 (8th Cir. 1976) ; PRIVACY:WIRETAP ACT. http://ilt.eff.org/index.php/Privacy:_Wiretap_Act#Electronic_Communications (İET: 9.10.2007).

[275] DEPARTMENT OF JUSTICE, The Provider Exception.

verilmiş olan bu yetkilerini aşarak, yaptıkları araştırmayla ilgisi olmayan bilgiler elde etmek suretiyle kötüye kullanamazlar[276].

Servis sağlayıcıları sadece belirlenen sınırlar dahilinde bu yetkilerini kullanabilirler, bu sınırlar ise servis sağlayıcının haklarının korunması olarak belirlenmiştir. Servis sağlayıcıları, kendi haklarının korunmasını temin etmek amacıyla iletişime müdahale edebilir ve elde edilen bilgileri kolluğa verebilirler. Ancak, servis sağlayıcıları kolluk güçlerince yürütülen bir soruşturma çerçevesinde bu yetkilerini kullanamazlar. Örneğin, McClelland-McGrath, 31 F. Supp. 2d 616 (N.D. Ill. 1998), davasında, adam kaçıran bir kişi hakkında soruşturma yapan kolluk görevlileri, şüphelinin telefonunun bir kaçak (cloned) telefonla görüşmeler yaptığından bahisle, servis sağlayıcıdan şüphelinin telefonunu dinlemeye almasını istemiş, kabul edilen talep sonunda gerçekleştirilen dinlemeyle elde edilen bilgiler şüphelinin yakalanmasını sağlamıştır. Şüphelinin kolluk görevlileri hakkında yaptığı şikayet sonrasında, kolluk görevlileri 2511(2)(a)(i) uyarınca yaptıklarının yasal olduğunu, servis sağlayıcının, kendi haklarını korumak amacıyla klonlanmış(ruhsatsız) telefonu takip edebileceklerini iddia etmiştir. Mahkeme, servis sağlayıcının haklarını koruma amacının ötesine geçen dinlemenin madde kapsamında olmadığına hükmetmiştir. Mahkemeye göre, şüphelinin yerinin tespit edilmesi amacı, servis sağlayıcının haklarının korunmasına ilişkin değildir[277].

2511 (2) (a) (ii) hükmüne göre, 1978 tarihli FISA'da tanımlanan kişiler tarafından bir talep getirildiği takdirde, telefon santrali operatörü ve servis sağlayıcısının çalışanları, talep edilen hukuki yardımı (iletişimin dinlenmesine ilişkin bilgi, ekipman, teknik yardım) vermek zorundadırlar. Bu talep esnasında, yetkili hakim tarafından usulüne göre verilmiş ve bu yardımın yapılmasına cevaz veren bir mahkeme kararı olmalıdır. Mahkeme kararı olmaksızın bu yardımın yapılması hususu da öngörülmüştür. 2518(7) maddesinde belirtilen kişi veya Adalet Bakanı tarafından, mahkeme kararının[278] gerekli olmadığı ve tüm yasal şartların karşılandığını beyan eden bir onay belgesi[279] ibraz edildiği takdirde bahse konu kişiler (telefon santrali operatörünün, kablolu veya elektronik servis sağlayıcısının çalışanları) bu yardımı yapmakla yükümlüdürler. Bu hizmeti sunan yetkililer, yargılama süreci gerektirmediği ve Adalet Bakanı veya diğer

[276] DEPARTMENT OF JUSTICE, The Provider Exception.

[277] DEPARTMENT OF JUSTICE, The Provider Exception; Benzer bir hüküm için Bk. ABD-Savage, 564 F.2d 728, 731 (5th Cir. 1977).

[278] 18 U.S.C. § 2511 (2)(a)(ii)(A).

[279] 18 U.S.C. § 2511 (2)(a)(ii)(B).

yetkililerin önceden izni olmadığı takdirde, iletişime yapılan bir müdahale olduğunu ve bu dinleme için kullanılan cihaz hakkındaki bilgileri ifşa edemezler. Bu hususta yapılacak izinsiz bir açıklama 2520 nolu maddede ifadesini bulan yaptırımlara tabidir[280].

Bir elektronik iletişim servis sağlayıcısının, iletişimin içeriğini açıklayabildiği diğer haller 18 U.S.C. § 2511(3)(b)'de sayılmıştır. Bu çerçevede, servis sağlayıcı tarafından hataen elde edilen ve bir suçun işlenmesine ilişkin olan bilgilerin kolluk görevlilerine açıklanması yasal sınırların aşılması anlamına gelmemektedir[281]. Bu kapsamda, orijinatör, alıcı ya da iletişimin planlanan alıcısı tarafından rıza verilmiş olması hali de iletişime yasal bir müdahale olarak kabul edilmektedir[282].

1.2.1.7.2.2.Servis Sağlayıcı Tarafından Elde Edilen Bilgilerin Kullanılması

1.2.1.7.2.2.1.Bildirim Öncesinde Elde Edilen Bilgiler

Kolluk görevlileri ve savcılar, servis sağlayıcının kendi haklarını korumak amacıyla yapmış olduğu bir takipten elde edilen bilgileri kullanmak konusunda oldukça dikkatli davranmalıdırlar. Servis sağlayıcı tarafından 2511(2)(a)(i) hükmü çerçevesinde elde edilen bilgilerde suç şüphesinin varolduğu kolluk görevlilerine sonradan bildirilmişse, diğer bir ifadeyle, servis sağlayıcı kendi inisiyatifi ile takibi yapmış, elde edilen bilgilerin de bir suça ilişkin deliller olduğu anlaşılmış ise kolluk görevlilerinin bu bilgileri kullanmasında herhangi bir sakınca yoktur[283].

1.2.1.7.2.2.2.Bildirim sonrası elde edilen bilgiler

Kolluk görevlileri ile servis sağlayıcı arasında irtibat kurulduktan sonra, kolluk görevlileri ancak belli şartların varlığı halinde servis sağlayıcı tarafından elde edilen bilgileri kullanabilir[284]. Bu şartlar aşağıdaki gibidir:

- Bir suçun mağduru olan servis sağlayıcı, kendi haklarını korumak amacıyla dinleme yapmakta ve elde edilen bilgileri açıklamaktadır.

---

[280] 18 U.S.C. § 2511 (2)(a).

[281] 18 U.S.C. § 2511(3)(b)(vi); DEPARTMENT OF JUSTICE, The inadvertently Obtained Criminal Evidence Exception.

[282] 18 U.S.C. § 2511(3)(b)(ii) '…with the lawful consent of the originator or any addressee or intended recipient of such communication'.

[283] DEPARTMENT OF JUSTICE, The Provider Exception.

[284] 18 U.S.C. § 2511(2)(a)(i) .

- Yapılan dinlemenin, polisiye amaçlara hizmet etmekten çok servis sağlayıcının kendi haklarını koruma amacıyla başlatıldığı kolluk tarafından teyit edilmelidir.

- Kolluğun yönlendirmesi, görevlendirmesi ve talepte bulunması olmamalıdır.

- Kolluk yapılan takibe katılmamış ya da kontrolünde tutmamış olmalıdır.

Kanun tarafından öngörülmemiş olmakla birlikte, servis sağlayıcı tarafından imzalanan, haklarını bildiğini ve takibi kendi haklarını korumak amacıyla ve rızaen yaptığını belgeleyen bir dokümanın kolluk görevlilerince tanzim edilmesi tavsiye edilmektedir[285].

1.2.1.7.3.Dahili Hat Marifetiyle İletişim

Kongre, kanun çalışmaları esnasında, bu istisnanın oldukça dar bir amacının olmasını hedeflemiştir. Bu istisna öncelikli olarak işyerlerine, müşterilerle iş görüşmeleri yapan çalışanlarının performanslarını değerlendirme imkanı vermek amacıyla kanun metnine konmuştur. Bu bağlamda, bir işverenin işyerindeki performansı ölçme amaçlı olarak dahili konuşmaları dinlemesi Teknik Dinleme Kanunu hükümlerinin ihlali olarak değerlendirilmemiştir[286]. Bu konuda mahkemelerce verilen kararlarda bir istikrar olduğu söylenemez. Bu durum, kanunda yer alan 'sıradan iş akışı içerisinde'(ordinary course of business) ifadesinden kaynaklanmaktadır. Bazı mahkemeler bu ifadeyi oldukça geniş yorumlamıştır. Hatta Simpson-Simpson, 490 F.2d 803, 809 (5th Cir. 1974) kararında, kocanın karısının telefonunu kaydetmesinin Bölüm III'ün ihlali anlamına gelmediğine karar verilmiştir. Anonymous-Anonymous, 558 F.2d 677, 678-79 (2d Cir. 1977) kararında da benzer bir yorum yapılmış ve gözaltındaki kızıyla görüşen karısının telefonlarını dinleyen kocanın bu eylemi Bölüm III'e aykırı bulunmamıştır. Bununla birlikte, diğer bazı mahkemeler, bu genişletici yorumdan uzak durmuş ve bazen açıkça bazen de dolaylı olarak 'sıradan iş akışı içerisinde'(ordinary course of business) ifadesinden gizli bir dinleme hakkının doğmadığı hükmüne varmışlardır[287]. Kempf-Kempf, 868 F.2d 970, 973 (8th Cir. 1989) kararında, özel durumlar dışında Bölüm III'ün iletişime yapılacak herhangi bir müdahaleyi yasakladığı, eşler arasında dinlemenin mazur görüldüğünü ortaya koyan herhangi bir hüküm bulunmadığı vurgulanmıştır. Harpel-ABD, 493 F.2d 346, 351 (10th Cir. 1974) kararında ise, usulune göre alınmış bir yetki ya da rıza bulunmaksızın dahili hat kapsamında yapılan gizli bir telefon kaydının,

---

[285] DEPARTMENT OF JUSTICE, The Provider Exception.

[286] Bk. Briggs-American Air Filter Co., 630 F.2d 414, 418 (5th Cir. 1980).

[287] İşin olağan akışı içerisinde bir dahili hat dinlemesi vukubulduğunda, böyle bir rutin uygulamaya başvurulduğu hususunun ilgililere bildirilmesi gerekmektedir. Bk. STEVENS/DOYLE, s. 11.

kanunda yer alan ‘sıradan iş akışı içerisinde’(ordinary course of business) ifadesi kapsamına girmediğine karar verilmiştir. Bazı kararlarda[288] ise, dahili hat istisnasının dar bir şekilde yorumlanması gerektiğine vurgu yapılmış, bu istisna kapsamına sadece işyerlerindeki dinlemenin girdiği belirtilmiştir[289].

Kolluk görevlileri için de bu istisna geçerli olup, rutin ve genel bir uygulamanın parçası olarak kolluk güçlerinin çalışma ofisleri ve müştemilatında (polis departments) ve cezaevlerindeki dahili hatlardan yapılan görüşmeler Teknik Dinleme Kanunu anlamında bir istisna teşkil etmektedir. Diğer bir ifadeyle bu tür iletişimler bu kanun ile belirlenen şartlar gerçekleşmeksizin denetlenebilecektir[290].

1.2.1.7.4.Kamuya Açık Bilgiler

Kamuya açık olacak şekilde tasarlanmış bir elektronik iletişim sisteminden ve kamunun kullanımına hasredilmiş bir istasyondan yapılan yayından elde edilen bilgiler iletişimin yasadışı olarak elde edilmesi kapsamına girmez[291]. Mesela, radyo programlarına telefonla katılan birinin, radyoda yaptığı konuşmanın üçüncü kişilerce kayda alınması mahkeme kararını gerektirmemektedir[292]. Federal İletişim Komisyonu[293] yetkililerinin, Amerikan mevzuatının 47 nolu başlığının 5. babında sayılan görevlerini ifası bağlamında, radyo ile iletilen kablolu, elektronik ve sözlü iletişimi dinlemeleri (intercept), açıklamaları veya bu bilgileri kullanmaları yasadışı sayılmamıştır[294]. Bir radyo iletişimi hali hazırda herkese açıksa bu iletişim Anayasa’nın dördüncü maddesinde ifadesini bulan mahremiyet beklentisi (reasonable expectation of Privacy) kapsamında yer almaz. Bununla birlikte halihazırda ulaşılabilir olmayan (readily accessible) bir iletişim, başkalarının müdahalesine (interception) açık değildir[295].

---

[288] Bk. Deal-Spears, 980 F.2d 1153, 1158 (8th Cir. 1992).

[289] DEPARTMENT OF JUSTICE, The Provider Exception; STEVENS/DOYLE, s.10.

[290] STEVENS/DOYLE, s. 11.

[291] 18 U.S.C. § 2511(2)(g)(i); AN OVERVIEW OF ELECTRONIC SURVEILLANCE, History and Current Status, D.1.2

[292] ÖZDOĞAN, (2004), s. 42-43.

[293] (Federal Communications Commission) ABD’de eyaletlerarası iletişim hakkında düzenlemeler yapan bağımsız ajans.

[294] 18 U.S.C. § 2511 (2)(b).

[295] Radyo yayıncılığı, kamu güvenliği ilgili yayınlar (polis, itfaiye, vd.),amatör radyo, radio, citizens band(range of radio frequencies set aside for two-way radio communication by citizens and businesses in the USA); (radio receiver/transmitter used to communicate on Citizens Band frequencies), vb. servisler koruma kapsamında olmayan, diğer bir ifadeyle herkesin ulaşımına açık iletişim türleridir. (AN OVERVIEW OF ELECTRONIC SURVEILLANCE, History and Current Status.)

Gemi, uçak, vb. araçlardan yapılan yayınlar[296]; hükümet, kolluk güçleri, sivil savunma, polis veya itfaiye gibi kamuyu korumaya özgülenmiş kurumların yayınları[297]; kendilerine verilen frekanstan yayın yapan istasyondan yapılan yayınlar[298] ile denizcilik ve havacılık iletişim sistemlerinden yapılan yayınlar bu kapsamda olup, bu yayınların dinlenmesi ve kayda alınması yasadışı değildir[299].

1.2.1.8.Denetleme ile Elde Edilen Delilin Muhafazası

Dinleme sonucunda elde edilen delilin muhafaza edilmesi, bu işlemi gerçekleştiren görevlilere bir yükümlülük[300] olarak yüklenmiştir. Delillerin muhafazası, delillerin gizliliğini sağlamak bakımından gereklidir. Bu işlem ayrıca, delillerin imha edilmesi veya ortadan kaldırılması riskini yok etmek için de zorunludur.[301] Teknik Dinleme Kanununda böyle bir hüküm öngörülmesinin amacı, elde edilen delilin gerçek durumu yansıttığının ve değiştirilmediğinin garanti altına alınmasıdır[302]. Madde 2518(8)'te dinleme ile elde edilen delilin muhafazası için yapılacak işlemler sayılmıştır. Anılan maddeye göre,

- Dinlenilen bilgi banda veya benzeri bir cihaza (other comparable device) kaydedilmelidir. Maddede vurgulanan husus; yapılan kaydın, silinmesi ve değiştirilmesi mümkün olmayan bir şekilde gerçekleştirilmesidir[303].

- Mahkeme kararı ile belirtilen süre veya verilen ek süre bitiminde, elde edilen kayıtlar mühürlenip derhal yetkili mahkemeye teslim edilir. Burada kullanılan 'sürenin bitiminde derhal' (immediately after the expiration) ifadesi, yargısal otoritenin meseleye bir an önce vaziyet etmesini sağlamak bakımından önemlidir[304].

Kayıtlar, hakimin kararlaştıracağı bir yerde muhafaza altında tutulur. Deliller hakimin onayı olmadığı takdirde imha edilmeyecektir. Muhafaza için kanunda öngörülen süre

---

[296] 18 U.S.C. § 2511 (2)(g)(ii)(I).

[297] 18 U.S.C. § 2511 (2)(g)(ii)(II).

[298] 18 U.S.C. § 2511 (2)(g)(ii)(III).

[299] STEVENS/DOYLE, s. 14 ; ABD hukukundaki bu yaklaşım, AİHM tarafından da kabul edilmektedir. Sivil havacılıkta kullanılan bir radyo kanalı aracılığıyla yapılan bir haberleşme, başka kullanıcıların da erişebileceği bir dalga boyunda yapıldığı için AİHM tarafından özel haberleşme olarak nitelendirilmeyerek özel hayata müdahale sayılmamıştır. (ÇOKSEZEN, s. 4.).

[300] AN OVERVIEW OF ELECTRONIC SURVEILLANCE, History and Current Status,D.1.2 .

[301] ÖZDOĞAN, (2004), s. 38-39.

[302] AN OVERVIEW OF ELECTRONIC SURVEILLANCE, History and Current Status,D.1.2.

[303] 18 U.S.C. § 2517 (1) ; WONG, 3.3.14.

[304] 18 U.S.C. § 2518(8) (a) ; WONG, 3.3.14.

10 yıldır. Kayda alınan bandın açıklanması ve kullanılması amacıyla kaydedilmesi 2517 nolu maddenin birinci ve ikinci paragraflarındaki hükümler çerçevesinde mümkündür. Bu durumlar aşağıdaki gibidir:

- Kablolu ve Elektronik İletişim ile Sözlü İletişim[305] başlığını taşıyan 119. kısımda belirtilen hükümler çerçevesinde yetkilendirilmiş olan bir kolluk görevlisinin, elde ettiği delilleri başka bir görevlinin bilgisine sunması. Bunun için ön şart, bu aktarma işleminin hem bilgiyi veren hem de alan kişinin mesleğinin icrası bakımından uygun olmasıdır[306].

- 119. kısımda belirtilen hükümler çerçevesinde yetkilendirilmiş olan bir kolluk görevlisinin, elde ettiği delilleri kendi meslek kurallarına uygunluk arz ettiği takdirde kullanması[307].

- 119. kısımda belirtilen hükümler çerçevesinde, iletişimin denetlenmesi yöntemiyle elde edilen delilleri alan kişinin, yemin veya yalan söylemediğine ilişkin bir tasdik beyanı[308] tahtında bu bilgileri açıklaması[309].

Dinleme kayda geçirildikten sonra vurulan mühür veya mührün vurulmadığı hallerde niçin mühür vurulmadığını izah eden ve 2517(3) tahtında yapılmış ikna edici bir açıklama delillerin kullanılabilmesi için önşarttır[310]. Yapılan dinleme başvuruları ve verilen dinleme izinleri hakim tarafından mühürlenmektedir. Başvurular ve kararlar hakimin tespit edeceği bir yerde muhafaza altına alınır ve hakim kararı olmadıkça imha edilemez. Muhafaza süresi on yıldır. Yapılan başvurular ve verilen kararlar ancak yetkili

---

[305] Chapter 119: Wire And Electronic Communications Interception And Interception Of Oral Communications http://www4.law.cornell.edu/uscode/html/uscode18/usc_sup_01_18_10_I_20_119.html (İET:29.10.2007).

[306] 18 U.S.C. § 2517 (1).

[307] 18 U.S.C. § 2517 (2).

[308] Madde metninde geçen 'while giving testimony under oath or affirmation' ifadesindeki 'affirmation' kelimesi 'yemin yerine geçen söz' anlamına gelmektedir. Affirmation, vicdani veya dini düşüncesi nedeniyle yemin verdirilemeyen kişiler için ihdas edilmiş bir kurumdur. Bu kişiler yemin etmemekte, bunun yerine yalan beyanda bulunmadıklarını ifade sadedinde bir olumlama, bir tasdik beyanında bulunmaktadırlar. Yemin yerine 'affirmation' kurumunu tercih edenler arasında Yehova Şahitleri ile bir Protestan mezhebi olan Dostlar Topluluğu (Society of Friends) da vardır. http://www. britannica. com/ search?query=affirmation&ct= (İET:22.9.2007).

[309] 18 U.S.C. § 2517 (3).

[310] 18 U.S.C. § 2518(8)(a). 2517'de belirtilen hükümler çerçevesinde yetkilendirilmiş olan bir kolluk görevlisi, dinleme neticesinde elde ettiği delilleri yeminle ifade verme esnasında kullanabilir.

hakime makul bir neden sunulması halinde açıklanabilir[311]. Bu hükümlerin ihlali mahkemeye itaatsizlik[312] olarak kabul edilip cezalandırılacaktır[313].

1.2.1.9. İlgiliye Bildirim

İletişimin denetlenmesi tedbiri doğası itibariyle gizlidir. Geleneksel arama tedbirinden farklı olarak bu tedbirin meyve verebilmesi, hedef kişinin tedbirden habersiz olmasıyla doğru orantılıdır. Geleneksel aramada, ilgili kişi haberdar edilerek (knock and notice) kendisi hakkında uygulanacak tedbir en başta bildirilir. Bu davranışla hedef kişiye muhatap olacağı hukuki tedbirin doğası en baştan aktarılmış ve özel hayatına müdahale edileceği keyfiyeti bildirilmiş olur. Böylece kişi, bu tedbirin hukukiliğini olabilecek en kısa zamanda sorgulamak imkanına ulaşmıştır. Halbuki iletişimin denetlenmesinde durum farklıdır[314]. Berger kararında, bildirime ilişkin düzenlemenin bulunmaması nedeniyle ilgili New York Kanunu eleştirilmiş, dinleme sonrasında telefonunun dinlendiği bilgisinin verilmemesi ve sanığın mahkemede kendi aleyhine delil olarak kullanılacak bilgilerden haberdar olamaması silahların eşitliği ilkesine aykırı bulunmuştur[315]. Bu eleştiri çerçevesinde hazırlanan Teknik Dinleme Kanunu, kararda isimleri geçen kişilere ve mahkemenin gerek duyması halinde diğer ilgili şahıslara, telefonlarının dinlemeye alındığına dair bilgi verilmesi yükümlülüğü getirmiştir[316].

Makul bir süre içinde, fakat her halükarda mahkeme kararı verilmesi için yapılan başvurudan itibaren 90 gün içinde, 2518 (7)(b) çerçevesinde verilen denetleme kararı hakkında hazırlanacak envanter, yapılan başvuruda ismi geçen kişilere ve dinlemeye taraf olan diğer kişilere[317] tebliğ edecektir[318]. Bu envanterde aşağıdaki hususlar yer alır:

---

[311] 18 U.S.C. § 2518 (8)(b).

[312] Mahkemeye karşı kasıtlı olarak yapılmış itaatsizlik. Bu fiil, mahkeme kararına karşı olabileceği gibi mahkeme huzurunda yapılan saygısızlık da bu kapsamda itaatsizlik sayılır. Sivil ve cezai olmak üzere iki türlü itaatsizlik olabilir. http://www.lectlaw.com/def/c118.htm (27.11.2007) İtaatsizlik doğrudan ya da dolaylı olabilir. Doğrudan itaatsizlik mahkeme huzurunda ve mahkemenin intizamını bozan davranışlar olarak tanımlanırken, dolaylı itaatsizlik mahkemece verilmiş bir karara karşı riayetsizlik neticesinde ortaya çıkmaktadır. http://en.wikipedia.org/wiki/Contempt_of_court (27.11.2007) .

[313] 18 U.S.C. § 2518 (8)(c).

[314] DEMPSEY, "Communications Privacy In The Digital Age: Revitalizing The Federal Wiretap Laws To Enhance Privacy".

[315] ÖZDOĞAN, (2004), s. 39.

[316] ÖZDOĞAN, (2004), s. 39-40.

[317] Bu kişilerin tespiti hakimin takdirinde olup, hakim yargılama ve adaletin tecellisi bakımından gerekli gördüğü kişilere tebligat yapar.'(and such other parties to intercepted communications as the judge may determine in his discretion that is in the interest of justice).

[318] AN OVERVIEW OF ELECTRONIC SURVEILLANCE: History and Current Status, D.1.2; WONG,3.3.15;JUDGE/KALUNIAN/QUANT "Brief Overwiev of the WiretapLaw".

- Mahkeme kararı veya emrin nedenleri[319],

- Mahkeme kararı veya emrin yürürlüğe giriş tarihleri, ne kadar bir süre için dinlemenin yapıldığı, onaylanmış/onaylanmamış denetleme kararı veya denetleme talebinin reddine ilişkin karar[320]**,**

- Bu dönemde iletişimin denetlenme veya denetlenmeme nedenleri[321].

Hakim, kendisine yapılan bir başvuru ile (upon the filing of a motion) bu kişiye veya avukatına dinlemeye konu olan iletişim parçalarına, dinleme başvurusuna ve dinleme kararına ulaşma imkanı verebilir[322]. Hakim, adaletin tecellisi bakımından yararlı olacağına kanaat getirmesi halinde bu talebi kabul edebilir. Taraflardan biri tarafından yapılacak bir taleple ve makul bir neden gösterilmesi şartıyla hakim, bahse konu envanterin tebliğini erteleyebilir[323].

Bildirimde bulunma Anayasa'dan kaynaklanan bir zorunluluk olduğundan, bu hükme aykırı davranılması elde edilen delilin imhası gibi ciddi bir sonucu gerektirmektedir. Böyle bir bildirimi gerekli gören Kongrenin bu hükmü koymasındaki temel amaç iletişimin denetlenmesinin makul ve haklı gerekçelere bina edildiği hususunda topluma güvence sunmaktır. İletişimin denetlenmesine ilişkin başvuru sonucunda mahkeme tarafından verilen kararın olumlu ya da olumsuz olması önemli değildir. Böyle bir tedbirin bitimi sonrasında, en azından ilgili kişi hakkında böyle bir tedbirin uygulandığını bilme hakkına sahiptir. Böylece mahremiyet alanına haksız olarak girildiğini düşünen ilgili kişi, istediği takdirde, yapılan işleme karşı gerekli hukuki yollara başvurma imkanını elde etmiş olacaktır[324].

1977'deki Donovan-ABD davasında Mahkeme, hakkında dinleme kararı verilen kişinin isminin mahkeme kararında sehven yazılmamış olmasının, bu karara istinaden elde edilen delillerin sıhhatine engel olmayacağına hükmetmiştir. Bu davada mahkemenin temas ettiği hususlardan bir diğeri de, dinleme sonrası hakkında dinleme kararı verilen

---

[319] 18 U.S.C. § 2518(8)(d)(1).

[320] 18 U.S.C. § 2518(8)(d)(2).

[321] 18 U.S.C. § 2518(8)(d)(3).

[322] Buradaki '…may in his discretion make available to such person or his counsel for inspection such portions of the intercepted communications' ifadesi, hakimin taleple bağlı olmadığını, bu talebi kabul etmeyebileceğini ifade sadedinde kullanılmıştır.

[323] 18 U.S.C. § 2518(8)(d).

[324] JUDGE/KALUNIAN/QUANT "Brief Overwiev of the WiretapLaw"; AN OVERVIEW OF ELECTRONIC SURVEILLANCE: History and Current Status,D.1.2.

kişiye bilgi verme yükümlülüğü ile ilgilidir. Mahkeme, görevlilerin herhangi bir kasta dayanmaksızın, şüpheliye dinleme işlemiyle ilgili bilgi vermemeleri durumunda, bu durumun dinleme ile elde edilen delillerin sanığın aleyhine kullanılmaması için yeterli sebep oluşturmayacağına karar vermiştir[325].

1.2.1.10.Denetleme ile Elde Edilen Bilgilerin Açıklanması

İletişimin denetlenmesi ile elde edilen bilgilerin açıklanması Madde 2517(1), (2) ve (3)'te düzenlenmiştir. Bu maddelere göre, denetlemeyi yapan şahıs, tedbirle elde ettiği bilgileri, açıklanmasında mahsur olmayan çalışma arkadaşlarına, yaptığı işin gereği olarak açıklamak durumunda olduğu kişilere ve herhangi bir devlet makamı huzurunda yeminli ifade verirken açıklayabilir[326].

Madde 2517'de tedbirle ile elde edilen bilgilerin açıklanması ve kullanılmasına ilişkin hükümler yer almaktadır. Kablolu, elektronik ve sözlü iletişimin denetlenmesi başlıklı 119 nolu kısımda belirtilen hükümler çerçevesinde yetkilendirilmiş olan bir kolluk görevlisinin, elde ettiği delilleri başka bir görevlinin bilgisine sunması 2517(1) de düzenlenmiştir. Bunun için ön şart, bu aktarma işleminin hem bilgiyi veren hem de alan kişinin mesleğinin icrası bakımından uygun olmasıdır[327]. 2517(2)'de düzenlenen hüküm ise; yine aynı kısımda belirtilen hükümler çerçevesinde yetkilendirilmiş olan bir kolluk görevlisinin, elde ettiği delilleri, kendi meslek kurallarına uygun olduğu takdirde kullanmasına ilişkindir[328].

2517(3)'te ise, 'Kablolu ve Elektronik İletişim ile Sözlü İletişim' [329] başlığını taşıyan kısımda belirtilen hükümler çerçevesinde, elde edilen delilleri alan kişinin bu bilgileri bir Federal veya eyalet makamı önünde açıklaması düzenlenmiştir. Burada önemli olan husus, bu açıklamanın yemin verdirilerek ya da açıklayacak kişinin yalan söylemediğine ilişkin bir tasdik beyanında bulunması suretiyle yapılmasıdır[330].

Madde 2518(9)'a göre, dinlemeden elde edilen bilgilerin mahkeme önünde kullanılması halinde, denetlemeyi yapan organ, dinlemeye takılan kişilere en az 10 gün öncesinden

---

[325] ÖZDOĞAN, (2004), s. 18-19.

[326] 18 U.S.C. § 2517; ÖZDOĞAN, (2004), s. 39-40.

[327] 18 U.S.C. § 2517 (1).

[328] 18 U.S.C. § 2517 (2).

[329] Section 119: Wire And Electronic Communications Interception And Interception Of Oral Communications.

[330] 18 U.S.C. § 2517 (3).

tedbir başvurusunu, tedbire dair mahkeme kararının örneğini ve ilgili evrakı (accompanying documents) vermek zorundadır[331]. Bu belgelerin en az on gün içinde verilmesinin mümkün olmaması halinde, ilgili tarafların bu bilgileri gecikmeli olarak almasının haklarını haleldar etmeyeceğinin (…the party will not be prejudiced by the delay in receiving such information) yetkili hakim tarafından tespit edilmesi halinde bu süre şartı uygulanmayabilir[332].

1.2.1.11.İletişime Yasadışı Müdahalenin Yaptırımı

Bilerek bir kimsenin iletişimine müdahale eden, teşebbüs eden veya başka birine ileten (procure)[333]; yasadışı olarak elde edilen iletişim bilgilerini kullanan, kullanmaya teşebbüs eden veya başkasına kullanması için ileten[334]; bilginin iletişimin dinlenmesi marifetiyle elde edildiğini bilerek veya bilecek durumda olarak, iletişimden elde edilen bilgileri ifşa eden veya ifşa etmeye teşebbüs eden[335]; bilginin iletişimin dinlenmesi marifetiyle elde edildiğini bilerek veya bilecek durumda olarak iletişimden elde edilen bilgileri kullanan, kullanmaya teşebbüs eden veya başka birine tedarikte bulunan (procure) bulunan[336] kişiler 2511(4) uyarınca 5 yıla kadar hapis cezasıyla cezalandırılır ya da 2511, (5) hükmü uyarınca hukuk davasına maruz kalırlar[337]. Suç oluşabilmesi için eylemin kasten yapılması gerekmektedir. Dolayısıyla, taksirle (inadvertently) yapılan iletişime müdahale suç değildir[338].

Bununla birlikte, yapılan müdahalenin iyiniyetle (in good faith) ve kanun hükümlerine riayet edilerek (with full regard for the law) yapılması durumunda bile mahkemeler kanunun ihlal edildiğine hükmedebilmektedirler[339]. Komşunun dinlenmesi suretiyle elde

---

[331] ÖZDOĞAN, (2004), s. 39-40.

[332] 18 U.S.C. § 2518(9).

[333] 18 U.S.C. § 2511 (1)(a).

[334] 18 U.S.C. § 2511 (1)(b).

[335] 18 U.S.C. § 2511 (1)(c).

[336] 18 U.S.C. § 2511 (1)(d).

[337] DEPARTMENT OF JUSTICE, Remedies For Violations of Title III; STEVENS/DOYLE, s. 8; Hukuk davası açma için öngörülen süre, davalının ihlali öğrendiği tarihten itibaren 2 yıldır.(18 U.S.C. § 2520 (e)).

[338] Eylemin kasıt içeren bir halet-i ruhiye içinde işlenmesi gerektiğinin altını çizmek bakımından 1968 tarihli Teknik Dinleme Kanununda değişiklik yapmak üzere ihdas edilmiş alt komite 'wilful ' yerine 'intentional' ifadesini ikame etmiştir. (STEVENS/DOYLE, Dp. 17).

[339] İyi niyet ilkesinin mahkemelerce ihlal nedeni olarak yorumlanmadığı davalara da rastlanmaktadır. Ojeda Rios-ABD, davasında, dinleme sonrasında kaydedilen bilgilerin hemen mühürlenmesi yerine 118 gün sonra mühürlenmesinin her hangi bir kasıttan dolayı yapılmadığı ve görevlilerin iyi niyetli oldukları düşüncesiyle elde edilen delillerin mahkemede kullanılabileceği kararına varmıştır. OJEDA RIOS-ABD, 495 U.S. 257 (1990), http://supreme.justia.com/us/495/257/case.html (İET:4.1.2008).

edilen ve akabinde polise sunulan bilgiler ya da malul olduğu sonradan anlaşılan bir mahkeme kararına dayanılarak elde edilen bilgiler yasadışı müdahaleden elde edilmiş bilgiler olarak kabul edilmektedir[340]. Burada önemli olan eksiklikler teknik eksiklikler değildir. İletişimin denetlenmesi gibi olağanüstü nitelikteki bir tedbire başvurulmasını gerektiren olmazsa olmaz şartlardaki maddi (substantial) eksiklikler mahkeme kararını malul hale getirebilirler[341]. Örneğin, makul sebep (probable cause) şartı yokluğuna rağmen elde edilen bilgiler delil olarak kabul edilmeyecektir. Teknik Dinleme Kanunu, yasadışı olarak müdahaleye konu olan iletişimin tarafı olan herkese, bu iletişim sistemini kullanmaya yetkili olup olmadığına bakılmaksızın, bu yöntemle elde edilen bilgilerin ortadan kaldırılmasını isteme hakkını verir[342].

Kanundan kaynaklanan görevlerini yapan kişilerin iyi niyetle ve görevlerini ifa esnasında yaptıkları işlem ve eylemler hakkında bir koruma getirilmiştir. Cezai ve hukuki takibat ise, genellikle bu kişilerin görevlerini kötüye kullandıkları hususunda kanaat olduğunda gündeme gelmektedir. İyi niyetle yapılan işlem ve eylemlerden kaynaklanan hataların mazur görülmesi ile ilgili olarak Hakim Learned Hand tarafından yaklaşık yarım asır önce ortaya konan yaklaşım çarpıcıdır. Bu yaklaşıma göre, görevlerini ihmal eden ya da kötüye kullanan (truant to their duties) kişiler hakkında takibat yapılması tabiidir. Ancak dürüst bir şekilde yanılan(honestly mistaken) ve başkalarının hatalarından mutazarrır olan kişinin cezalandırılması doğru değildir. Bu konuda dengeli bir yaklaşımın tesis edilmesi gerekir. Öte yandan nitelikli bağışıklık (qualified immunity) olarak adlandırılan sisteme göre, makul bir insanın bilebileceği yasal ve anayasal hakları ihlal etmeyen bir görevlinin takdir hakkı içeren kararları cezai ve sivil takibattan muaf olmalıdır[343].

Teknik Dinleme Kanunu'nun bu konuyla ilgili hükümlerine riayetsizlik neticesinde, para cezasının yanı sıra mağdur lehine tazminata hükmedilebilir. Bu bağlamda, avukat masraflarına da hükmedilebilir[344].

Hükümet görevlilerinden birinin iletişime yasal olmayan bir müdahalede bulunması halinde, kişisel bir kusurunun bir mahkeme veya hükümet organı tarafından tespit edilmesi şartıyla, ilgili kişi hakkında disiplin takibatı da başlatılır. Takibatın

[340] DEPARTMENT OF JUSTICE, Remedies For Violations of Title III.

[341] GIORDANO-ABD, 416 u.s. 505 (1974), 527http://supreme.justia.com/us/416/505/case.html.

[342] DEPARTMENT OF JUSTICE, Remedies For Violations of Title III.

[343] DEPARTMENT OF JUSTICE, Remedies For Violations of Title III.

[344] 18 U.S.C. § 2520.; STEVENS/DOYLE, s.17-18.

başlatılabilmesi için kişinin iradi ya da kasti (willful veya intentional) bir eyleminin olması gerekir. Bu konuda ilgili takibatı başlatan devlet organı başkanınca bir disiplin cezası verilmemesine karar verilmesi halinde, bu kararın gerekçeleri o kurumun bağlı olduğu Genel Müfettişe bildirilir[345]. Öte yandan, iletişimin denetlenmesi tedbirinin uygulanması yoluyla elde edilmiş bilgileri kanunun belirlediği sınırların[346] dışında isteyerek (wilfully) açıklamak da yasadışı kabul edilmiştir[347].

1.2.1.12.Adli Amaçlı İletişimin Denetlenmesinde Delil Yasağı

Teknik Dinleme Kanunu, ABD Anayasası'nın 4. bölümünde arama ve elkoyma için öngörülen hükümlerden daha ağır müeyyideler ihtiva etmektedir. Bunlar neticesinde birtakım cezai ve sivil yaptırımlar öngörülmüş, bunun yanı sıra bu kurallara riayet edilmeden elde edilen bilgilerin delil sayılmaması gibi birtakım hukuki sonuçlar da belirlenmiştir. Böylece, aslında Anayasa'nın 4. maddesinde sayılan şartları taşıyan bir usuli işlemden elde edilen bilgiler, Teknik Dinleme Kanunu'ndaki şartları karşılamadığı için geçersiz sayılmaktadır[348].

Kanuna uygun bir şekilde dinlemenin yapılmadığı durumlarda, dinleme mağduru olan kişiye Teknik Dinleme Kanunu, iki farklı çare sunmaktadır. Bunlardan ilki usulsüz dinleme ile elde edilen delillerin mahkemede kullanılamaması (delil yasağı) garantisidir[349]. Sunulan çarelerin ikincisi ise, mağdura tazminat davası açma hakkının tanınmasıdır[350].

Donovan-ABD davasında verilen karar, delil yasağı getirilmesinin gerekçesini açıklaması bakımından önemlidir. Anılan karara göre, bilgilerin delil hüviyetini kazanmasının önlenmesi (suppression) uygulaması, iletişimin denetlenmesi tedbirini sadece kanun koyucunun öngördüğü sınırlar dahilinde tutmak niyetinden kaynaklanmaktadır[351].

---

[345] 18 U.S.C. § 2520 (f); STEVENS/DOYLE,s. 8.

[346] 18 U.S.C. § 2517.

[347] 18 U.S.C. § 2520 (g).

[348] AN OVERVIEW OF ELECTRONIC SURVEILLANCE, History and Current Status.

[349] DEPARTMENT OF JUSTICE, Remedies For Violations of Title III; İletişimin denetlenmesi ile elde edilen bilgilerin delil olarak kabul edilmemesi sonucunu doğuran gerekçeler arasında mahkeme kararı için yapılan başvurudaki eksiklikler ya da 'olmazsa olmaz' birtakım unsurların bulunmamasıdır. Örneğin, makul sebep (probable cause) şartı yokluğuna rağmen elde edilen bilgiler delil olarak kabul edilmeyecektir.(AN OVERVIEW OF ELECTRONIC SURVEILLANCE: History and Current Status).

[350] ÖZDOĞAN, (2004), s. 40.

[351] STEVENS/DOYLE, Dp.65.

Delil yasağı kapsamına giren üç hal bulunmaktadır. Bunlar;

- Dinlemenin yasadışı yollardan yapılmış olması[352],
- Verilen mahkeme kararının veya emirin (order of authorization or approval) usule uygun olmaması[353],
- Mahkeme kararında veya emirde belirlenen hususlara dikkat edilmeden dinlemenin yapılmış olmasıdır[354].

Sayılan bu hallerin yanı sıra, doktrinde, delil yasağının uygulanılması gerektiren üç durum daha sayılmaktadır. Bu durumlar[355];

- Dinlenilen görüşmelerin yetkili hakime tam olarak sunulmaması,
- Dinleme sonrasında konuşma kayıtlarının herhangi bir geçerli mazeret olmaksızın usule uygun şekilde mühürlenmemesi,
- Dinleme ile elde edilen bilgilerin, hakkında dinleme kararı çıkarılan kişi(ler) aleyhine kullanılması durumunda, bu kişilere dinlenildiklerine dair bilgi verilmemesi,

halleridir. Teknik Dinleme Kanunu kapsamında açıklanması yasaklanan bilgiler mahkemede veya başka bir devlet organı önünde delil olarak kullanılamaz. Bununla birlikte, delil yasağı prensibinin önemli rol (central role) ve "iyi niyet (good faith) olarak adlandırılan iki önemli istisnası vardır[356]. Önemli rol istisnası ile ilgili olarak, Giordano davasında[357] mahkeme, dinleme kararının, yetkilendirilmiş Baş Savcı Yardımcısı yerine Baş Savcının Baş Yardımcısı tarafından onaylanmış olmasının bu kararla yapılan dinlemelerden elde edilen bilgileri yasal delil olmaktan çıkarmayacağına hükmetmiştir. Mahkemenin bu kararı verirken dayandığı nokta "önemli rol" prensibi olmuştur. Bu ilke uyarınca, yetkili savcı yerine ondan daha kıdemli olan ancak yetkisi olmayan bir savcının imza atması, dinleme ile elde edilen delilin kullanımını yasaklayacak önemde

---

[352] 18 U.S.C. §2518(10)(a)(i).

[353] 18 U.S.C. §2518(10)(a)(ii).

[354] 18 U.S.C. §2518(10)(a)(iii).

[355] ÖZDOĞAN, (2004), s. 40.

[356] ÖZDOĞAN, (2004), s. 40; STEVENS/DOYLE, s. 21-23.

[357] GIORDANO-ABD, 416 u.s. 505 (1974), http://supreme.justia.com/us/416/505/case.html (İET: 12.12. 2007).

bir hata değildir. Aynı şekilde ABD-Donovan (1977) davasında mahkeme, dinleme sonrası dinlenilen (hedef) şahsın dinlenildiğine dair bilgilendirmenin yapılmamasının, hedef şahıs hakkında telafisi mümkün olmayacak önyargılara neden olmaması halinde, dinleme ile elde edilen bilgilerin mahkemede kullanılmasına mani olamayacağı, diğer bir ifadeyle delil yasağını gerektirecek bir durumun oluşmayacağına karar vermiştir. Delil yasağı prensibinin diğer bir istisnası da iyi niyet doktrinidir. ABD-Ojeda Rios (1990) davasında, dinleme sonrasında kaydedilen bilgilerin hemen mühürlenmesi yerine 118 gün sonra mühürlenmesinin her hangi bir kasıttan dolayı yapılmadığı ve görevlilerin iyi niyetli oldukları düşüncesiyle elde edilen delillerin mahkemede kullanılabileceği kararına varmıştır[358]. Donovan davasında Mahkeme, ayrıca, hakkında dinleme kararı verilen kişinin isminin mahkeme kararında sehven yazılmamış olmasının, bu karara istinaden elde edilen delillerin sıhhatine engel olmayacağına hükmetmiştir[359].

Kişisel kayıtlarla elde edilen bilgiler, kolluk kuvvetleri tarafından yapılan kayıtlara kıyasla daha kolay bir şekilde delil hüviyetini kazanmaktadırlar. Nitekim, kolluk güçlerince yapılan iletişimin denetlenmesi esnasında birtakım kurallara riayet zorunlu kabul görülmektedir. Bu kuralları gösteren ve ABD-McKeever davasında belirlenen 7 kriterlik test, kayıtların delil hüviyetini kazanması için gerekli olan doğruluk, aslına uygunluk, güvenilirlik gibi şartları belirlemesi bakımından önemlidir[360].

1977'deki Donovan davasında[361], hakkında dinleme kararı verilen kişiye bilgi verme yükümlülüğü ile ilgili olarak Mahkeme, görevlilerin herhangi bir kasta dayanmaksızın, şüpheliye dinleme işlemiyle ilgili bilgi vermemeleri durumunda, bu durumun dinleme ile elde edilen delillerin sanığın aleyhine kullanılmaması için yeterli sebep oluşturmayacağına karar vermiştir.

---

358 OJEDA RIOS-ABD, 495 U.S. 257 (1990), http://supreme. justia.com /us/495/257/case.html (İET:4.1. 2008).

359 ÖZDOĞAN, (2004), s. 18-19.

360 Bu testteki unsurlar şunlardır: 1-Kayıt cihazı bu bilgileri kayıt kapasitesini haizdir, 2-Operatör cihazı çalıştırabilir bir haldedir. 3- Kayıt aslına sadık ve doğrudur, 4- Kayıt üzerinde herhangi bir silinti, değiştirme veya ekleme yapılmamıştır. 5- Kaydın mahkemeye ibraz edilen hali orijinal olarak muhafaza edilen halidir. 6-Kayıttaki kişiler tespit edilmiştir 7- Kayıt konusu iletişim gönüllü olarak yapılan diyalogların sonucudur, herhangi bir zorlamaya maruz kalmamıştır. (STEVENS/DOYLE,s. 21-23).

361 ÖZDOĞAN, (2004), s. 18-19.

1.2.1.13.Adli Amaçlı İletişime Müdahalenin Denetimi

ABD'de, özel hayata müdahalenin minimum düzeye çekilebilmesi için, bir kısmı uygulamadan bir kısmı ise mevzuattan kaynaklanan birtakım güvenceler sağlanmaya çalışılmıştır. Bu önlemler; genel önlemler, yargı denetimi, yasama denetimi ve kamu denetimi olarak tasnif edilebilir.

1.2.1.13.1.Genel Önlemler

Mahremiyetin ihlal edilmesinin en aza indirilmesini sağlamak bakımından öngörülen tedbirlerden biri, kolluk görevlilerinin, yasadışı sayılabilecek nitelikte bilgiler ortaya çıktığında müdahaleye ara verilmesidir. Bu uygulamayla, mahkeme kararında belirlenen alanın dışına taşan bir içeriğin fark edilmesi durumunda şalter kapatma benzeri bir uygulamayla takibin durdurulmasıdır. Takibi yapan kolluk görevlisinin belli aralıklarla takibe dönüp sakıncalı içeriğin geçip geçmediğini kontrol etmesi gibi takibin yeniden başlatılması için gerekmektedir[362]. Bu uygulama bir fanteziden öteye geçmeyen ve hayatın gerçekleriyle uyuşmayan bir nitelik arzetmektedir. Filtrelemeyi bütünüyle cihazın başında oturan bir kolluk görevlisine teslim etmek, keyfiliğe prim vermek anlamına gelecektir ki, bu da yeknesak sonuçların elde edilmesine engel olabilecektir.

Önlem olarak belirtilebilecek diğer bir faaliyet de, dinlenilen bilgi banda veya benzeri bir cihaza (other comparable device) kaydedilmesidir. Maddede vurgulanan husus; yapılan kaydın, silinmesi ve değiştirilmesi mümkün olmayan bir şekilde gerçekleştirilmesidir[363]. Mahkeme kararı ile belirtilen süre veya verilen ek süre bitiminde, elde edilen kayıtlar mühürlenip derhal yetkili mahkemeye teslim edilir. Burada kullanılan 'dinleme süresinin bitiminde derhal'(immediately after the expiration) ifadesi, yargısal otoritenin meseleye bir an önce vaziyet etmesini sağlamak bakımından önemlidir[364].

ABD'de iletişimin denetlenmesi konusunda tartışılan bir diğer husus da, aile bireylerinin birbirlerinin iletişimine müdahale yetkilerinin olup olmadığıdır. Bu bağlamda, ebeveynin tedip hakkını geniş yorumlayan bazı mahkemeler, reşit olmayan çocuklarının iletişimlerinin ebeveynleri tarafından, yine onların yararları için kayda alınmasını

---

[362] WONG, 3.3.13.

[363] 18 U.S.C. § 2517 (1); WONG, 3.3.14.

[364] 18 U.S.C. § 2518(8) (a); WONG, 3.3.14.

onaylamaktadırlar[365]. Öte yandan, çoğunluk tarafından kabul görmemekle birlikte (Heggy-Heggy, 944 F.2d 1537, 1539 (10th Cir. 1991); Kempf-Kempf, 868 F.2d 970, 972 (8th Cir. 1989); Pritchard-Pritchard, 732 F.2d 372, 374 (4th Cir. 1984)), bazı federal mahkemeler, eşlerden birinin yekdiğerinin iletişimini denetlemesini onaylamaktadırlar[366].

1.2.1.13.2. Yargı Denetimi

İletişimin denetlenmesine ilişkin olarak ABD'de[367] kurulmuş sistem, suiistimallerin önlenmesini sağlamak bakımından yargısal denetime önem vermiştir. Bu denetleme, hem yargının kendi içindeki denetimi hem de yargıya karşı hesap verme şeklinde ortaya çıkmaktadır.

İletişimin denetlenmesine ilişkin olarak mahkeme tarafından verilen karardan, verilmiş kararın uzatılmasına ilişkin karardan ya da bu yöndeki bir talebin reddedildiğine ilişkin karardan itibaren 30 gün içinde ilgili hakim ABD Mahkemeleri İdari Ofisine (İdari Ofis) [368] bir rapor[369] sunar. Raporda aşağıdaki hususların bulunması gerekmektedir[370]:

- İletişimin denetlenmesine ilişkin karar veya uzatma kararı verildiği hususu[371],

---

[365] STEVENS/DOYLE, Dp.46.

[366] STEVENS/DOYLE, s.16-17.

[367] Birleşik Krallık'ta, iletişimin denetlenmesine ilişkin sistemi denetlemek üzere bir de mahkeme ihdas edilmiştir. RIPA'nın 65 vd. maddeleri uyarınca kurulan bu sistem, iletişimin denetlenmesi ile ilgili şikayetleri, örneğin istihbarat memurlarının davranışlarını ya da genel olarak iletişimin denetlenmesi ile ilgili davranışları denetleyen bir mahkeme öngörmüştür. Yüksek yargı mensuplarının üyesi olduğu bu mahkeme, RIPA kapsamında vukubulan iletişimin denetlenmesi ile ilgili şikayetlerin götürüldüğü bir mercidir. Kişinin AİHS haklarının ihlali ile ilgili, özellikle de orantılılık ilkesiyle ilgili şikayetleri değerlendiren mahkemenin tazminata hükmetme yetkisi olduğu gibi, iletişimin denetlenmesi ile ilgili olarak verilmiş bir kararı ortadan kaldırma ya da iptal etme yetkisi de vardır. RIPA'nın 67. bölümü hükmüne göre, bu mahkeme tarafından verilen kararlara karşı yargı yolu açık değildir, yani herhangi başka mahkemeye itiraz başvurusu yapılamaz. FOSTER, Steve; Human Rights and Civil Liberties, Longman, 2003 , s. 389; RIPA, Bölüm:65-70, http://www.opsi.gov.uk/Acts/acts2000/ukpga_20000023_en_2#pt1-ch1-pb1-l1g1 , (İET: 19. 12.2007).

[368] ABD Mahkemeleri İdari Ofisi 1939 yılında kurulmuştur. 18 U.S.C. § 28 U.S.C. 601 sayılı madde ile ihdas edilen bu kurumun başkanı ve başkan yardımcısı Amerikan Yüksek Mahkemesi Başkanı tarafından Hakimler Kurulu'yla (Judicial Conference) yapılan istişare sonrasında atanmaktadır. Bu ofis, mahkemelerin yargısal nitelikte olmayan işlerine bakmakla yükümlüdür. http://www.uscourts. gov/ understand 03/ content7_0.html (İET:25.10.2007).

[369] ABD'de, 2006 yılında hakimler tarafından iletişimin denetlenmesine ilişkin olarak verilen kararlara ilişkin istatistiki bilgiler için Bk. http://www.uscourts.gov/wiretap06/Table22006.pdf 16.11.2007 ; MECHAM, Leonidas Ralph "Report of the Administrative Office of the United States Courts on Applications for Orders Authorizing or Approving the Interception of Wire, Oral, or Electronic Communications" (İET,25.10.2007).

[370] 18 U.S.C. § 2519 (1), W ONG, 3.3.18.

[371] 18 U.S.C. § 2519 (1)(a).

- İletişime yapılan müdahalenin süresi, verilen uzatma kararlarının sayısı ve süreleri[372],
- Tedbire konu olan suç[373],
- Başvuruyu yapan kişinin ve ajansın isimleri ile onay veren kişinin isimleri[374],
- İletişimin müdahalesinin yapıldığı mekan, tesis veya yerin niteliği[375].

İletişimin denetlenmesi için mahkemelere başvuran savcılar da, her yıl Ocak ayında İdari Ofis'e rapor sunmakla yükümlüdürler. Bu raporda; hakimlerin raporunda yer alan hususların yanı sıra aşağıdaki noktalar da raporda yer alır:

- İletişimin denetlenmesi tedbirine konu olan, suçlayıcı niteliği haiz olan ve haiz olmayan materyallerin niteliği ve sıklığı[376],
- İletişimi denetlenen kişilerin sayısı[377],
- Şifreleme (kodlama) içeren mahkeme kararlarının sayısı, bu kodlamanın, kolluk görevlilerini tedbirle elde edilen bütün metine ulaşmaktan alıkoyup koymadığı[378],
- İletişimin denetlenmesi tedbirinde kullanılan toplam insan kaynağının niteliği, sayısı ve maliyeti ile bu tedbir için kullanılan diğer kaynaklar[379],
- İletişimin denetlenmesi tedbiri marifetiyle verilen toplam tutuklama ve mahkumiyet sayısı ile yapılan yargılama sayısı[380].

Öte yandan, iletişimin denetlenmesi kararını veren hakim, bu tedbiri uygulayan makamdan, düzenli aralıklarla, örneğin 10 günde bir, düzenli raporlar sunmasını

---

[372] 18 U.S.C. § 2519 (1),(d).

[373] 18 U.S.C. § 2519 (1),(e).

[374] 18 U.S.C. § 2519 (1),(f).

[375] 18 U.S.C. § 2519 (1),(g).

[376] 18 U.S.C. § 2519 (2)(b)i, ii.

[377] 18 U.S.C. § 2519 (2)(b)iii.

[378] 18 U.S.C. § 2519 (2)(b)iv.

[379] 18 U.S.C. § 2519 (2)(b)v.

[380] 18 U.S.C. § 2519 (2)(b)c,d,e,f.

isteyebilir[381]. Bu raporlar iletişimin denetlenmesine ilişkin aşamalar hakkında bilgi verdiği gibi aynı zamanda hakkında tedbir uygulanan kişiye tanınmış bir güvencedir[382].

1.2.1.13.3. Yasama Denetimi

Amerikan Kongresi[383] iletişimin denetlenmesi işlemleri hakkında denetleme yapmaktadır. Bu denetim iki türlüdür:

1.2.1.13.3.1.Parlamento Denetimi

Adalet ve İstihbarat Komitesi oturumlar açmak ve kolluğun cevaplaması için sorular sormak suretiyle bu sürece dahil olmaktadır. İletişime yönelik müdahaleler aynı zamanda Kongrenin Daimi İstihbarat Komitesi[384] ile Senato'nun İstihbarat Komitesi[385] tarafından da denetlenmektedir. Bu iki komite istihbarat kaynaklarının kötüye kullanılıp kullanılmadığını ve istihbarat faaliyetlerinin yasal bir şekilde yapılıp yapılmadığını denetlemektedir[386]

1.2.1.13.3.2. Kongreye Rapor Verme Zorunluluğu

ABD Mahkemeleri İdari Ofisi (Administrative Office) Başkanı, iletişimin denetlenmesi hususunda yapılan başvurular, bir önceki yılda verilen mahkeme kararlarına ilişkin istatistik ile veriler hakkındaki analizi ihtiva eden bir raporu her yıl Nisan ayında Kongreye sunar[387].

Teknik Dinleme Kanunu, İdari Ofis'in, Kongre'ye iletişimin denetlenmesi hususunda yapılan başvuruları ve verilen kararları istatistiksel bilgi çerçevesinde takdim eden bir rapor hazırlamasını öngörmüştür. Bu raporda, soruşturma konusu suçlar türü, iletişimin

---

[381] 18 U.S.C. § 2518(6).

[382] WONG,3.3.16.

[383] Birleşik Krallık'ta da bir rapor sistemi bulunmakla birlikte, bu sistem ABD'de varolan sistemden farklıdır. Malone davasında ihlal kararı verilmesi sonrasında Birleşik Krallık, iletişimin denetlenmesi kurumunu ciddi bir revizyona tabi tutmuş, bu bağlamda, bu tedbirin kötüye kullanılmasını engellemek bakımından birtakım tedbirler getirilmiştir. Bu tedbirlerden ilki yasama denetimidir. Bu bağlamda, yüksek bir yargısal görevde bulunan bağımsız bir görevli (Interception of Communications Officer) Başbakan aracılığıyla Parlamento'ya iletişimin denetlenmesine ilişkin sistemle ilgili bir rapor verir. RIPA, Bölüm:57;http://www. opsi.gov.uk/Acts/acts2000/ukpga_20000023_en_2#pt1-ch1-pb1-l1g1, (İET:19.12.2007); FOSTER, s.389.

[384] HOUSE PERMANENT SELECT COMMITTEE ON INTELLIGENCE, http://intelligence. house.gov/ AboutTheCommittee. aspx? Section=1 (İET:25.10.2007).

[385] SENATE SELECT COMMITTE ON INTELLIGENCE, http://intelligence.senate.gov/ (İET:25.10.2007).

[386] WONG, 3.2.6.

[387] 18 U.S.C. § 2519 (2).

denetleneceği yer, bu tedbirin maliyeti, bu tedbirin uygulanması ile gerçekleştirilen tutuklama, yargılama ve mahkumiyetlerin sayısı hakkında bilgi bulunur[388].

1.2.1.13.4. Adli Amaçlı İletişimin Denetlenmesinde Bireysel Şikayet

İletişimi takip altına alınmış kişi; bir mahkeme, bir bölüm, bir görevli, bir ajans, vs. tarafından yapılan bir soruşturma, kovuşturma, yargılama gibi bir süreç esnasında iletişimin denetlenmesi yoluyla elde edilmiş bilgilerin, iletişim içeriklerinin (contents of the intercepted communication) ortadan kaldırılmasını (suppression) talep edebilir. Bu bağlamda ilgili kişi, iletişiminin yasadışı olarak takip altına alındığını[389] veya bu konuda verilen emir veya mahkeme kararının yetersiz olduğunu[390] ya da yapılan denetlenmenin verilen emre veya mahkeme kararına uygun olarak yapılmadığını[391] dile getirerek talepte bulunabilir[392]. Bu başvuru kabul edildiği takdirde, tedbirle elde edilen bilgiler, 'Kablolu ve Elektronik İletişim ile Sözlü İletişim' başlıklı bölüm[393] hükümlerinin ihlal edilmesi suretiyle elde edilmiş kabul edilecektir. Hakim, adalet açısından muhik bir yarar gördüğü takdirde, iletişimin takip altına alınmasından mutazarrır olduğunu beyan eden kişi veya avukatına, takip altına alınmış, denetlenmiş iletişim parçalarına veya bu parçalardan elde edilmiş delillere ulaşma imkanı verebilir[394].

---

[388] 2006 REPORT OF THE DIRECTOR OF THE ADMINISTRATIVE OFFICE; 2006 yılında eyalet ve federal düzeyde toplam olarak gerçekleştirilen 1839 iletişimin denetlenmesi vakası 2005 yılı rakamlarına göre yüzde 4'lük bir artışa tekabül etmektedir. Federal yetkililer tarafından yapılan başvuruların sayısı geçen yıla oranla yüzde 26 oranında düşerek 461 olmuş, eyalet kovuşturma görevlileri tarafından yapılan başvurular ise yüzde 20 artarak 1378'e çıkmıştır.2006 yılında yapılan iletişimin denetlenmesi ortalama 40 gün sürmüştür. Bu rakam 2005 yılında 43 gün olarak gerçekleşmiştir. 2006 yılında hakkında iletişimin denetlenmesi tedbiri uygulanan kişi sayısı geçen yıla göre artarak 107'den 122'ye çıkmıştır. Suçlayıcı bilgiler ihtiva eden iletişimin denetlenmesi oranı geçen yıla oranla yüzde 2 düşerek yüzde 20 olmuştur. Her iki yılın rakamların mukayesesi için ayrıca Bk. 2005 REPORT OF THE DIRECTOR OF THE ADMINISTRATIVE OFFICE OF THE UNITED STATES COURTS ON APPLICATIONS FOR ORDERS AUTHORIZING OR APPROVING THE INTERCEPTION OF WIRE, ORAL, OR ELECTRONIC COMMUNICATIONS, April 2006, http://www.uscourts.gov/wiretap05/WTText.pdf(İET: 23.11.2007).

[389] 18 U.S.C. § 2518 (10) (a) (i).

[390] 18 U.S.C. § 2518 (10) (a) (ii).

[391] 18 U.S.C. § 2518 (10) (a) (iii).

[392] Bk. WONG,3.3.23.

[393] Chapter 119—Wire And Electronic Communications Interception And Interception Of Oral Communications, http://www4.law.cornell.edu/uscode/html/uscode18/usc_sup_01_18_10_I_20_119.html (İET:29.10.2007).

[394] 18 U.S.C. § 2518 (10) (a)(III) 'The judge,… may in his discretion make available to the aggrieved person or his counsel for inspection such portions of the intercepted communication or evidence…' .

1.2.2. Numara ve Rota Tespit Kanununa Göre İletişimin Tespiti

1.2.2.1.Numara ve Rota Tespiti Kavramı ve Kapsamı

Teknik Dinleme Kanunu, hükümet görevlilerine gerçek zamanlı ve depo edilmemiş kablolu ya da elektronik iletişim içeriğini denetleme imkanı tanımakta iken, Numara ve Rota Tespit Kanunu ise gerçek zamanlı olmak kaydıyla adresleme bilgileri ve içerik dışı bilgileri tespitle ilgili hükümler ihtiva etmektedir.

Numara ve Rota Tespit Kanunu[395] (The Pen/Trap Statute), Teknik Dinleme Kanunu ve FISA'dan farklı olarak kablolu ve elektronik iletişime ait adresleme ve sair içerik dışı(non-content) bilgilere ilişkin bir yasal düzenlemedir[396]. Gerçek zamanlı[397] (real-time) olması gereken bu bilgiler, aynı zamanda Teknik Dinleme Kanunu gibi bilginin iletimi (transmission) esnasında elde edilen depo edilmemiş bilgilerdir[398]. Bu kanun, Teknik Dinleme Kanunu ve FISA'ya nazaran daha ılımlı (less stringent) hükümler içermektedir[399].

Numara ve rota tespit bilgilerinin anayasal koruma altında olup olmadığı hususunda verilen 1979 tarihli Smith-Maryland davasında Yüksek Mahkeme, numara ve rota tespit cihazlarının kolluk tarafından kullanılmasının, ABD Anayasa'sının 4. maddesiyle koruma altına alınan özel hayat hakkını kısıtlamadığına karar vermiştir. Mahkemenin, içerik dışı olarak tanımladığı bu bilgiyi 'yasal mahremiyet beklentisi' dışında kabul etmesine[400] tepki olarak Kongre, 1986 yılında Numara ve Rota Tespit Kanununu çıkarmıştır. Bu kanun ile, 1968 tarihli Teknik Dinleme Kanunu'nda öngörülmemiş olan içerik dışı bilgilerle ilgili düzenleme yapılmış ve bir yasal boşluk doldurulmuş oldu. 2001 tarihli Patriot Kanunu ile bu kanunda yapılan değişiklikle de, (tuşlama) dialing, yönlendirme (routing), adresleme (addressing) veya sinyal (signaling) bilgileri (dras bilgileri) bu kanun kapsamına sokuldu[401].

---

[395] 18 U.S.C. § 3121-3127 maddelerinde düzenlenmiştir. Bk. (Title 18 > Part II > Chapter 206, http://www4.law.cornell.edu/uscode/ search/display.html? terms=3121&url= /uscode/ html/ uscode18/ usc_sec_18_00003121----000-.html (İET:15.10.2007); MacARTHUR, s.3 .

[396] Bk. AN OVERVIEW OF ELECTRONIC SURVEILLANCE, History and Current Status.

[397] WONG, 3.2.6.

[398] SCHWARTZ, The Pen Register Act, The Statistics; DEPARTMENT OF JUSTICE, Pen/Trap Statute; MADDOX, s. 339.

[399] WONG, 3.5.1.

[400] SCHWARTZ,The Pen Register Act, The Statute.

[401] SCHWARTZ, The Pen Register Act, The Statute; Dinamik olmayan IP adresleri DRAS bilgilerine örnek olarak verilebilir.(SCHWARTZ, The Pen Register Act, The Statute).

Genel hatlarıyla ifade etmek gerekirse, telefon numarası tespit cihazı (pen register[402]), giden aramalara ilişkin bilgileri , rota tespit cihazı (trap and trace device[403]) ise gelen aramalara ilişkin bilgileri kaydeden cihazlardır. Her ne kadar kanunda, telefonla yapılan haberleşmelere referansta bulunulmuş ise de, birçok mahkeme, bu kanunun bilgisayar marifetiyle yapılan haberleşmelere[404] de şamil olduğuna karar vermiştir[405]. Nitekim, 2001 tarihli Patriot Kanunu, Numara ve Rota Tespit Kanunu'nun geniş çapta iletişim teknolojilerine uygulanacağını teyit etmiştir[406].

Kanun'da geniş tanımlara[407] yer verilmiştir. Tanımların bu kadar geniş tutulması, anılan kavramlara ilişkin unsurların kapsamından kaynaklanmaktadır[408]. Üzerinden kablolu veya elektronik bir iletişim aktarılan cihaz ifadesi geniş bir alanı kaplamakta olup; sabit telefon, cep telefonu, İnternet kullanıcı hesabı, elektronik posta hesabı veya IP adresi bu kapsama girmektedir. Öte yandan, tanımda geçen tüm tuşlama (dialling), routing (yönlendirme), adresleme (addressing) ve sinyal (signalling) bilgileri ifadesi hemen hemen tüm içerik dışı bilgileri karşılamaktadır. Diğer bir önemli nokta ise, gerek 'pen register' ifadesinin gerekse 'trap' ifadesinin hem bir cihazı hem de bir yazılım sürecini ifade etmek için kullanılmış olmasıdır. Bu tanımlamaların kapsamının geniş tutulmuş olması nedeniyle, savcılar ve kolluk görevlileri bazı cihazların bu cihazlar kapsamına girip girmediklerinin değerlendirilmesi hususunda 'Bilgisayar Suçları ve Fikri Haklar Bölümü'nden görüş almaları gerekmektedir[409]. Bununla birlikte; pen register ifadesi,

---

[402] 18 U.S.C. § 3127(3).

[403] 18 U.S.C. § 3127(4).

[404] İnternet başlıklarında (header) hem gelen hem de giden bilgiler bulunduğundan, tüm başlığı okuyan bir cihaz bir numara ve rota tespit cihazı olarak adlandırılabilir. Bununla birlikte, tüm başlığın(entire heading) kapsamına konu başlığı(subject line) girmemektedir. (DEPARTMENT OF JUSTICE, Pen/Trap Statute).

[405] 18 U.S.C. § 3127(3); DEPARTMENT OF JUSTICE, Pen/Trap Statute; SCHWARTZ, The Pen Register Act, The Statute.

[406] Bk. Patriot Kanunu 216. madde ,115 Stat. 272, 288-90 (2001).

[407] Numara tespit cihazı olarak adlandırılan 'pen register' ifadesi 'device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication' olarak tanımlanmıştır. 'Trap and trace device' ise, 'a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication' olarak tanımlanmıştır. Bk. 18 U.S.C. § 3127 (3), 18 U.S.C. § 3127 (4).

[408] WONG, 3.2.6.

[409] DEPARTMENT OF JUSTICE, Pen/Trap Statute.

kablolu veya elektronik iletişimin sağlayıcısı veya müşterisi tarafından faturalandırma amacıyla kullanılan cihazı veya süreci kapsamaz[410].

Normal şartlar altında, bir numara veya rota tespiti yapılması gerektiğinde kolluk güçleri mahkeme kararını ilgili servis sağlayıcısına iletir ve gerekli tespitin yapılmasını ister. Ancak, servis sağlayıcının bunu yapamadığı hallerde veya bazı nadir durumlarda, kolluk güçleri DCS 1000[411] gibi cihazları kurabilir. Bu gibi hallerde, hükümet, aşağıdaki bilgileri mühürlenmiş olarak 30 gün içinde mahkemeye ibraz etmek zorundadır[412]:

- Cihazı kuran veya cihaza giriş yapan görevlinin kimliği[413],
- Cihazın kurulma ve sökülme tarihi ile cihaza giriş tarihleri, cihaza yapılan girişlerin toplam süresi[414],
- Cihazın kurulma zamanındaki konfigürasyonu ile bu konfigürasyonda daha sonra yapılan değişiklikler[415],
- Bu cihaz marifetiyle elde edilen deliller[416].

---

[410] '…but such term does not include any device or process used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device or process used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business…' 18 U.S.C. § 3127(3).

[411] DCS1000, eski adı Carnivore (etobur) olan bir dijital toplama sistemine verilen addır. Bu sistemle, kolluk güçleri, takibat altındaki kişilerin internet haberleşmelerini izlemektedir. Ancak işin çarpıcı tarafı, internet servis sağlayıcılarının bilgisayarına yerleştirilen bu sistem marifetiyle, FBI'ın takibatı altında olmayan kişilerin elektronik mesajları da alınabilmektedir. LUENING, Erich, "Don't be fooled: DCS 1000 still a 'Carnivore' at heart", http://news.zdnet.com/2100-9595_22-528089.html, (İET:4.10.2007) Carnivore adını taşıyan bir sistemi içeren bir program marifetiyle tüm İnternet erişim şirketleri ağlarının özel bir bilgisayara bağlanması hedeflenmiştir. Kullanıcıların İnternetten alıp verdiği tüm bilgilerin (e-postalar, ziyaret edilen İnternet siteleri vs.) bir ana bilgisayarda kaydedilmesini ve arşivlenmesini sağlayacak bu sistemle özel kelimeleri barındıran yazışmalar, sakıncalı sitelere ziyaretler, şüpheli şahıslara yollanan mektuplar, anında fişlenmeye ve daha 'detaylı' takibe yol açacaktı. Bu projenin kamuya sızmasıyla Carnivore'un yerine ikame edildiği iddia edilen DCS-1000 resmen kabul edilmiş değildir. Bu şekilde bilgi topladığı iddia edilen diğer bir program ise Magic Lantern adını taşıyor. ABD'de bir mafya ailesi ile yapılan mücadele esnasında, liderin, örgütü PGP adlı yazılımla şifrelediği e-postalarla yönettiği anlaşılınca, klavyeye Magic Lantern adlı bir işlemci yerleştirildi. Bu program ile basılan her tuş kaydedilip FBI ajanlarına e-postayla iletiliyordu. Şifrelerinin yanı sıra mektuplar, yazılan web adresleri gibi yığınla değerli bilgi FBI'a akıyordu. Örgüt bu şekilde çökertildi ancak mahkeme bu belgelerin yasal olarak toplanıp toplanmadığını öğrenmek için FBI'ı sorgulayınca Magic Lantern de ortaya çıkmış oldu. KUZULOĞLU, M. Serdar "Dikkat, e-kulaklar işbaşında!", Radikal, 06/07/2002, (İET:4.10.2007).

[412] DEPARTMENT OF JUSTICE, Pen/Trap Orders.

[413] 18 U.S.C. § 3123(a)(3)(A)(i).

[414] 18 U.S.C. § 3123(a)(3)(A)(ii).

[415] 18 U.S.C. § 3123(a)(3)(A)(iii).

[416] 18 U.S.C. § 3123(a)(3)(A)(iv).

Numara ve rota tespit cihazının kurulması esnasında, kablolu veya elektronik iletişimin içeriğinin kayda alınması veya deşifre edilmesinin önlenmesini mümkün kılacak teknolojinin kullanılması zorunluluğu getirilmiştir[417].

1.2.2.2. Başvuru Şartları

Numara ve rota tespitine ilişkin karar alınabilmesi için, başvuran görevlileri ve de bağlı bulundukları kurumu, yaptıkları fonksiyonlar itibariyle tanıtan bir başvuru[418] yapılması gerekmektedir. Yemin ya da affirmation tahtında[419] yapılan başvuruda, talep edilen tedbir ile devam eden bir ceza soruşturması[420] arasında bir bağlantı olduğu kanaatinin[421] ortaya konulması gerekmektedir.[422] Başvuruyu yapacak kişi;

- Federal suçlarda Hükümet adına görevlendirilmiş bir savcı[423],
- Eyalet bazında da söz konusu eyalet adına görevlendirilmiş soruşturmacı ya da kolluk görevlisidir[424].

Başvuru dilekçesinde Hükümet adına başvuruyu yapan savcının ismi ve tedbire konu soruşturmayı yürüten kolluk görevlisinin ismi[425] ile elde edilmesi muhtemel olan bilgilerin sürdürülen soruşturma ile ilgili olduğuna ilişkin bir serfitika bulunmalıdır[426].

1.2.2.3. Mahkeme Kararı

Numara ve Rota Tespit Kanunu çerçevesinde yetkili mahkemeye[427] yapılmış bir başvuru yapılması halinde, ilgili mahkeme gerekli unsurların varlığına ilişkin olarak

---

[417] 18 U.S.C. § 3121(c); DEPARTMENT OF JUSTICE, Pen/Trap Orders.

[418] 18 U.S.C. § 3122(b)(1).

[419] 18 U.S.C. § 3122(a)(1).

[420] 18 U.S.C. § 3122(b)(2)).

[421] 18 U.S.C. § 3122(b) (2). 'a certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency.' Bu hususu teyit eden diğer bir hüküm 3123 (a)(2)'de yer almaktadır '…the court shall enter an ex parte order authorizing the installation and use of a pen register or trap and trace device within the jurisdiction of the court, if the court finds that the State law enforcement or investigative officer has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation'.

[422] DEPARTMENT OF JUSTICE, Pen/Trap Statute; WONG,3.5.3; SCHWARTZ, The Pen Register Act, The Statute.

[423] 18 U.S.C. § 3122(a)(1).

[424] 18 U.S.C. § 3122(a)(2).

[425] 18 U.S.C. § 3122(b)(1).

[426] 18 U.S.C. § 3122(b)(2).

[427] 18 U.S.C. § 3127(2)(a).

yaptığı araştırma sonucunda numara ve/veya tespit cihazının kurulması ve kullanılmasına ilişkin kararı verir. Mahkeme, başvuru dilekçesinde sunulan unsurların doğruluğunu anlamak bakımından yargısal bir soruşturma yapmak durumunda değildir[428]. Bu kanun çerçevesinde alınacak bir mahkeme kararı, çok sıkı şartlara bağlanmış Teknik Dinleme Kanunu'na kıyasla daha hafif bir usul getirmiştir[429]. Numara ve rota tespitine ilişkin kararın gerekliliği ve hukukiliğini denetleyecek olan kurum Adalet Bakanlığıdır. Mahkeme Adalet Bakanlığının (Attorney General) bu hususstaki olumlu beyanı ve talebi üzerine[430] hüküm tesis eder[431]. Numara veya rota tespit kararı herhangi bir federal savcı tarafından talep edilebilir ve herhangi bir yer mahkemesi (any federal district judge or magistrate) tarafından bu taleple ilgili karar verilebilir. Eyaletler müracaatta bulunacak makamları tayin edebilirler. Kanunda belirtilen şartların varlığı halinde mahkeme mutlaka kabul kararı vermek zorundadır[432]. İçeriğe ilişkin denetleme talepleri hakkında karar veren mahkeme ise kabul ya da red şeklinde karar verebilir, yani takdir mahkemeye bırakılmıştır ('…If the request meets the statutory requirements, the court must grant the order. By contrast, interception orders are subject to the judge's discretion'...). Konuyla ilgili başvuruda makul sebeplerin olduğunu gösteren olgusal anlatım zorunlu değildir. Makul sebebin varolduğunu beyan sadedinde bir sertifika yeterlidir. Mahkeme kararı aldırılmasının amaçlarından birisi, servis sağlayıcılarını kendi aralarında bir işbirliği yapmaya zorlamak ve onları sivil ve cezai sorumluluktan kurtarmaktır[433]. 1997 tarihi itibariyle numara ve/veya rota tespit kararı çıkarılmasına yönelik hiçbir başvuru reddedilmiş değildir[434].

---

[428] DEPARTMENT OF JUSTICE, Pen/Trap Statute; SCHWARTZ, The Pen Register Act, The Statute.

[429] Numara ve rota tespiti cihazlarının kullanımında ciddi bir artış gözlemlenmektedir. 1995 yılında, federal düzeyde, 7899 kişiyi etkileyen toplam 3414 numara tespiti (pen register) yapılmıştır. Toplam 3902 kişiyi etkileyen ve aynı yılda yapılmış rota tespiti (trap and track) sayısı ise 1558'e ulaşmıştır. (DEMPSEY, "Communications Privacy In The Digital Age: Revitalizing The Federal Wiretap Laws To Enhance Privacy").

[430] 18 U.S.C. § 3123(a)(1).

[431] "The judicial role in approving use of trap and trace devices is ministerial in nature." DEPARTMENT OF JUSTICE, Pen/Trap Statute; EFF ANALYSIS OF PATRIOT ACT.

[432] EHRLICH, s. 8; EFF ANALYSIS OF PATRIOT ACT ; SCHWARTZ, The Pen Register Act, The Statute; New York Telephone Co-ABD, 434 U.S. 159 (1977) kararında Yüksek Mahkeme, numara ve rota tespit cihazları ile elde edilen bilgilerin sınırlı kapsamına vurgu yapmış ve bu cihazların kurulması ile elde edilen bilgilerin iletişimin içeriği, kişilerin kimlikleri, vs.hakkında kolluk görevlilerine bilgi sağlamadığını ifade etmiştir. Mahkemeye göre, numara ve rota tespit cihazı ile elde edilecek bilgilerin soruşturmayla ilgili olduğu yönündeki savcı beyanının (certification) varlığı halinde hakim, bu cihazın kurulmasına karar vermek zorundadır.(THE USA PATRIOT ACT, EPIC Report.).

[433] AN OVERVIEW OF ELECTRONIC SURVEILLANCE: History and Current Status.

[434] DEMPSEY, "Communications Privacy In The Digital Age: Revitalizing The Federal Wiretap Laws To Enhance Privacy".

Numara ve rota tespiti kararı en fazla 60 günlük bir süre için verilebilir[435]. Bununla birlikte bu 60 günlük sürenin uzatılabilmesi, 18 U.S.C. § 3122 no'lu maddeye göre tanzim edilmiş bir başvurunun olması şartıyla mümkündür[436]. Verilecek uzatma 60 günü geçemez[437].

Numara ve rota tespitine ilişkin mahkeme kararı, kararı veren mahkemenin bulunduğu yer dışında da geçerlidir. Bu hüküm, 11 Eylül olayları akabinde çıkarılan Patriot Kanunu'yla getirilmiştir. Daha önceden bu karar, sadece mahkemenin yargı çevresinde geçerliydi[438]. Federal düzeyde bir başvuru olması durumunda, verilen mahkeme kararı, ilgili kablolu veya elektronik servis sağlayıcılarını bağlar[439]. Örneğin, federal bir savcının talebi doğrultusunda bir telefondan yapılan aramaların izlenmesi hususunda verilen bir mahkeme kararı sadece o hattı hizmete açmış olan servis sağlayıcı bölgesel şirketi değil, aynı zamanda geniş kapsamlı hizmet sunan servis sağlayıcılarını ve diğer eyaletlerin bölgesel servis sağlayıcılarını da kapsar. Yani telefon görüşmesinin yapılmasında aracılık yapan tüm şirketler hakkında bu karar geçerlidir[440].

Verilen mahkeme kararında, ilk servis sağlayıcının belirtilmesi yeterlidir. İlk servis sağlayıcı dışındakilerin isminin belirtilmesi zorunlu değildir[441]. Kolluk güçlerinin yapması gereken şey, ilgili mahkeme kararını servis sağlayıcıya ibraz etmektir. Servis sağlayıcının talep etmesi halinde, kolluk güçleri, kararın bu servis sağlayıcıya şamil olduğunu gösteren 'yazılı veya elektronik bir belge' takdim etmek zorundadırlar[442]. Böyle bir uygulamanın altında yatan temel neden, kolluk kuvvetlerinin ilerleyen aşamalarda soruşturmanın nerelere ulaşacağını baştan bilemeyecek olmaları gerçeğinden kaynaklanmaktadır. Gerçekten de, soruşturmanın her bir safhasında yeni bir durumla karşı karşıya kalan kolluk kuvvetlerinin her bir yeni durumda yeni bir servis

---

[435] 18 U.S.C. § 3123(c)(1).

[436] 18 U.S.C. § 3123(c)(2).

[437] WONG: 2005, 3.5.6; EHRLICH, s. 8.

[438] EHRLICH, s. 8.

[439] 18 U.S.C. § 3123(a)(1).

[440] DEPARTMENT OF JUSTICE, Pen/Trap Orders; Benzer bir durum internet servis sağlayıcıları için de geçerlidir. Federal savcı, bir bilgisayara veya IP adresine giren iletişimleri takip için karar aldırmışsa, bir bilgisayar korsanı tarafından bu mağdur bilgisayara yapılan haksız fiile aracılık eden tüm bilgisayarlar bu takip kapsamına girerler. (DEPARTMENT OF JUSTICE, Pen/Trap Orders).

[441] 18 U.S.C. § 3123(b)(1)(A).

[442] 18 U.S.C. § 3123(a)(1).

sağlayıcının ismini mahkemeye ibraz etmeleri durumunda soruşturmaların önemli bir ölçüde gecikmesi kaçınılmaz olacaktır[443].

Numara ve Rota tespit Kanunu çerçevesinde verilmiş kararda, üçüncü kişilerin CALEA Kanunu[444] kapsamında iletişime ilişkin denetimin yapılması noktasında yetkililere yardımı[445] öngörülebilir[446].

1.2.2.4. Mahkeme Kararı Olmaksızın İletişimin Tespiti

Teknik Dinleme Kanunundaki uygulamanın bir benzeri Numara ve Rota tespit kanununda da yer almaktadır. Adalet Bakanlığının üst düzey bir yetkilisi[447] tarafından belirlenmiş bir kolluk görevlisinin acil hallerde mahkeme kararı olmaksızın, numara ve/veya rota tespiti yapması mümkündür[448].

Mahkeme kararı olmaksızın numara ve rota tespiti yapılabilmesi için en az bir yıl hapis cezasını gerektiren bir suç olması ve hakkında tedbir uygulanması talep edilen suçun, bir kişiye yönelik hayati tehlikeyi veya ciddi fiziksel yaralanmayı[449], organize suçlarla ilgili bir komployu[450], milli güvenlik çıkarlarını tehdit eden bir komployu,[451], korunan bir bilgisayara karşı devam eden bir komployu[452] içermesi gerekmektedir[453].Bu kurumun hayata geçirilebilmesinin diğer bir şartı da, tespitin başlamasından itibaren 48 saat içinde mahkeme kararı alınması için başvuruda bulunulmasıdır[454].

Mahkeme kararının yokluğunda yapılan denetleme, hedeflenen bilgi elde edildiğinde veya mahkeme kararı için yapılan başvuru reddedildiğinde biter. Bu hallerden hangisi

---

[443] DEPARTMENT OF JUSTICE, Pen/Trap Orders.

[444] CALEA Kanunu için Bk. 18 U.S.C. § 2522, Communications Assistance for Law Enforcement Act, http://www4.law.cornell.edu/uscode/search/display.html?terms=2522&url=/uscode/html/uscode18/usc_sec_18_00002522----000-.html (İET:3.11.2007).

[445] 18 U.S.C. § 3124(f).

[446] WONG, 3.5.5.

[447] 18 U.S.C. § 3125 (a) '…Attorney General, the Deputy Attorney General, the Associate Attorney General, any Assistant Attorney General, any acting Assistant Attorney General, or any Deputy Assistant Attorney General, or by the principal prosecuting attorney of any State or subdivision thereof acting pursuant to a statute of that State…'

[448] WONG,3.5.7.

[449] 18 U.S.C. § 3125(a)(1)(A).

[450]18 U.S.C. § 3125(a)(1)(B).

[451] 18 U.S.C. § 3125(a)(1)(C).

[452] 18 U.S.C. § 3125(a)(1)(D).

[453] WONG, 3.5.7.

[454] 18 U.S.C. § 3125(a)(2); WONG, 3.5.7.

önce gerçekleşirse dinleme o zaman sona ermiş sayılır[455]. Kolluk görevlileri tarafından bir numara veya rota tespit cihazının, 48 saat içinde mahkemeye başvuru yapılmaksızın, bilerek kurulması ve kullanılması halinde bu işlem yasadışı sayılacaktır[456]. Bu hizmetin yerine getirilmesi esnasında kaynaklanan masraflar için, servis sağlayıcı ve diğer ilgililere gerekli ödeme yapılacaktır[457].

1.2.2.5. Servis Sağlayıcının Sorumluluğu

Mahkeme kararı servis sağlayıcıya birtakım sorumluluklar yüklemektedir. Bunlardan ilki, tespit ile elde edilen bilginin mahkeme aksini kararlaştırmadığı takdirde mühürlenmesidir.[458] İkinci yükümlülük ise, numara ve/veya rota tespiti yapıldığının gizli tutulması zorunluluğudur. Mahkeme aksini kararlaştırabilir[459]. Üçüncü bir yükümlülük ise, numara ve rota tespit cihazlarının kurulması amacıyla gerekli olan her türlü yardımın yapılmasıdır[460].

Bununla birlikte, 3124 hükmü çerçevesinde numara ve rota tespit cihazlarının kurulması esnasında kolluk görevlilerine yardım etmek yükümlülüğünde olan servis sağlayıcıları, görevlilere yardım esnasında doğmuş olan masrafların karşılanmasını talep edebilirler[461]. Mahkeme kararını uygulayan ve bu kapsamda iletişime ait numara ve rota tespit bilgilerini açıklayan servis sağlayıcı ve çalışanları hakkında kolluk kuvvetlerine yaptığı yardımdan dolayı dava açılamaz[462].

Mahkeme, 2522[463] nolu madde hükmü çerçevesinde, CALEA kanunu hükümlerinin uygulanması için bir karar çıkarabilir[464].

---

[455] 18 U.S.C. § 3125(a)(2)(b).

[456] 18 U.S.C. § 3125(a)(2)(c).

[457] 18 U.S.C. § 3125(a)(2)(d).

[458] 18 U.S.C. § 3123(d)(1).

[459] 18 U.S.C. § 3123(d)(2).

[460] 18 U.S.C. § 3124(a), (b).

[461] 18 U.S.C. § 3124((c).

[462] 18 U.S.C. § 3124((c)(d).

[463] 18 U.S.C. § 2522 (a) “Enforcement by Court Issuing Surveillance Order” (İletişimin Denetlenmesine İlişkin Mahkeme Kararınının İnfazı) başlıklı madde.

[464] 18 U.S.C. § 3124(f).

1.2.2.6.Yasadışı Numara ve Rota Tespitinin Yaptırımı

Kanun koyucu, Numara ve Rota Tespit Kanunu veya FISA uyarınca verilmiş bir mahkeme kararı olmaksızın numara ve rota tespiti yapılmasına ilişkin genel bir yasak getirmiştir[465]. Bu yasağa kasten riayet etmeyenler bir yıla kadar hapis veya para cezasına veya bu cezaların ikisine birden mahkum edilebilirler[466].

Bununla birlikte, numara veya rota tespit cihazının kablolu veya elektronik servis sağlayıcı tarafından kullanılması durumunda veya kullanıcının rızasının mevcudiyeti halinde cezai yaptırımdan muafiyet getirilmiştir. Bunun yanı sıra, numara ve rota tespiti; servis sağlayıcının haklarının veya kablolu iletişimin tamamlanmasına yardım eden başka bir servis sağlayıcının korunması amacıyla yapıldığı takdirde yine cezai hükümler uygulanmayacaktır[467].

1.2.2.7.Numara ve Rota Tespiti İşlemlerinin Denetimi

Numara ve Rota Tespiti Kanunu, müdahalenin denetimi bağlamında Teknik Dinleme Kanunu'na kıyasla daha gevşek hükümler içermektedir. Bu durum, Teknik Dinleme Kanunu'nun taalluk ettiği hürriyet kısıtlamalarının ciddi boyutlarda olmasından, başka bir anlatımla Numara ve Rota Tespit Kanununda öngörülen hak kısıtlamalarının daha yüzeysel bilgilere yani iletişim bilgileri olarak adlandırdığımız adresleme ve sair içerik dışı (non-content) bilgilere ilişkin olmasından kaynaklanmaktadır.

1.2.2.7.1.Numara ve Rota Tespit Cihazlarının Varlığının Açıklanamaması

Mahkeme kararı ile yapılan tespitle elde edilen kayıtlar mühürlenir ve mahkeme kararından itibaren 30 gün içinde numara ve rota tespit cihazının kurulması ve kullanılması kararını veren mahkemeye sunulur[468]. Servis sağlayıcı (mülkiyet sahibi veya kiralayan) ve yardım etmekle yükümlü kişiler, cihazın kurulduğu ve kullanıldığını ayrıca bir soruşturmanın var olduğunu aboneye veya üçüncü kişilere açıklayamazlar[469]. Mahkemenin aksini kararlaştırması hali[470] saklıdır[471].

---

[465] 18 U.S.C. § 3121(a).

[466] 18 U.S.C. § 3121(d).

[467] 18 U.S.C. § 3121(b).

[468] 18 U.S.C. § 3123(a)(3)(B).

[469] 18 U.S.C. § 3121(d)(2).

[470] 18 U.S.C. § 3123)(d)(1).

[471] WONG, 3.5.9.

Numara ve Rota Tespit Kanunu çerçevesinde çıkarılmış mahkeme kararları, Teknik Dinleme Kanunu'nda olduğu gibi düzenli olarak kamuoyuna açıklanmamaktadır. Ancak EPIC (Electronic Intelligence Privacy Center) 1987-1998 yılları arasındaki numara ve rota tespit kararlarını ve kararlar akabinde verilen uzatma kararlarını yayınlamıştır[472]. Aşağıdaki tablodan[473] da görüleceği üzere 1987 yılında 1682 olan numara tespit kararları, 1998 yılında 3262'ya çıkmıştır. Rota tespit kararları sayısı da 91'den 1558'e çıkarak müthiş bir artış göstermiştir.

Yıl	Numara Tespit	Uzatma	Rota Tespit	Uzatma
1987	1682	1217	91	6
1988	1978	1736	213	31
1989	2384	1999	308	105
1990	2353	2445	475	81
1991	2445	2425	577	138
1992	3145	2876	972	219
1993	3423	3299	2153	3777
1994	3696	3409	1311	1146
1995	3414	3200	1558	1419
1996	3262	2854	1317	1338
1997	4369	4266	1409	1390
1998	4886	4621	2437	2770

1.2.2.7.2.Numara ve Rota Tespiti Kapsamında Yargı ve Yasama Denetimi

Numara ve rota tespit cihazının kullanılması keyfiyeti, ABD Mahkemeleri İdari Ofisine (İdari Ofis) bildirilmelidir. Bu rapor dışında İdari Ofis'e sunulması gereken başka bir husus bulunmamaktadır[474].

[472] SCHWARTZ,The Pen Register Act, The Statistics.

[473] ELECTRONIC PRIVACY INFORMATION CENTER (EPIC), Approvals for Federal Pen Registers and Trap and Trace Devices 1987-1998, (Source: US Justice Department Annual Reports to Congress) http://www.epic.org/privacy/wiretap/stats/penreg.html (İET:10.11.2007).

[474] WONG, 3.5.10.

Öte yandan, Adalet Bakanı her yıl Kongreye Numara ve Rota Tespit Kanunu çerçevesinde yapılan tespitlere ilişkin rapor vermek durumundadır. Bu raporda aşağıdaki hususlar yer alacaktır[475]:

- Mahkeme tarafından verilen izin kapsamında yapılan tespitin süresi, varsa tespit kararının sayısı ve süresi[476],
- Başvuru ve mahkeme kararı konusu suç[477],
- İlgili soruşturma sayısı[478],
- Bu tespit kapsamına giren cihaz (facility) sayısı[479],
- Başvuruyu yapan kolluk görevlisinin ve onayı veren yetkilinin kimlik bilgileri ile başvuru konusu yer ismi[480].

1.2.3.Dış Güvenlik İstihbarat Kanununa Göre İletişimin Denetlenmesi (Foreign Intelligence Surveillence Act)(FISA)

1.2.3.1.FISA'yı Doğuran Tarihsel Süreç

İkinci dünya savaşından sonra başlatılan Shamrock (Yonca) operasyonu ile Amerikan Ordusu, RCA Global, ITT World Communications and Western Union International gibi şirketlere sensörler yerleştirmişti. İstihbarat akışını sağlamak amacıyla, Amerikan Savunma Bakanlığı (Department of Defense) şirketlerden iletişime müdahaleye devam edilmesini, şirketlerin bu eylemlerinin cezai sorumluluktan muaf olduğunu ifade etmiştir. Kamuoyundan saklanan bu uygulama Başkan Truman'ın bilgisi dahilinde devam etmiştir. 1949 ile 1975 yılları arasında ise, başkanlara bildirilmeden uygulama sürdürülmüştür. 1970'li yıllar itibariyle, tüm iletişimi kayda alan manyetik bantlar aracılığıyla aylık yaklaşık 150 000 mesaj (message) incelenmek üzere denetlenmiştir[481].

---

[475] WONG, 3.5.11; 18 U.S.C. § 3126.

[476] 18 U.S.C. § 3126(1).

[477] 18 U.S.C. § 3126(2).

[478] 18 U.S.C. § 3126(3).

[479] 18 U.S.C. § 3126(4).

[480] 18 U.S.C. § 3126(5)

[481] DONOHUE, s. 9-10.

Shamrock operasyonunun yanısıra Milli Güvenlik Ajansı (NSA-National Security Agency), sivil itaatsizlik hareketlerine, savaş karşıtı eylemlere vs. karışan kişileri takip altına almıştır. Minaret adı verilen çok gizli bir proje başlatılmış, bu tür hareketleri başlatan ya da teşvik eden NSA olmasına rağmen, bu ajansın isminin bu tür hareketlerle anılması bir şekilde engellenmiştir. NSA, ABD'den Küba'ya seyahat eden vatandaşlarını takip etmekle başlattığı faaliyetlerini, daha sonra Başkan'ı tehdit ettiğine inanılan kişileri listelemekle devam ettirdi. FBI ve Narkotik Bürosu (The Bureau of Narcotics and Dangerous Drugs) bu listeye, terör ve uyuşturucu suçlarına karıştığı iddia edilen kişileri de dahil etmeye başladı. Nihai olarak, 1971 yılında bu program tüm cezai aktivitelere ve yıkıcı aktiviteleri destekleyen tüm faaliyetlere teşmil edildi. Ekim 1973'de NSA bu uygulamayı sona erdirdi. Bununla birlikte, anayasal haklarını kullanan yüz binlerce insan takibe maruz kalmaktan kurtulamadı[482].

CIA de, Chaos adı verilen bir program çerçevesinde ülke içinde karşı casusluk projesi yürütmüştür. Başkan Lyndon Johnson (1963-1969) ve Richard Nixon (1969-1974)[483] dönemlerinde savaş karşıtı eylemlerle dış güçler arasında irtibat kurulması çabaları bu programın hayata geçirilmesine neden olmuştur. CIA tarafından 4'ü Başkan Johnson'a, biri de Başkan Nixon'a sunulan toplam 5 raporda, bu hareketlerin arkasında herhangi bir dış güç bağlantısı kurulamadığı ifade edilmiş, ancak bu arada, yaklaşık 300 000 ABD vatandaşı takip mağduru olmuştur[484]. 1945 ile 1975 yılları arasında milli güvenlik saikiyle yapılan teknik takipler, siyasi gücün bir enstrümanı haline gelmiş, her bir takip aslında dar bir çerçevede başlamış olmasına rağmen gittikçe daha fazla Amerikan vatandaşını kapsamına almıştır[485].

Milli güvenlik gerekçesiyle ve mahkeme kararı bulunmaksızın iletişimin denetlenmesi sorunu, ilk olarak United States-United States District Court davasında ele alınmıştır. Bu dava, bir grup Vietnam savaşı protestocusunun Michigan-Ann Arbor'daki askere

---

[482] DONOHUE, s. 9-10.

[483] http://www.whitehouse.gov/history/presidents/chronological.html .(İET:)

[484] Bu dönemde Amerikan ordusu, teknik takip yoluna başvurmuş, Conus adı verilen bir operasyon çerçevesinde yaklaşık 100 000 siyasi aktivistin iletişimine müdahale edilmiştir. Haklarında takibat yapılan kişiler arasında, Senatörler Adlai Stevenson(III), J. William Fulbright ve Eugene McCarthy, Parlamenter Abner Mikva, şarkıcı Joan Baez ve sivil haklar savunucusu Martin Luther King de vardır. Bunun yanısıra ACLU (American Civil Liberties Union-Amerika Sivil Özgürlükler Birliği), Americans for Democratic Action (Demokratik Hareket Taraftarı Amerikalılar), NAACP(National Association for the Advancement of Colored People-Renkli İnsanların Terakkisi Milli Birliği), the American Friends Service Committee(Amerikalı Dostlar Hizmet Komitesi) ve the Southern Christian Leadership Conference(Güney Hristiyan Liderlik Konferansı) gibi sivil hak savunucusu örgütler de vardır. DONOHUE, s. 12.

[485] DONOHUE, s. 9.

alma bürosunu ve birkaç hükümet binasını havaya uçurma denemesi ile ilgilidir. Mahkeme kararı olmaksızın milli güvenlik saikiyle elde edilen ve yargılamada kullanılan delillerin yasadışı olduğu iddiasıyla ilgili olarak Mahkeme, hükümetin milli güvenlikle ilgili suçlar hakkında yapılacak soruşturmada, önceden alınmış bir mahkeme kararının gerekli olduğuna hükmetmiştir. Bununla birlikte, Mahkeme, bu tür suçların farklı bir politikayı gerektirdiğini vurgulayarak, Kongrenin, bu tür suçlarla ilgili soruşturma tekniklerinin sıradan suçlarla aynı olup olmaması gerektiği hususunda bir araştırma yapmasını tavsiye etmiştir[486]. Gerçekten de, bu karar tarihi itibariyle, Teknik Dinleme Kanunu, Başkan'a milli güvenlikle ilgili konularda tedbir almasına izin vermesine rağmen[487], sadece adli nitelikli suçlarla ilgili delil toplama amacına matuf olması halinde iletişimin denetlenmesine imkan tanımaktaydı[488].

FISA, 1978'de kanunlaştırılmış[489] ve daha sonra 1986 tarihli ECPA ve Patriot Kanunu ile bazı hükümleri değişikliğe uğramıştır. Kanun, NSA[490]'nin adının karıştığı iç casusluk tartışmaları ile FBI, CIA ve NSA'ya isnat olunan casusluk skandallarının ortaya çıkması sonrasında yasalaştırılmıştır. Bu istihbarat skandallarının bir kısmı, Senatör Frank Church tarafından başkanlık edildiği için Church Committe[491] olarak adlandırılan bir komitenin yayınladığı raporlarla belgelenmiştir[492].

---

[486] BULZOMI,"Foreign Intelligence Surveillance Act".

[487] AN OVERVIEW OF ELECTRONIC SURVEILLANCE, History and Current Status, D.1.3.

[488] BULZOMI,"Foreign Intelligence Surveillance Act".

[489] (Public Law 95-511), http://www.cnss.org/PL%2095-511.pdf , (İET:25.9.2007).

[490] Milli Güvenlik Ajansı (NSA-National Security Agency), gizli bilgileri korumak için şifreleyen, şifreleri çözen ya da iletişim konularıyla ilgili diğer hususlarla ilgilenen hükümet ajansıdır. 1952 yılında kurulmuş olmasına rağmen, bu ajans, 1975 yılında bile pek çok ABD vatandaşının bilmediği bir örgüttü. Savunma Bakanlığının bir parçası olarak yapılandırılan bu örgütün yazılı bir programı(charter) bulunmamaktaydı. NSA'nın öncelikli misyonu elektronik istihbarat teminiydi. Bu misyon, 1970'li yıllarda binlerce kişinin NSA'da istihdam edilmesine neden olmuştur. Genellikle rejim muhalifi ABD vatandaşları hakkında çalışmalar yapan NSA, Minaret adı verilen bir projeyle, barış grupları, siyah hakları için kurulmuş örgütler, vs. hakkında takibat başlatmıştı. http://www.aarclibrary.org/publib/church/reports/vol5/contents.htm , (İET:25.9. 2007).

[491] Church Committee tarafından kaleme alınmış 14 raporda, ABD istihbarat ajanslarının kuruluş, çalışma tarzı ve suiistimalleri hakkında önemli bilgiler mevcuttu. 1975 ve 1976 yıllarında yayınlanmış olan bu raporlarda, ABD'nin, bazı ülkelerin liderlerine ilişkin suikast girişimlerine ilişkin birtakım iddia ve tespitler bulunmaktaydı. Bu bağlamda, Kongo lideri Patrice Lumumba, Küba lideri Fidel Castro, Dominik Cumhuriyeti lideri Rafael Trujillo, Vietnam'dan Diem kardeşler ve Şili'den General Rene Schneider hakkındaki suikast eylemleri hakkında ABD ile ilgili olarak ithamlar bulunmaktaydı. Bu 14 rapor, istihbarat faaliyetleri ile ilgili olarak, kamuoyunun bilgisine sunulmuş en geniş kapsamlı çalışma olarak görülmektedir. http://www.aarclibrary.org/publib/church/reports/contents.htm,(İET:30.10.2007); Church Committee hakkında bilgi için ayrıca Bk. DONOHUE, s.13.

[492] DONOHUE, s. 13; ADLER, Andrew: "The Notice Problem, Unlawful Electronic Surveillance, and Civil Liability Under the Foreign Intelligence Surveillance Act", 61 U. Miami L. Rev. 393, University of Miami Law Review, 2007, s.3; KHAN, s.68.

1.2.3.2.Kavram ve Kapsam

Bu şartlar çerçevesinde 1978 tarihinde kanunlaştırılan FISA[493], bir suçla ilgili delil elde etmeyi amaçlayan 1968 tarihli Teknik Dinleme Kanunundan farklı olarak, yabancı istihbarat bilgisine ulaşmayı hedefleyen ve önleme amaçlı iletişimin denetlenmesine imkan tanıyan bir kanundur[494]. İletişimin denetlenmesi ile ilgili birtakım özel usulleri kapsayan bu kanun, yüksek düzeyde gizlilik içeren bir tarzda çalışmaktadır[495].

Bir ABD vatandaşının FISA kapsamında iletişiminin denetlenebilmesi için, bu kişinin yabancı bir devletin ajanı olduğu gibi bilgi ve iddiaların nedenleriyle birlikte FISA mahkemesine ibraz edilmesi gerekmektedir. Bu tür faaliyetlere katılanlar ile yardım ve yataklık edenler de bu kapsamdadır[496]. FISA, yabancı istihbarat ve karşı istihbarat elde etmek amacına matuf olduğundan dolayı, 1968 tarihli Teknik Dinleme Kanunu'nda öngörülen birtakım emniyet subaplarından yoksun olarak ortaya çıkmıştır[497]. Casusluk ve karşı casusluk faaliyetlerinin yanı sıra ülke dışı bağlantılı suçlar da bu, kanunun kapsamına girmektedir[498]. Teknik Dinleme Kanunu gibi gerçek içeriğe ilişkin müdahaleyi düzenleyen FISA kapsamına, yabancı kaynaklı suçlar girmektedir. Ancak bu kapsama girmesi için suçlunun Amerikan vatandaşı olmaması ya da Amerikalı olmasına rağmen suçun ABD dışından bir bağlantısı olması gerekmektedir[499].

Kongre, milli güvenliğe ilişkin suçlarda iletişimin denetlenmesi imkanını kullanabilmek bakımından, gerekli olan yetki ve prosedürün belirlenmesi için, FISA'yı çıkarmıştır. FISA ile, milli güvenliğe ilişkin suçlarda arama ve iletişimin denetlenmesi yoluna başvurabilmek için önceden alınmış bir mahkeme kararının gerekli olduğuna hükmedilmiştir. Bu kanunla ayrıca, bir mahkeme kurulmasına karar verilmiştir. Mahkemenin amacı, milli güvenliğe ilişkin suçlarda arama ve iletişimin denetlenmesi

---

[493] Foreign Intelligence Surveillence Act (FISA), U.S.C. § 1801-1811 maddelerinde düzenlenmiştir. Bk. TITLE 50, CHAPTER 36, SUBCHAPTER I , http://www4.law.cornell.edu/ uscode/html/uscode50/ usc_ sup 01 50 10 36 20 I.html .

[494] ÖZDOĞAN, (2004), s. 22; DEMPSEY, "Communications Privacy In The Digital Age: Revitalizing The Federal Wiretap Laws To Enhance Privacy"; WONG, 2005: 3.2.4; MacARTHUR, s. 2.

[495] STEVENS/DOYLE, s. 46.

[496] AN OVERVIEW OF ELECTRONIC SURVEILLANCE: History and Current Status, D.1.3.

[497] DEMPSEY, "Communications Privacy In The Digital Age: Revitalizing The Federal Wiretap Laws To Enhance Privacy".

[498] ÖZDOĞAN, (2004), s. 22; DEMPSEY, "Communications Privacy In The Digital Age:Revitalizing The Federal Wiretap Laws To Enhance Privacy"; WONG, 3.2.4.

[499] ÖZDOĞAN, (2004), s. 22, WONG, 3.2.5; AN OVERVIEW OF ELECTRONIC SURVEILLANCE: History and Current Status, D.1.3.

tedbirlerinin kullanılmasına ilişkin hükümet yetkilerinin denetlenmesi ve bu yetkilere makul sınırlar getirilmesidir[500].

1.2.3.3.Başvuru Şartları

FBI ve CIA, FISA kapsamındaki suçlar hakkında yapılacak iletişimin denetlenmesini yürütmek hakkını haiz olan kurumlardır. Bu kurumlar tarafından yapılacak talep sonrasında, FISA mahkemesi iletişimin denetlenmesine ilişkin kararı verir[501]. Başvurular bu kurumlar adına Adalet Bakanlığı tarafından yapılır[502]. Dinleme işleminin sona ermesinden sonra, dinleme kayıtları mühürlenerek mahkemeye teslim edilir[503].

Teknik Dinleme Kanunu'nda yer alan hususlara benzer unsurların başvuru dilekçesinde yer alması gerekmektedir. Bunlar[504];

- Başvuruyu yapan Federal görevlinin ismi[505],
- ABD Başkanı tarafından Adalet Bakanı'na verilen yetki ve Bakan'ın bu başvuruyu yaptığını gösteren onay[506],
- Hakkında takip yapılacak kişinin kimliği ve biliniyorsa hedefin anlatımı[507],
- Hakkında iletişimin denetlenmesi tedbirine başvurulan hedefin, yabancı bir güç veya yabancı bir gücün ajanı olduğuna ilişkin açıklama[508]. Tedbirin yöneltildiği her tesis veya yerin, yabancı bir güç veya yabancı bir gücün ajanı tarafından kullanıldığını, kullanılmakta olduğunu[509] gösteren olayların anlatımı[510],
- En aza indirgeme ilkesinin uygulandığına ilişkin bir açıklama[511],

---

[500] 50 U.S.C. § 1803(b); BULZOMI,"Foreign Intelligence Surveillance Act"; DONOHUE, s. 15; KHAN, s. 69.

[501] ÖZDOĞAN, (2004), s. 22; WONG, 3.4.3.

[502] SCHWARTZ,The Statutes: FISA and National Security Letters.

[503] ÖZDOĞAN, (2004), s. 22.

[504] DONOHUE, s. 14-15; AN OVERVIEW OF ELECTRONIC SURVEILLANCE: History and Current Status, D.1.3; SCHWARTZ, The Statutes: FISA and National Security Letters.

[505] 50 U.S.C. § 1804(a)(1).

[506] 50 U.S.C. § 1804(a)(2).

[507] 50 U.S.C. § 1804(a)(3).

[508] 50 U.S.C. § 1804(a)(5).

[509] 50 U.S.C. § 1803(a)(4)(B).

[510] 50 U.S.C. § 1803(a)(4).

[511] 50 U.S.C. § 1803(a)(5).

- Elde edilmek istenen bilginin türü ve takip konusu edilecek iletişim ve faaliyetlerin çeşidi[512],

- Milli Güvenlik İşleri Kurumu Başkan Yardımcısı veya Başkan tarafından milli güvenlik veya savunma alanında uzmanlaşmış görevliler arasından aday gösterilen ve Başkan tarafından, Senato'nun onayıyla atanan görevliler tarafından verilen sertifika veya sertifikalar[513] (Bu sertifikalarla; elde edilmek istenen bilgilerin yabancı istihbarata dair olduğu[514], iletişimin denetlenmesinin esas amacının yabancı istihbarat bilgisi elde etmek olduğu[515], bu bilgilerin normal yollarla elde edilmesinin mümkün olmadığı[516], elde edilmek istenen bilginin 1801(e)'de sayılan kategorilere ilişkin olduğu[517] hususları açıklanır ve bu bilgiler bir olay anlatım belgesi[518] ile ibraz edilir.)

- İletişimin denetlenmesine hizmet edecek araçlara ve bu amacın gerçekleşmesi bakımından fiziksel girişin gerekip gerekmediğine ilişkin açıklamalar[519],

- Bu bölüm tahtında, herhangi bir hakime önceden yapılmış başvuruyu ve bu başvuruda adı geçen kişi, yer, tesis vs. hakkında yapılmış başvuruları gösteren bir açıklama[520],

- Tedbirin muhtemel süre hakkındaki kanaat[521].

Sayılan şekil şartlarının yanı sıra, normal soruşturma yöntemleriyle bu delillerin elde edilmesinin mümkün olmadığına ilişkin bir beyan da gereklidir[522].

Bu takibin amacı, yabancı istihbarat elde etmek amacıyla bir yabancı devlet ya da yabancı devlet ajanının takibe alınmasıdır. Yapılan işlemin asıl amacının, yabancı istihbarat elde edilmesi olduğu talepte vurgulanmalıdır. Bir kişinin yabancı ülke adına ajanlık yaptığının gösterilmesi için aşağıdaki hallerin ispatına yarayan deliller

---

[512] 50 U.S.C. § 1803(a)(6).

[513] 50 U.S.C. § 1803(a)(7).

[514] 50 U.S.C. § 1803(a)(7)(A).

[515] 50 U.S.C. § 1803(a)(7)(B).

[516] 50 U.S.C. § 1803(a)(7)(C).

[517] 50 U.S.C. § 1803(a)(7)(D).

[518] 50 U.S.C. § 1803(a)(7)(E).

[519] 50 U.S.C. § 1803(a)(8).

[520] 50 U.S.C. § 1803(a)(9).

[521] 50 U.S.C. § 1803(a)(10).

[522] AN OVERVIEW OF ELECTRONIC SURVEILLANCE: History and Current Status, D.1.3.

sunulmalıdır[523]. (Bununla birlikte, bu şartların varolduğu ilgili yetkili tarafından beyan edildikten sonra, mahkemenin bu beyan tutanağındaki bilgilerin olup olmadığını araştırma çabasına girmesine neden yoktur.)

- İlgili kişi yabancı bir gücün görevlisi veya o güç adına çalışandır,
- Yabancı bir ülke adına hareket etmektedir.
- ABD kanunlarının ihlali anlamına gelecek bir istihbarat toplama suçunu, bilerek işlemektedir.
- Bilerek sabotaj, uluslararası terörizm vs. suçları işlemekte veya bu suçların hazırlanmasına yabancı bir ülke adına katılmaktadır.

FISA kapsamında yapılan her başvuru, yemin tahtında imzalanmalı ve bu başvurunun bir yabancı güç veya bir yabancı gücün ajanı hakkında olduğu hususu, Savunma Bakanı veya Bakan Yardımcısı tarafından tasdik edilmiş olmalıdır. Bu başvuru Adalet Bakanlığı tarafından incelenir ve Adalet Bakanı tarafından tasdik edilir. Bu süreç sonrasında, FISA mahkemesi kararını verir[524].

1.2.3.4.FISA Kapsamında Önleme Amaçlı İletişimin Denetlenmesinin Şartları

FISA ile ilgili inceleme yapılırken, 1968 tarihli Teknik Dinleme Kanunu'nda belirlenen şartların karşılanıp karşılanmadığı da incelenmekle birlikte; bu süreç, casusluk ve karşı casusluk olayları için tasarlandığından, Teknik Dinleme Kanunu'ndaki korumaların hepsinin bu kanunda yer almadığı[525] anlaşılmaktadır. Bu kanunun doğasından kaynaklanan nedenlerden dolayı, bazı unsurların mahkeme kararı verilmesi için şart olarak belirlenmemiştir. Bunlardan ilki, makul sebep şartıdır. Makul sebep şartı, hakimin karar verirken varlığını arayacağı şartlar arasında değildir. İletişimin denetlenmesi başvurusu, bir federal görevli tarafından yapılmış ve Adalet Bakanı tarafından onaylanmış olduğu takdirde[526] yetkili hakimin makul bir sebep şartını aramasına gerek kalmamaktadır[527]. Görüldüğü üzere, burada çok önemli bir hususun irdelenmesi mahkemeye bırakılmamıştır. Mahkeme, makul sebebin (probable cause) var olup

---

[523] DECKER, s. 17; 50 U.S.C. § 1804.

[524] AN OVERVIEW OF ELECTRONIC SURVEILLANCE, History and Current Status, D.1.3.

[525] DEMPSEY, "Communications Privacy In The Digital Age: Revitalizing The Federal Wiretap Laws To Enhance Privacy".

[526] 50 U.S.C. § 1805 (a)(2).

[527] 50 U.S.C. § 1805 (a)(3); EFF ANALYSIS OF PATRIOT ACT.

olmadığı hususunda bir araştırma yapmakla yükümlü kılınmamış, bu sorumluluk ve yetki talepte bulunan hükümetin omuzlarına yüklenmiştir. Elde edilmek istenen bilginin milli güvenliğe ilişkin olduğu ve bilginin normal yollarla temin edilemeyeceği hususlarının, kanunda belirlenen görevliler tarafından teyit edilmesi, başvuru şartı olarak belirlenmiştir[528]. Makul sebep yerine, Patriot Kanunu[529] ile istihbarat toplayabilmek için 'Önemli hedef'(significant purpose)[530] kriteri getirilmiştir[531]. 'Önemli' (significant) kelimesinin tanımlanmamış olmasından kaynaklanan belirsizlik tutarsızlıklara ve yeknesak olmayan uygulamalara neden olabilmektedir. Yabancı istihbarat toplama gerekçesiyle, cezai soruşturmalarla iç içe geçmiş konularda FISA hükümleri uygulanmaktadır. Hak ve hürriyetlerin korunması hususunda Teknik Dinleme Kanunu'na göre çok daha gevşek hükümler içeren FISA uygulanarak, bir nevi hile yöntemiyle cezai soruşturmalarda delil elde edilmektedir[532].

Öte yandan, FISA'ya göre yapılan denetlemelerde son çare prensibinin uygulanması şartı da bulunmamaktadır[533]. Daha doğru bir ifadeyle, bu şartın varlığı mahkeme tarafından inceleme konusu yapılmamaktadır. İletişimin denetlenmesi için başvuruda bulunulduğunda, yetkili tarafından ibraz edilen sertifikada, bu tedbire son çare olarak başvurulduğu şeklindeki beyan yeterlidir[534]. Bu bağlamda denilebilir ki, bu kanun yabancı istihbarat ve karşı istihbarat elde etmek amacına matuf olduğundan dolayı 1968 tarihli Teknik Dinleme Kanununda öngörülen birtakım emniyet subaplarından yoksun olarak ortaya çıkmıştır[535].

Bununla birlikte, FISA çerçevesinde bir mahkeme kararı verilebilmesi için gerekli olan ve 'en aza indirgeme ilkesi' (minimization procedures)[536] olarak adlandırılan kurala

---

[528] DONOHUE, s.14-15; EFF ANALYSIS OF PATRIOT ACT; AN OVERVIEW OF ELECTRONIC SURVEILLANCE: History and Current Status, D.1.3.

[529] Patriot Kanunu, Madde 218.

[530] 50 U.S.C. § 1804(a)(7)(B) maddesinde yer alan ifade aşağıdaki gibidir: '… iletişimin tespitinin önemli hedefi yabancı istihbarat elde etmektir.'

[531] In Re Sealed Case 310 F.3d 717 Foreign Int. Surv. Ct. Rev. 2002, http://www.prosecutingterrorists.com/inresealedcase.pdf); KHAN, s.70.

[532] THE USA PATRIOT ACT, EPIC Report.

[533] ÖZDOĞAN(2004), s. 100; DEMPSEY, "Communications Privacy In The Digital Age: Revitalizing The Federal Wiretap Laws To Enhance Privacy".

[534] 50 U.S.C. § 1804 (a)(7)(C).

[535] DEMPSEY, "Communications Privacy In The Digital Age: Revitalizing The Federal Wiretap Laws To Enhance Privacy"; ÖZDOĞAN, (2004), s. 22.

[536] 50 U.S.C. § 1805 (a)(4).

riayet edilmesi gerekmektedir[537]. En aza indirgeme ilkesine uygunluk (Compliance with minimization procedures) başlıklı madde hükmü uyarınca, bir ABD vatandaşı hakkında iletişimin denetlenmesi suretiyle elde edilen bilgilerden, ilgili federal görevli tarafından sadece 'en aza indirgeme' ilkesine riayet edilmesi kaydıyla (in accordance with the minimization procedures) kullanılabileceği ve açıklanabileceği ifade edilmektedir. Bu şartın varlığını denetleme yetkisi hakime verilmiştir. Madde, bu bilgilerin kullanılması ve açıklanmasında ilgilinin, yani iletişimine müdahale edilen ABD vatandaşının rızasının aranmayacağı ifade edilmektedir. Bu bilgilerin ancak ve ancak yasal amaçlar için kullanılabileceği ifade edilmektedir[538]. En aza indirgeme kuralına, acil durumlarda çıkarılan iletişimin denetlenmesi tedbirinde de riayet edilmelidir[539].

1.2.3.5.Mahkeme Kararı

FISA Kanunu çerçevesinde verilecek kararı çıkaracak makam FISA Mahkemesi (FISC-Foreign Intelligence Surveillence Court) olarak adlandırılan özel görevli[540] ve gizli[541] bir mahkemedir. Mahkeme ABD Yüksek Mahkemesi Başkanı tarafından, 7 yargı bölgesinden atanmış olan 11 hakimden oluşur[542]. Yılda iki defa Washington D.C.'de gizli olarak toplanan[543] bu mahkeme, ülkenin herhangi bir eyaletindeki[544] önleme amaçlı iletişimin denetlenmesine[545] ilişkin başvurulara ilişkin kararı veren mahkemedir[546]. Hakim, FISA uyarınca yapılmış başvuruyu reddederse, red gerekçelerini izah eden bir rapor hazırlamak durumundadır. Bu rapor FISA İtiraz Mahkemesine[547] gönderilir. ABD Yüksek Mahkemesi Başkanı tarafından atanan 3 hakimden oluşan bu mahkeme başvuruların reddine ilişkin olarak verilen kararı incelemekle yükümlüdür. FISA İtiraz

---

[537] WONG, 3.4.8; DONOHUE, s. 14-15; STEVENS/DOYLE, s. 48-50.

[538] 50 U.S.C. § 1806(a).

[539] 50 U.S.C. § 1805 (f)(2); WONG, 3.4.8.

[540] Bu mahkemenin FISA sürecini kontrol etmek dışında herhangi bir fonksiyonu yoktur. STEVENS/DOYLE, s. 46.

[541] DONOHUE, s. 14; EFF ANALYSIS OF PATRIOT ACT.

[542] 50 U.S.C. § 1803 (a) hükmüne göre Yüksek Mahkeme Başkanının atayacağı 11 hakimden en az üçü District of Columbia (Washington şehri ile aynı alanı kaplayan ve ABD'nin başkenti olarak kabul edilen bölge) ve 20 millik bir alan içinde ikamet eden hakimler arasından seçilirler. Bu hakimler, başvuru dilekçelerini almak ve iletişimin denetlenmesine ilişkin başvuruları sonuçlandırmakla yükümlüdürler.

[543] AN OVERVIEW OF ELECTRONIC SURVEILLANCE: History and Current Status, D.1.3.

[544] Eyalet ile kastedilen, ABD'yi oluşturan eyaletlerdir. Bu eyaletlere, District of Columbia, Puerto Rico, Trust Territory of Pacific Islands ile ABD'nin egemenliği altındaki herhangi bir yer de dahildir. (50 U.S.C. § 1801, (o)).

[545] 50 U.S.C. § 1801, (f)'de FISA kapsamındaki elektronik iletişimin alanı belirtilmiştir.

[546] WONG,3.4.2; AN OVERVIEW OF ELECTRONIC SURVEILLANCE, History and Current Status, D.1.3.

[547] 50 U.S.C. § 1803(b).

Mahkemesinin verdiği gerekçeli karara karşı da, temyiz merci olan Yüksek Mahkemeye başvurulması mümkündür[548].

FISA Mahkemesi, 2003 yılına kadar yapılan başvuruların hiçbirisini reddetmemişken, 2003 tarihinde yapılan 4 başvuruyu reddetmiştir. Amerikan Hükümeti bu red kararlarına karşı itiraz yoluna başvurmamıştır[549]. Bu bölüm tahtında atanmış hakimler, en fazla yedi yıl görev yaparlar. Hakimlerin yeniden görevlendirilmeleri mümkün değildir[550].

Bu kapsamda yapılacak işlemler seri muhakeme usulune tabidir ve olabilecek en kısa süre içinde sonuçlandırılmalıdır. Tutulan kayıtlar, (yapılan başvurular, verilen mahkeme kararları vs.) Baş Hakim (Chief Justice) tarafından Adalet Bakanı ve Milli İstihbarat Direktörü (Director of National Intelligence) ile istişare halinde koruma altına alınır[551].

Hakimin FISA kapsamında iletişimin denetlenmesine ilişkin karar verirken, aşağıdaki şartlara riayet etmesi gerekmektedir[552]:

- Başkan, Adalet Bakanına FISA kapsamında bir başvuruya onay vermesi hususunda yetki vermiş olmalıdır[553].
- Başvuru, bir federal görevli tarafından yapılmış ve Bakan tarafından onaylanmış olmalıdır[554].
- Hakkında iletişimin denetlenmesi tedbiri uygulanacak olan hedef, ya yabancı bir güç ya da yabancı ülke ajanı olmalıdır[555].
- Hakkında takip izni verilecek olan yer ve cihazların her birinin, yabancı bir güç veya yabancı bir gücün ajanı tarafından bir suçun işlenmesinde kullanılıyor veya kullanılmak üzere olması gerekmektedir[556].

---

[548] 50 U.S.C. § 1803(b); BULZOMI,"Foreign Intelligence Surveillance Act", ; DONOHUE, s. 15; Ayrıca, Bk. DECKER, s.17; ADLER, s.3.

[549] WONG, 3.4.4; Bk. The Attorney General's 2003 report submitted to the Administrative Office of the US Courts pursuant to FISA, 30 April 2004.

[550] 50 U.S.C. 1803(d).

[551] 50 U.S.C. § 1803(c).

[552] WONG,3.4.8; DONOHUE, s. 14-15; STEVENS/DOYLE, s. 48-50.

[553] 50 U.S.C. § 1805 (a)(1).

[554] 50 U.S.C. § 1805 (a)(2).

[555] 50 U.S.C. § 1805 (a)(3)(A).

[556] 50 U.S.C. § 1805 (a)(3)(B).

- 1801. maddede tanımlanan en aza indirgeme (minimization procedures)[557] denilen kavrama riayet edilmiş olmalıdır.

Bu tedbire başvurulması için gerekli nedenlerin varolup olmadığı hususunu[558], başka bir ifadeyle makul sebebin (probable cause) olup olmadığını araştırmak mahkemeye bırakılmamıştır. Milli güvenlik ya da milli savunma yetkilisinin bu hususta mahkemeye vereceği teyit mahkeme açısında yeterlidir[559]. Görüldüğü üzere, burada, çok önemli bir hususun irdelenmesi mahkemenin yetkisi dahilinde değildir. Bu bağlamda, önceden belirlenmiş ve milli güvenlik ya da milli savunma yetkilisinin mahkemeye vereceği teyit mahkeme açısından yeterli görülmüştür[560].

FISA çerçevesinde bir iletişimin denetlenmesi tedbirinin birtakım şekil şartlarına bağlandığı görülmekle birlikte, FISA mahkemesinin sadece bir şekli tasdik makam olarak kullanıldığı da iddia edilmektedir. Gerçekten de, 1979 ile 2003 yılları arasında FISA mahkemesi 16450 başvurudan sadece 3 tanesini reddetmiştir[561]. Hükümet yetkilileri, bu sonucu kendi profesyonellikleri ile açıklamaktadırlar[562].

1978 ile 1995 yılları arasında yürütme her yıl ortalama 500 talepte bulunmuşken, bu rakam, 11 Eylül olayları sonrasında, 2002 yılında 1228'e ve 2003'te de 1727 çıkmıştır. Tarihinde ilk defa 2002 ve 2003 yıllarında, Adalet Bakanlığı'nca FISA kapsamında talep edilen iletişimin denetlenmesi talepleri, diğer talepleri geride bırakmıştır. 2006 yılı itibariyle mahkeme kararı sayısı 2181'e ulaşmıştır. Önleme amaçlı iletişimin denetlenmesi talepleri bakımından, 1997 ile 2006 yılları arasındaki dönemde, yüzde 342'lik bir artış görülmüştür[563]. FISA kapsamında karşılanması gerekli olan şartlar daha

---

[557] 50 U.S.C. § 1805 (a)(5).

[558] 50 U.S.C. § 1805 (a)(3); EFF ANALYSIS OF PATRIOT ACT.

[559] DONOHUE, s. 14-15; EFF ANALYSIS OF PATRIOT ACT; AN OVERVIEW OF ELECTRONIC SURVEILLANCE, History and Current Status, D.1.3.

[560] DONOHUE, s. 14-15; EFF ANALYSIS OF PATRIOT ACT.

[561] İstatistikler için Bk. "FOREIGN INTELLIGENCE SURVEILLANCE ACT", http://fas.org/irp/ agency/ doj/ fisa (İET: 20.11.2007).

[562] DONOHUE, s. 15; Kongre tarafından yapılan değişikliklerle, olgusal kanıt (factual proof) zorunluluğu ortadan kaldırılmıştır. Başvuran hükümet yetkilisi ya da ajansı, telefonu dinlenecek kişinin uluslararası terörizmde neden ve nasıl kullanılacağını izah etmek zorunda değildir. Bunun yerine, elde edilecek bilginin bir Amerikan vatandaşını doğrudan ilgilendirmediğini, bu bilginin uluslararası terörizme karşı koruma sağlanması amacıyla kullanılacağını göstermek yeterli olacaktır. Sivil hak taraftarlarınca hararetli bir şekilde eleştirilen bu husus, 31 Aralık 2005 tarihine kadar yürürlükte kalacak şekilde (sunset clause) belirlenmişken, Kongre bu hükmü sürekli hale getirmiştir. Bk. USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. 109-177, 102, 120 Stat. 192 (2006); AN OVERVIEW OF ELECTRONIC SURVEILLANCE: History and Current Status, D.1.3.

[563] SCHWARTZ, FISA, The Statistics.

düşük eşikte olduğundan, diğer bir ifadeyle, Teknik Dinleme Kanunu ve ABD Anayasası'nın 4. bölümünde belirlenen sıkı şartlar burada öngörülmediğinden, hükümet bu yolla daha fazla bilgi toplama şeklinde bir tercih yapmıştır. FISA'nın bu şekilde kullanılması ile McCarthy[564] dönemine geri dönüldüğü iddia edilmektedir[565].

1.2.3.6.İletişim Aracı Belirtilmeksizin Bir Kişi Adına Çıkarılan Mahkeme Kararı

Patriot Kanunu ile yapılan değişiklik sonrasında, hakkında takibat yapılan, ancak takipten kaçmak için değişik yöntemlere başvuran kişiler ile ilgili olarak, gerekli şartların varlığı halinde gezici takip (roving tap) denilen bir iletişimin denetlenmesi yöntemine başvurulmaktadır. FISA, gezici takip kurumunu Bölüm III'te sayılan şartların varlığı halinde hayata geçirebilmektedir[566].

Patriot Kanunu'nun 206. maddesi ile yapılan değişiklikle[567], hedef kişinin (intelligence target) kullandığı bir cihazın takibe alınması yerine, FISA Mahkemesinin vereceği bir karar marifetiyle kişinin kullanabileceği tüm cihazların denetlenmesine imkan tanınmaktadır. Teröristlerin, kullandıkları iletişim araçlarını çabucak ve ustalıkla değiştirebildikleri ve bu konuda eğitim aldıkları gerçeğinden hareket edilerek çıkarılan bu hüküm gelişmiş yöntemleri kullanan teröristlerin daha kolay takibini sağlaması bakımından hükümetin elini güçlendirmiştir. Teknik Dinleme Kanunu çerçevesinde uyuşturucu suçları gibi suçlar hakkında başlatılmış cezai soruşturmalar kapsamında uzun bir süreden beri başvurulagelen bu uygulama, FISA kapsamındaki suçlara da böylelikle uygulanmaya başlamıştır[568].

Bu genel uygulama ile masum kişilerin özel hayatlarının ihlal edileceği yönünde kamuoyunda ciddi endişeler ortaya çıkmıştır. Örneğin, hedef kişi tarafından kullanılacağı istihbar edilen ve bu bilgiyi müteakiben FBI tarafından takibe alınan bir

---

[564] Joseph Raymond McCarthy ,1908-1957 yıllara arasında yaşamış ve anti komünist düşünceleri ile tanınmış bir Amerikan Senatördür. 1950 yılından başlayarak aşırı anti komünist söylemlerin savunucusu olan ve soğuk savaş döneminde federal hükümet de dahil olmak üzere heryerde birçok Sovyet casusu ve komunist olduğunu iddia eden McCarthy hakkında, bu iddialarını ispatlayamaması nedeniyle Senato'da sansür kararı çıkarılmıştır. McCarthy, komünistlik suçlamasıyla yaygın bir baskı ve sindirme kampanyasının sürdürüldüğü dönemin simgesidir. McCarthyism ifadesi, McCarthy'nin anti komunist uygulamalarına verilen addır.Bugun bu tabir genellikle, demogoji içeren ve ispatlanamayan suçlamalar hakkında kullanılmaktadır.http://en.wikipedia.org/wiki/Joseph_McCarthy,(2.12.2007); http://www.apl.org/history/mccarthy/biography.html (İET: 2.12.2007).

[565] DONOHUE, s. 15.

[566] WONG, 3.4.6; EFF ANALYSIS OF PATRIOT ACT; THE USA PATRIOT ACT, EPIC Report.

[567] 206.madde ile 50 U.S.C. § 1823(C)(2)(B) değiştirilmiştir.

[568] PATRIOT ACT FACT SHEET, 30 Mart 2005 tarihi itibariyle bu madde 49 defa kullanılmış ve özellikle uluslararası terörizm suçları ve casusluk suçlarında etkin olarak istihdam edilmiştir.(PATRIOT ACT FACT SHEET).

İnternet kafeyi kullanan tüm kişilerin iletişimleri takibe maruz kalmış olacaktır. Takibe alınan yerin bir kütüphane olduğu varsayımı bu endişenin boyutlarını artırmaktadır. Kütüphane yetkililerinin böyle bir takibin yapıldığını kullanıcılara açıklamaktan men edildiği hallerde, durum kuşkusuz daha da ağırlaşmış olacaktır. Genel nitelikli bir gezici takip emrinin ciddi anayasa ihlalleri oluşturduğu ve Anayasa'nın 4. maddesinin ihlali anlamına geldiği, EPIC gibi bazı sivil toplum kuruluşları tarafından iddia edilmektedir. Nitekim, iletişimin denetlenmesine imkan tanıyan mahkeme emri takibe alınacak yeri kesin olarak belirtmemektedir. Kanunlara bağlı ABD vatandaşlarının da, bu tür takiplere konu olması ihtimali endişe ile karşılanmaktadır[569].

1.2.3.7.Mahkeme Kararı Olmaksızın İletişimin Denetlenmesi

FISA'ya göre, Adalet Bakanı, mahkeme kararı olmaksızın yabancı istihbarat elde edilmesi için bir yıllığına yetki çıkarabilir[570]. Bu yetkinin çıkarılabilmesi bakımından Adalet Bakanının aşağıdaki hususları garanti etmesi gereklidir[571];

- Elde edilmek istenen iletişim içeriği, yabancı güçler arasında geçen ifadelere ilişkindir[572],
- Elde edilmek istenen teknik istihbarat yabancı devletin açık ya da özel (exclusive) kontrolu altındaki yerlere ilişkindir[573].
- Takip bir ABD vatandaşının tarafı olduğu bir iletişime ilişkin değildir[574].
- İletişime müdahale eden yetkililer en aza indirgeme usullerine riayet edilecektir ve Adalet Bakanı bu usullere riayet edildiği hususunu, hem Meclis İstihbarat Komisyonuna hem de Senato İstihbarat Komisyonuna en az 30 gün önceden bildirecektir[575].

Bu yöntemin kullanılması için ayrıca, bu amaçla çıkarılacak bir mahkeme kararının gerektirdiği şartların da varolması gereklidir[576].

---

[569] THE USA PATRIOT ACT, EPIC Report.

[570] 50 U.S.C. § 1802(a)(1); KHAN, s.70.

[571] WONG, 3.4.8.

[572] 50 U.S.C. § 1802(a)(1)(A)(i).

[573] 50 U.S.C. § 1802(a)(1)(A)(ii).

[574] 50 U.S.C. § 1802(a)(1)(B).

[575] 50 U.S.C. § 1802(a)(1)(C).

[576] 50 U.S.C. § 1805 (f)(2).

Bu yöntemin hayata geçirilmesi için diğer bir şart da, bu konuda karar almaya yetkili hakime, Adalet Bakanı ya da onun tayin edeceği kişi tarafından, acil denetleme emrinin (emergency electronic surveillance) verildiği ve en kısa süre içinde ve nihayetinde 72 saat içinde bu konuda mahkemeye başvuruda bulunulacağı hususunda bilgi verilmesidir[577]. Bu bağlamda, mahkemeye 72 saat içerisinde müracaat yapılmalıdır[578].

Bu tedbir uygulanırken en aza indirgenme prensibine riayet edilmelidir[579]. Acil durum için öngörülen tedbir, aşağıdaki hallerden birinin varlığı durumunda sona erer:

1. Bu yöntemin başvurulmasına ilişkin Adalet Bakanlığı talimatından itibaren 72 saatlik sürenin geçmiş ve mahkeme kararının alınamamış olması,
2. İletişimin denetlenmesi ile amaçlanan bilginin elde edilmiş olması,
3. Yetkili mahkemenin kendisine iletilen başvuruyu reddetmesi.

Acil denetleme emrinin reddedilmesi ya da başka bir şekilde sona ermesi halinde, bu konuda çıkarılmış bir mahkeme kararı bulunmadıkça elde edilen bilgiler delil hüviyetini kazanamayacak ve bir mahkeme ya da başka bir organ[580] huzurunda kullanılamayacaktır. Verilen red kararına karşı 1803 nolu madde hükmü uyarınca FISA İtiraz Mahkemesine başvurulabilir. Bu şekilde alınan bilginin kullanılması, bir kimsenin hayatına ya da vücut bütünlüğüne yönelebilecek bir tehlikenin işaret edilmesi hali dışında yasaktır. Bu durumun varlığına Adalet Bakanı tarafından karar verilecektir[581].

Öte yandan FISA, savaş zamanlarına münhasır olmak üzere ayrı bir olağanüstü yetki vermektedir. 'Savaş zamanında yetkilendirme başlıklı' maddede, yetki Başkana verilmiş olmakla birlikte, bu yetkinin Adalet Bakanı tarafından kullanılabileceği belirtilmektedir. Madde metninde geçen 'may' yardımcı fiili bu yetkinin kullanılmasının bir zorunluluk olmadığını, Başkanın ihtiyarına bırakıldığını ifade etmesi anlamında önemlidir. Bu yetkiyle hükümet mahkeme kararı olmaksızın ve on beş gün süreyle yabancı istihbarat elde edilebilir[582].

---

[577] 50 U.S.C. § 1805 (f)(2); ADLER, s.5.

[578] KHAN, s.70.

[579] 50 U.S.C. § 1805 (f)(2).

[580] '…in any trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof…' 50 U.S.C. § 1805 (f)(2).

[581] 50 U.S.C. § 1805 (f)(2).

[582] 50 U.S.C. § 1811.

1.2.3.8.Süre

Mahkeme kararının teknik takibin amacına ulaşması gerekli olan bir süre (The period necessary to achieve its purpose) için geçerli olacağı hükmü FISA'da yer almaktadır. Bununla birlikte bu sürenin 90 günden fazla olamayacağı hükme bağlanmıştır[583]. Tedbirin yabancı güce karşı kullanılması halinde bu sürenin uzadığı görülmektedir. Bu takdirde süre, başvuru dilekçesinde belirlenen süre veya her halukarda en fazla bir yıl olabilir[584]. Teknik takibin yabancı bir ülke ajanı hakkında yapılıyor olması halinde ise, bu süre yabancı bir güce karşı yapılan takipte olduğu gibi dilekçede beyan edilen zaman dilimidir. Ancak bu süre 120 günü geçemez[585].

Uzatma kararları da dahil olmak üzere, tüm kararlar federal hakimce verilmektedir[586]. Mahkeme kararı süresinin uzatımı için gerekli olan şartlar ilk başvuru dilekçedeki şartlardır[587].

1.2.3.9.İlgiliye Bildirim ve Elde Edilen Bilgilerin Açıklanması

FISA hükümleri, Bölüm III'ten farklı olarak, iletişimi denetime tabi tutulan kişiye bildirim zorunluluğu getirmemektedir[588]. Bir ABD vatandaşı hakkında iletişime müdahale yoluyla elde edilen bilgi, ilgili kişinin rızası aranmaksızın kullanılabilir ve açıklanabilir. Ancak bu yetkinin kullanılabilmesi yasal amaçlarla sınırlıdır(lawful purposes)[589].

Elde edilen bilgiler Adalet Bakanının onayıyla mahkemede delil olarak kullanılabilir[590].

1.2.3.10.FISA Kapsamında Numara ve Rota Tespiti

FISA kapsamında numara ve rota tespiti de yapılabilmektedir[591]. Bu kanun kapsamında, kolluk güçlerinin uluslararası terör soruşturmalarında numara ve rota

---

[583] 50 U.S.C. § 1805 (e)(1);WONG, 3.4.7; EFF ANALYSIS OF PATRIOT ACT.

[584] 50 U.S.C. § 1805 (e)(1)(A).

[585] 50 U.S.C. § 1805 (e)(1)(B); WONG,3.4.7; AN OVERVIEW OF ELECTRONIC SURVEILLANCE, History and Current Status, D.1.3.; EPIC, FBI'ın Patriot Kanunuçıkmadan istediğinde uzatma kararı alabildiğini, bu nedenle böyle bir kanun değişikliğinin nedeninin anlaşılamadığını iddia etmektedir. Bk. EPIC REPORT, Patriot Sunset.

[586] PATRIOT ACT FACT SHEET; EPIC REPORT, Patriot Sunset.

[587] WONG, 3.4.7.

[588] AN OVERVIEW OF ELECTRONIC SURVEILLANCE, History and Current Status, D.1.3; DEMPSEY, "Communications Privacy In The Digital Age: Revitalizing The Federal Wiretap Laws To Enhance Privacy".

[589] WONG, 3.4.10.

[590] AN OVERVIEW OF ELECTRONIC SURVEILLANCE, History and Current Status, D.1.3 ; EFF ANALYSIS OF PATRIOT ACT.

tespit cihazlarını kullanmaları mümkün hale getirilmiştir[592]. Adalet Bakanı veya belirlenmiş olan bir yetkili, yemin tahtında yapacakları yazılı bir müracaatla başvuruda bulunabilirler. Bu müracaat, FISA mahkemesine ya da bir baş hakim tarafından tayin edilen yetkili bir hakime (United States Magistrate Judge specifically appointed by the Chief Justice) yapılabilir. Müracaatta, hakkında takip kararı çıkarılacak cihazın uluslararası bir terör suçunu işlemiş olan, işlemekte olan ya da işleyecek olan bir kişi tarafından kullanılmakta olduğu, kullanıldığı ya da kullanılacağı bilgisi bulunmalıdır. Bu kişinin yanı sıra, yabancı bir güç veya bu gücün bir ajanı da aynı hükme tabidir[593]. Uluslararası bir terör suçuna katıldığından şüphe edilen bir Amerikan vatandaşı bir numara ya da rota tespit cihazının hedefi olabilir. Bu tedbirin hedefi olan kişilere bir bildirimde bulunma zorunluluğu getirilmemiştir. Bu yetki en fazla 90 gün için verilebilir ve talep halinde yetki 90 gün süreyle uzatılabilir[594].

1.2.3.11.FISA Kapsamında Önleme Amaçlı İletişimin Denetlenmesinin Denetimi

Teknik Dinleme Kanunu ile kıyaslandığında, FISA kapsamında özel hayatın korunması için belirlenen önlemlerin daha hafif olduğu söylenebilir. Bu önlemler aşağıdaki gibidir:

1.2.3.11.1.Yargı Denetimi

Bölüm III'te olduğu gibi FISA'da da Adalet Bakanı'nın ABD Mahkemeleri İdari Ofisine (İdari Ofis) yıllık bir rapor sunması zorunluluğunu getirilmiştir[595]. Bununla birlikte, FISA kapsamında açıklanan bilgiler, Bölüm III'tekine kıyasla önemli bir ölçüde sınırlandırılmıştır. Adalet Bakanı iletişimin denetlenmesine yönelik olarak yapılan toplam başvuruları, mahkeme kararlarını ve uzatma kararlarını içeren bir envanteri[596] İdari Ofis'e sunar. Bu rapor; verilen, düzeltilen ve reddedilen kararları da içermektedir[597]. Bunun dışındaki bilgiler gizlilik kaydı (classified) taşıdığı için bu raporda yer almaz[598]. Bu bilgiler kamuya açıklanmaz[599].

---

[591] AN OVERVIEW OF ELECTRONIC SURVEILLANCE: History and Current Status, D.1.3.

[592] AN OVERVIEW OF ELECTRONIC SURVEILLANCE: History and Current Status, D.1.3.; MacARTHUR, s.3; 18 U.S.C. § 3121(a).

[593] KHAN, s.70.

[594] MacARTHUR, s.3; DONOHUE, s.15 .

[595] 50 U.S.C. § 1807.

[596] 50 U.S.C. § 1807(a).

[597] 50 U.S.C. § 1807(a).

[598] WONG, 3.4.12.

[599] EFF ANALYSIS OF PATRIOT ACT.

1.2.3.11.2.Yasama Denetimi

Adalet Bakanı'nın, FISA kapsamında elde edilen bilgilere (intelligence) ilişkin olarak senede iki defa, Kongre Daimi İstihbarat Komitesi[600] ile Senato İstihbarat Komitesi'ni[601] tatminkar (fully inform) bir düzeyde bilgilendirmesi gerekmektedir. Maddede, iletişimin denetlenmesi hususunu düzenleyen bu bölümdeki hiç bir hükmün, anılan komitelerin fonksiyonlarını eda etmesine sınırlama getiremeyeceği ifade olunmaktadır[602].

Adalet Bakanlığı tarafından verilecek raporda, raporte edilen dönemde, hakkında iletişimin denetlenmesi tedbirine başvurulan her münferit ceza davası hakkında bilginin yer alması gerekmektedir[603].

1.2.3.12.Milli Güvenlik Mektupları (National Security Letters) (NSL)

FISA'nın yanı sıra, FBI'ya , milli güvenlik konularında üçüncü kişilerden bilgi alma imkanı sunan ve gerek Teknik Dinleme Kanunu gerekse FISA'nın birtakım şekli ve maddi şartlarını by pass etmek için ihdas edildiği iddia edilen[604] National Security Letters (Milli Güvenlik Mektupları) denilen başka bir yol daha mevcuttur[605]. NSL[606], FBI tarafından kaleme alınan, milli güvenlikle ilgili konularda bilgi temin edilmesini amaçlayan yazılı bir talimattır. Bir yargı organının denetimini öngörmeyen[607] bu yöntem mali kayıtlar ve kredi raporlarının belli kısımları hakkında ve bunun yanı sıra 'telecommunication attributes' denilen iletişim bilgileri[608] hakkında veri toplanmasını sağlamak bakımından muhatabına iletilir. NSL hakkındaki kanun hükmüyle[609]

---

[600] House Permanent Select Committee on Intelligence , http://intelligence.house.gov/AboutTheCommittee.aspx?Section=1 (İET:25.10.2007).

[601] SENATE SELECT COMMITTE ON INTELLIGENCE, http://intelligence.senate.gov/ (İET:25.10.2007).

[602] 50 U.S.C. § 1808(a)(1).

[603] 50 U.S.C. § 1808(a)(2)(A).

[604] DONOHUE, s. 19.

[605] MacARTHUR, Andrew P., "The NSA Phone Call Database: The Problematic Acquisition And Mining Of Call Records In The United States, Canada, The United Kingdom, And Australia", 17 Duke J. Comp. & Int'l L. 441, 2007, Duke Journal of Comperative and International Law, s. 4.

[606] Adalet Bakanının(The Attorney General) her yıl Kongreye sunmak zorunda olduğu raporda, 2005 yılı itibariyle, 9254 Amerikan vatandaşı hakkında NSL çıkarıldığı ve 3501 kişinin bu mektuplar kapsamına girdiği ifade edilmektedir. Oysa ki, bu rakamların aslında gösterilenden çok daha fazla olduğu, gerçek rakamın 2005 yılı itibariyle 47221 olduğu iddia edilmektedir. SCHWARTZ, FISA(The Statistics); ROSS, Brian/ WALTER, Vic: "Exclusive: Report Says FBI Violated Patriot Act Guidelines", 8 March 2007, http://blogs.abcnews.com/theblotter/2007/03/exclusive_repor.html ,(İET: 19.11.2007).

[607] KHAN, s.70.

[608] 18 U.S.C C. § 2703(c)(2)(USA PATRIOT Act § 210).

[609] 18 U.S.C. § 2709(a); NSL ile alınabilecek bilgiler arasında belli bir numaradan alınan ve bu numaradan yapılan telefon görüşmelerinin kronolojik dökümü,(h]istorical information on telephone calls made and

"subscriber information and toll billing records information, or electronic communication transaction records." talep edilir. Hükümet NSL'i, iletişimin içeriğinin elde edilmesi amacıyla kullanamaz[610]. NSL muhatabı olan kimse bu talebin bertaraf edilmesi ya da değiştirilmesi için mahkemeye başvurabilir. NSL muhataplarının hukuki durumları bakımından çok önemli sonuç doğuran başka bir durum da, muhatap hakkında böyle bir mektup alındığı hususunun açıklanmasını yasaklayan[611] bir konuşma ve açıklama yasağı (gag order[612]) çıkarılmasıdır[613].

Patriot Kanunu ile NSL hakkında da birtakım değişikliklere gidilmiştir[614]. FBI'ın NSL vasıtasıyla bilgi alma yetkisi daha geniş bir alana yayılmıştır[615]. Yapılan değişikliklerden ilki, bir NSL gönderilmesi konusundaki eşiğin daha aşağı çekilerek, aranan bilginin yabancı bir güç (devlet) ya da yabancı bir gücün (devlet) ajanı olması şartının kaldırılmasıdır[616]. Uluslararası terörizm veya istihbarata karşı koruma sağlamayı amaçlayan bir soruşturma ile ilgili(relevancy) olmak şartı NSL çıkarılması için yeterli hale gelmiştir[617]. İkinci değişiklik daha da çarpıcı bir durumun ortaya çıkmasına neden olmuştur. Patriot Kanunu, Washington'daki FBI karargahındaki sınırlı sayıda yetkiliye ait olan NSL çıkarma yetkisini, FBI'ın 56 değişik yerde bulunan taşra bürolarına da teşmil etmiştir[618].

---

received from a specified number), yerel ve uzak mesafeli görüşmelere ilişkin fatura bilgileri (local and long distance billing records), elektronik iletişime ilişkin işlem kayıtları, e posta adresleri, fatura kayıtları, ödeme şekilleri vs. bulunmaktadır. (e]lectronic communication transaction records (e-mails), including e-mail addresses"; ,"billing records and method of payment.) LICHTBLAU, Eric/RISEN,James "Aftereffects: Intelligence Gathering; Broad Domestic Role Asked For C.I.A. and the Pentagon ,2.5.2003, (İET:26.11.2007).http://query.nytimes.com/gst/fullpage.html?res=9F01E6D8173CF931A35756C0A9659C8B63 .

[610] MacARTHUR, s. 4.

[611] Kendisine, çalışanları ile ilgili olarak bir NSL gönderilen bir kişinin Washington Post gazetesinde isimsiz olarak yayınlanan yazısında, bu yöntemin kendi hukuk alanında meydana getirdiği olumsuzluklar ifade edilmektedir. Açıklama yasağı getiren ve uzun bir süreden beri devam eden bu mahkeme kararı ve bu kişinin NSL hakkındaki yorumları için Bk. "My National Security Letter Gag Order " Washington Post, Friday, 23 March 2007; Page A17, http://www.washingtonpost.com/wp-dyn/content/article/ 2007/ 03/ 22/ AR2007032201882.html (İET: 18.11.2007).

[612] 'Gag order' hükümet ya da bir mahkeme tarafındanan, sair zamanlarda da özel bir işveren ya da başka bir kurum tarafından verilen ve bir bilginin kamuya açıklanmasını yasaklayan bir emir ya da karardır. Gag order, genelde bir davada taraflar hakkında verilir. Basının bir konuda açıklama yapmasının yasaklanması da, bu kapsamdadır. http://en.wikipedia.org/wiki/Gag_order (İET: 18.11.2007).

[613] Bk. SCHWARTZ ,The Statutes: FISA and National Security Letters, DONOHUE, s. 19-22.

[614] SCHWARTZ,The Statutes: FISA and National Security Letters.

[615] USA PATRIOT Act, Sec. 105, 115 Stat. 365(yeniden kontrol et).

[616] 18 U.S.C. § 2709.

[617] 18 U.S.C. § 2709(b)(1); DONOHUE, s. 19-22.

[618] 18 U.S.C. § 2709(b).

Görüldüğü gibi, ABD mevzuatında iletişim bilgilerinin denetlenmesine imkan tanıyan birçok kanun hükmü bulunmakla birlikte, bu yasalara gerektiğinde by-pass eden bazı alternatif delil elde yöntemleri bulunmaktadır. Bu yöntemlerden biri olan NSL kamuoyunda çokça eleştiri almaktadır[619]. Herhangi bir yargı denetimi olmaksızın çıkarılan bu yetki ile, kişilerin en mahrem bilgi, belge ve kayıtları ele geçirilmekte, üstelik, tedbire muhatap olan kişinin, durumu herhangi bir kişi, yer ve tabii ki basına vermesi yasaklanmaktadır.

Bu uygulamanın iptal edilmesini sağlamak bakımından, hakkında terörle ilgili dava açılmış birkaç kişinin yanı sıra, American Civil Liberties Union, The Center for Constitutional Rights, National Association of Criminal Defense Lawyers gibi organizasyonlar tarafından dava açılmıştır[620].

1.2.4.Uygulamada Meydana Gelen Problemlerin Amerikan Mevzuatında Oluşturduğu Erozyon

Başta Teknik Dinleme Kanunu olmak üzere tüm yasal hükümler, mahremiyetin ihlalini olabildiğince azaltmaya çalışan bir zihniyet üzerine kurulmuş olmasına rağmen, zaman içinde belli bazı hükümler ve kurumlar yıpranmaya başlamıştır.

Bu problemlerin ilki, hakkında iletişimin denetlenmesi tedbiri uygulanacak suç sayısının artmasıdır. Aslında, Teknik Dinleme Kanunu'nun ilk olarak kanunlaştırıldığı tarihte, kanun koyucu, bu tedbire konu olabilecek suç sayısını oldukça dar tutmaya çalışmıştır. Bu suçlar, çoğunlukla organize suçlarla sınırlandırılmış ve sayıları 26 olarak belirlenmiştir. Ancak zaman içinde, birçok diğer suçun teknik dinleme kapsamına alınması ile, bu yöntem, hemen hemen tüm suçların soruşturulmasında kullanılan bir usul haline gelmiştir. Mevcut durum itibariyle, 1 yıldan fazla hapsi gerektiren suçların soruşturulmasında iletişimin denetlenmesine izin veren hükümler, mahremiyet hakkının ihlali riskini arttırmaktadır[621]. Öte yandan, Patriot Kanunu ileiletişimin denetlenmesi tedbirinin daha yaygınlaştığı, mahkemelerin kontrol yetkisinin azaltıldığı, İnternetin daha rahat takibe alındığı, İnternet servis sağlayıcısının içerik dışı abone bilgilerini mahkeme kararı olmaksızın kolluk güçlerine verdiği, yapılan yeni terörizm tanımıyla daha çok kişinin iletişiminin denetlendiği ve ABD'nin yabancı istihbarat servislerinin

---

[619] Başkan, halkta oluşan endişeleri gidermek amacıyla, bu tedbirin 45 günlük aralıklarla denetlendiğini açıklamıştır.(KHAN, s.71).

[620] KHAN, s.71.

[621] ÖZDOĞAN, (2004), s.100.

artık daha fazla ABD vatandaşını takibe aldığı iddia edilmektedir[622]. NSL denilen Milli Güvenlik Mektupları vasıtasıyla, milli güvenlikle ilgili konularda bir yargı organının denetimi olmaksızın[623] bilgi edinilebilmektedir. Bu yöntemle, mali kayıtlar ve kredi raporlarının belli kısımları hakkında, bunun yanı sıra iletişim detayları (telekomünikasyon attributes)[624] hakkında veri toplanması sağlanmaktadır. NSL muhataplarının hukuki durumları bakımından çok önemli sonuç doğuran başka bir durum da, muhatap hakkında böyle bir mektup alındığı hususunun açıklanmasını yasaklayan bir konuşma ve açıklama yasağı (gag order) çıkarılmasıdır[625]. ABD mevzuatında iletişim bilgilerinin denetlenmesine imkan tanıyan birçok kanun hükmü bulunmakla birlikte, NSL[626] gibi yargı denetimini saf dışı bırakan uygulamalar Amerikan toplumunda ciddi tepki çekmektedir.

Son çare prensibinin uygulamada olması gerektiği kadar işletilmemesi de, ABD hukukunda karşılaşılan problemlerden biridir[627]. İletişimin denetlenmesi için mahkeme kararı çıkarılması hususunda yapılan bir başvuru esnasında, kolluk görevlisinin, teknik takip dışındaki diğer yöntemlerin kullanılmasının zor olduğu şeklindeki beyanı bile, mahkemece, son çare prensibinin şartlarının karşılandığı şeklinde değerlendirilmektedir. Kolluk kuvvetleri, iletişimin denetlenmesine gelinceye kadar tüm diğer çareleri denememiş olsalar bile, iletişimin denetlenmesine ilişkin karar alabilmektedirler. Örneğin, ABD-Garcia kararında mahkeme, iletişimin denetlenmesi için diğer tüm normal yolların tüketilmiş olmasının gerekli olmadığını, bu yolların tüketilmiş olması prensibinin aslında mahkeme hakimine diğer geleneksel yollarda karşılaşılan güçlüklerin bildirilmesi anlamına geldiğini ifade etmektedir[628].

Son çare ilkesinin uygulamadaki yansıması ile ilgili problemler, aslında iletişimin denetlenmesi kararı verilebilmesi için gerekli olan bazı diğer şartlar bakımından da geçerlidir. Bu şartların belki de en önemlisi olan mahkeme kararının alınması, uygulamada arzu edilen filtreleme fonksiyonunu eda edememektedir. 1989 ile 1995

---

[622] EFF ANALYSIS OF PATRIOT ACT.

[623] KHAN, s.70.

[624] 18 U.S.C § 2703(c)(2)(USA PATRIOT Act § 210).

[625] DONOHUE, s. 20.; Bk. SCHWARTZ ,The Statutes: FISA and National Security Letters.

[626] Başkan, halkta oluşan endişeleri gidermek amacıyla, bu tedbirin 45 günlük aralıklarla denetlendiğini açıklamıştır.(KHAN, s.71).

[627] ÖZDOĞAN, (2004), s.100.

[628] DEMPSEY, "Communications Privacy In The Digital Age: Revitalizing The Federal Wiretap Laws To Enhance Privacy".

yıları arasında gerek eyalet gerekse federal düzeyde yapılan iletişimin denetlenmesi başvurularının hemen hepsi olumlu yanıt bulmuştur. Benzer şekilde, FISA mahkemesine 1979 ile 2003 yılları arasında yapılan 16450 başvurudan sadece 3 tanesi reddedilmiştir[629]. Kontrol yetkisini kaybeden[630] mahkemeler, ne gelirse onaylayan makamlar gibi algılanmaktadırlar[631]. Hükümet yetkilileri mevcut durumu kendi profesyonellikleri ile açıklasalar da, bu husus tartışmalı bir durum olarak durmaya devam etmektedir[632].

ABD'de yıllık olarak hazırlanan ve halkın bilgisine sunulan raporlardaki rakamlar da, akıllarda soru işaretleri bırakmaktadır. Örneğin, 1997 yıllık raporunda, Los Angeles kentinde bir yıl boyunca yapılan iletişimin denetlenmesine ilişkin sayının 24, verilen uzatma kararı sayısının da 13 olduğu belirtilmiştir. Bu raporda ayrıca, toplam denetleme süresinin ve uzatma süresinin ortalamasının 30'ar gün olduğu belirtilmiştir. Bununla birlikte, FBI tarafından Federal Register isimli bir resmi bültende yayınlanan 'Son Kapasite Duyurusu' adlı belgede, sadece Los Angeles kentinde, kentte hizmet veren her bir telefon servis sağlayıcıdan, aynı anda 46100 adet telefonu dinleyebilecek bir kapasitenin güvenlik güçlerine tahsisi talep edilmektedir. Bu talep rakamları ile yıllık denetim raporundaki rakamlar arasındaki büyük fark, denetim raporu mekanizmasının iyi çalışmadığı şeklinde düşüncelere neden olmaktadır[633].

Usulüne uygun bir şekilde elde edilmeyen delilin kullanılmasına örtülü olarak izin verilmesi de uygulamadaki problemlerdendir. Mahkeme kararı olmaksızın numara tespit cihazı kullanımı ile ilgili olarak verilen Smith-Maryland (1979) kararı, mahkeme kararı olmaksızın elektronik sinyal verici kullanımı ile ilgili olarak verilen ABD-Knotts (1983) kararı, mahkeme kararında ismi geçmeyen şahsın haberleşmesinin yine bu mahkeme kararına istinaden dinlenilmesi ile ilgili ABD-Donovan, (1977) kararı gibi kararlarla delil yasağı delinmiştir. Bu olaylar, Amerikan adalet mekanizmasının, şüphelinin itham edilmesi ile ilgili olarak elde edilen bilgileri her ne şekilde elde edilirse edilsin kullanmak istediğini göstermektedir[634].

---

[629] İstatistikler için Bk. "FOREIGN INTELLIGENCE SURVEILLANCE ACT", http://fas.org/irp/agency/doj/fisa (İET: 20.11.2007).

[630] EFF ANALYSIS OF PATRIOT ACT.

[631] ÖZDOĞAN (2004), s. 100-102; KHAN, s.80.

[632] DONOHUE, s.15.

[633] ÖZDOĞAN, (2004), s. 100-102.

[634] ÖZDOĞAN, (2004), s. 19-22.

ABD'de her geçen gün biraz daha artan bir düzeyde, mahkeme dışı (extrajudicial) inisiyatiflere girişilmektedir. Patriot Kanunu'nun 128 ve 206. maddeleriyle, terörizmle ilgili soruşturmaya muhatap kişiler hakkında susma kararı (gag order) çıkarılması yasallaştırılmış, anılan kanunun 204. maddesi de, Gizli Bilgiler Usulu Kanunu (Classified Information Procedures Act) kapsamındaki yargılamalar hakkında, yargılamayı yapan mahkemelere hükümet yetkililerinin sunum yapması hakkını vermiştir[635]. Patriot Kanunu'nun çıkarılması bile başlı başına bir eleştiri konusu olmuştur. Yürütme gücü ile sivil haklar arasındaki dengeyi yürütmenin lehine bozduğu iddia edilen[636] bu kanuna ilişkin hazırlık çalışmaları, 11 Eylül 2001 saldırısının vukubulmasından birkaç gün sonra başlamış ve kanun, Başkan Bush tarafından 26 Ekim 2001 tarihinde imzalanmıştır. 15'ten fazla önemli kanunda ciddi değişiklik yapan 322 sayfalık[637] bu kanun, acele olarak hazırlanmış, Kongre ve Senato'da yeterli bir düzeyde tartışılmamış hatta birçok milletvekili tarafından okunmamış[638] bir metin olarak görülmektedir[639]. Bu kanunla, birçok önemli alanda değişiklik yapılmış, iletişimin denetlenmesi hususunda hala tartışılan birçok adımlar atılmıştır.

ABD'de Patriot Kanunu ve akabindeki benzer nitelikli birkaç kanun ile yapılan değişiklikler kolluk güçlerini tatmin etmemiştir. Zaten geniş olan yetkilerinin[640] genişletilmesini talep eden kolluk görevlileri, mahkeme kararı olmaksızın iletişimin denetlemesine imkan tanıyan yetkilerin peşine düşmüşlerdir. Bu bağlamda kamuoyunda en çok ses getiren tartışma, Başkanın, başkanlık makamının doğasından kaynaklanan yetkilerle donatılması ve mahkeme kararı olmaksızın iletişime müdahale yetkisinin kendisine verilmesi istemine ilişkindir. Bu talebin sahibi olan ABD hükümeti, Başkan'ın FISA hükümlerini by pass edebileceğini iddia etmiştir. Bu çerçevede, Milli Güvenlik Ajansı (National Security Agency-NSA) tarafından oluturulacak bir veritabanında görüşmelerin kaydedilmesi yetkisinin başkana ait doğal bir yetki olduğu

---

635 COLE,David: "What Patriot II Proposes To Do", Georgetown University Law Center, February 10, 2003, http://www.cdt.org/security/usaPatriot/030210cole.pdf (İET:9.1.2008)

636 THE USA PATRIOT ACT, EPIC Report.

637 EFF Analysis Of The Provisions Of The USA PATRIOT Act, That Relate To Online Activities(October 31, 2001) Last updated October 27, 2003, http://w2.eff.org/ Privacy/ Surveillance/ Terrorism/ 20011031 eff usa patriot analysis.php (EFF ANALYSIS OF PATRIOT ACT)(İET: 17.9.2007).

638 DONOHUE, s., 19.

639 Amerikan Sivil Haklar Birliği (ACLU), birçok milletvekilinin metnini okumadan lehte oy kullandığını, terörle mücadele sloganı ile, bu kanunun büyük bir acelecilikle ve gizlice çıkarıldığını iddia etmektedir. Bk. AMERICAN CIVIL LIBERTIES UNION, "The Usa Patriot Act And Government Actions That Threaten Civil Our Liberties", http://www.aclu.org/FilesPDFs/patriot%20act%20flyer.pdf , (İET:24.11.2007).

640 KHAN, s.70; 50 U.S.C. &1811. FISA ile Başkan'a mahkeme kararı almaksızın iletişime müdahale edilmesi yetkisi verilmiştir. Bu yetki, Kongre'nin savaş ilanını müteakip 15 gün içerisinde kullanılmalıdır

savunulmaktadır. FISA'nın 1809(a)(1) no'lu maddesindeki hüküm bu iddiaya gerekçe gösterilmekte, bu maddenin FISA hükümlerine üstünlük kazandığı iddia edilmektedir. Başkanın, 'Silahlı Kuvvetleri Kullanma Yetkisi[641] çerçevesinde, ABD'ye yönlendirilmiş terörist faaliyeti engellemek amacıyla, gerekli olan her türlü gücü kullanabileceğini iddia eden bu kesim, Başkana, gerektiğinde bu konudaki mevzuatı bertaraf ederek olağanüstü yetkiler kullanma imkanının verildiğini[642] savunmaktadırlar.

Bu görüşe karşı çıkanlar da, FISA'nın metninin böyle bir yetkiye izin vermediğini, genel bir hüküm olarak kabul edilen Başkanın 'Silahlı Kuvvetleri Kullanma Yetkisi'nin, daha özel bir hüküm olan FISA'ya göre öncelik elde edemeyeceğini vurgulamaktadırlar. İkinci görüş sahipleri, Hamdan-Rumsfeld davasına atıf yapmakta ve Başkana savaş zamanlarında bile boş bir çek verilmediğinin[643], Mahkemenin bu hususu vurguladığını ifade etmektedirler[644]. 'Silahlı Kuvvetleri Kullanma Yetkisi'nden kaynaklanan bu yetkinin kullanılamayacağını iddia edenlerin bir diğer dayanağı da, bu yetkinin kişilerin tutuklanmaları amacıyla verildiği, bu nedenle sözkonusu yetkinin iletişimin denetlenmesine teşmil edilemeyeceğidir[645]. Bu tartışmanın devam ettiği günümüzde hükümetin bu yetkiyi kullandığı, buna gerekçe olarak da yukarıda belirtilen 'Silahlı Kuvvetleri Kullanma Yetkisi'ni gösterdiği bilinmektedir. Bütün bu olaylar, ABD'deki mevzuatın, sadece gerektiğinde başvurulan bir metin olduğu şüphesini akla getirmektedir.

Gerçeken de, iletişimin denetlenmesi tedbiri daha yasal bir zemine oturtulmadan önce başlayan bu hukukdışı müdahale, bu gün farklı bir formatta devam etmektedir. Mevcut mevzuattaki bazı yetkilerin çok geniş alanlara sirayet ettiği iddiasının kamuoyunda ciddi destek bulduğu günümüzde, bu yetkilerin de aşımı suretiyle hukuk süzgecinden geçmeyen yetkilerin talep edilmesi ve bu yetkilerin fiilen uygulanması endişe vericidir. Nitekim, hükümet, gerek Milli Güvenlik Ajansı(NSA) bünyesinde bir alternatif dinleme veritabanı oluşturarak, gerek Milli Güvenlik Mektuplar(NSL) vasıtasıyla mahkeme kararı

---

[641] ABD ve dünya kamoyunda çok ses getiren 'Silahlı Kuvvetleri Kullanma Yetkisi' (The Authorization for the Use of Military Force) ile, Taliban ve El Kaide'ye karşı Afganistan'da savaş yetkisi verilmiştir. (DECKER, s.10).

[642] DECKER, Brian R.; "The Future Of Unenumerated Rights: Part Two Of Three: Comment: "The War Of Information: The Foreign Intelligence Surveillance Act, Hamdan v. Rumsfeld, And The President's Warrantless-Wiretapping Program", Trustees of the University of Pennsylvania, University of Pennsylvania Journal of Constitutional Law, Lexis-Nexis online, (İET:1.11.2007), s.9-10.

[643] 'A state of war is not a blank check for the President'(MacARTHUR, s.7).

[644] MacARTHUR, s.7.

[645] DECKER, s. 10; MacARTHUR, s.12.

olmaksızın bazı iletişim bilgilerini temin ederek, gerekse Echelon[646] denilen dev kulaklar vasıtasıyla tüm dünyayı saran bir dinleme mekanizmasını kontrol ederek bu endişeleri haklı çıkarmaktadır.

[646] Amacı tüm internet, faks, telefon ve bilgi alışverişini takip etmek, denetlemek ve arşivlemek olan Echelon, kablosuz iletişimi takip için dev radar kulakları, yer iletişimini takip etmek için de yine antenler ve kablolara yerleştirilmiş dinleme üniteleri olan bir oluşumdur. Bu oluşumun, uluslararası ihalelerde Avrupalı şirketlerin tekliflerini dinleyerek, ABD'li şirketlere sızdırılması gibi olaylara karıştığı iddia edilmektedir. Bu sistemin varlığı, kurucusu ülkeler de dahil olmak üzere hiç kimse tarafından inkar edilmiyor. Echelon, http://www.fas.org/irp/ program/ process/ echelon.htm,(4.12.2007) KUZULOĞLU, M. Serdar, "Dikkat, e-kulaklar işbaşında!", Radikal, 06/07/2002, (İET,4.10.2007)Dikkat, e-kulaklar işbaşında!, Echelon sistemini diğer sistemlerden farklı kılan birkaç özellik bulunmaktadır. Bunlardan ilki, bu sistemin hemen hemen tüm iletişim türlerini kapsamasıdır. Bu bağlamda, telefon, faks, Internet, e-mail mesajları ve bütün bunların içerikleri müdahale kapsamındadır. İkinci özellik, bu sistemin ABD, Birleşik Krallık, Kanada, Avustralya ve Yeni Zelanda arasındaki anlaşmalar çerçevesinde yürütülmesidir. Bu ülkeler iletişime müdahale konusunda kendi ülkelerindeki imkanları diğerlerinin hizmetine açmakta, masrafları paylaşmakta ve ortaya çıkan bilgiyi ortak kullanmaktadırlar. Hukuk denetiminden uzak (legislation free area) olan bu sistemin hedefindeki kişiler, genellikle bu sistemi uygulayan ülkelerin vatandaşları değildir. Bu bağlamda, başka bir ülke vatandaşının Echelon tarafından yapılacak müdahalenin hukuka uygunluğunu kontrol edecek iç hukuk mekanizması bulunmamaktadır. Nitekim, bu kişi bahse konu ülkelerden birinde ikamet etmemektedir. Amerikan Kongresinde sadece Amerikan vatandaşlarının bu sistemden olumsuz olarak etkilenip etkilenmediği konusu gündeme gelmekte, böyle bir sistemin varlığının getirdiği problemlere değinilmemektedir. Report of the European Parliament On The Existence Of A Global System For The Interception Of Private And Commercial Communications (Echelon Interception System) (2001/2098(INI)) 11 July 2001, http://www.fas.org/ irp/program/ process/ rapport echelon en.pdf (İET:4.12.2007); MCCARTHY, Kieren: "What Are Those Words That Trigger Echelon?", http://www.theregister.co .uk/ 2001/ 05/31/what_are_those_words/ , İET: (4.10.2007).

BÖLÜM 2. AVRUPA İNSAN HAKLARI SÖZLEŞMESİ VE AVRUPA İNSAN HAKLARI MAHKEMESİ İÇTİHATLARINA GÖRE İLETİŞİMİN DENETLENMESİ

2.1.Avrupa İnsan Hakları Sözleşmesi'ne (AİHS) Göre Haberleşme Özgürlüğü ve Sınırlandırılması

2.1.1. AİHS'ye Göre Haberleşme Özgürlüğü

AİHS'nin özel hayat hakkını düzenleyen 8. maddesinde, herkesin, haberleşmesine saygı gösterilmesini isteme hakkına sahip olduğu ifade edilmiştir[647]. Hangi araç ve yolla olursa olsun başkalarıyla yapılan özel nitelikli haberleşmelerinin, kişilerin veya devlet organlarının müdahalelerinden bağımsız olarak yapılması hakkı olarak tanımlanan[648] haberleşme hakkı, iletişim aracının devlet ya da özel sektör tarafından işletildiğine bakılmaksızın her türlü iletişimi bu maddenin koruması kapsamına almıştır. Bu bağlamda, telefon görüşmeleri de dahil olmak üzere yazılı ve sözlü her türlü gönderi[649] özel hayat hakkının içinde kabul edilmektedir ve herkes özel hayatına, aile hayatına, konutuna ve haberleşmesine saygı gösterilmesi hakkına sahiptir[650].

2.1.2. AİHS'ye Göre Haberleşme Özgürlüğünün Sınırlandırılması

Haberleşme özgürlüğü, meşru ve yasal temellere dayandırılmak ve bireylere gerekli güvenceler sunulmak kaydıyla devletin müdahalesine konu olabilir[651]. Demokratik toplumun gerekleri, bu tür meşru müdahalelerin ölçüsü ve sınırı olarak belirlenmiştir[652]. Sınırlandırmanın yapılabileceği haller, AİHS'nin 8. maddesinin ikinci paragrafında sayılmıştır. Bu bağlamda, haberleşme hakkına bir kamu otoritesinin müdahalesi, ancak ulusal güvenlik, kamu emniyeti, ülkenin ekonomik refahı, dirlik ve düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve

---

[647] ŞEN, Ersan: İletişimin Dinlenmesi Tedbiri, Ceza Hukuk Dergisi, Seçkin Yayınları, S. 4, (İletişimin Dinlenmesi Tedbiri), s. 97.

[648] ANAYURT, Ömer ; Avrupa İnsan Hakları Hukukunda Kişisel Başvuru Yolu, Seçkin Yayınları, 2004, s. 116.

[649] ŞEN, (İletişimin Dinlenmesi Tedbiri), s.98.

[650] TEZCAN/ERDEM/SANCAKDAR, s. 237.

[651] ANAYURT, Avrupa İnsan Hakları Hukukunda Kişisel Başvuru Yolu, s. 117.

[652] ÜNAL, Şeref: Avrupa İnsan Hakları Sözleşmesi, İnsan Haklarının Uluslararası İlkeleri, TBMM Kültür, Sanat ve Yayın Kurulu Yayınları, 2001, s.220 .

hürriyetlerinin korunması için, demokratik bir toplumda zorunlu olan ölçüde ve yasayla öngörülmüş olmak şartıyla söz konusu olabilir.

2. maddede belirtilen sınırlandırmaların uygulanabilmesi, belli şartların mevcudiyetine bağlıdır ve bu sınırlandırmalar iki temel ilkeden hareketle uygulanabilmektedir. AİHS'de açıkça zikredilmemiş ilk prensibe göre, sözleşme tarafından açıkça teyit edilmeyen sınırlandırmalar kabul edilemez. Başka bir ifadeyle, bir müdahalenin sınırlama sınırları kapsamında kabul edilebilmesi için bu sınırlamaya sözleşmenin açıkça (expressly) izin vermesi gerekmektedir. Bu ilke sözleşmenin herhangi bir yerinde ifade edilmemiş olmakla birlikte sözleşmenin bütününün değerlendirilmesi ile ve çıkarsama yöntemi ile ortaya çıkmaktadır. Sınırlandırmalarla ilgili ikinci prensip, ilkinin aksine sözleşmenin ruhuyla değil lafzıyla teyit edilmiştir. Suiistimallerin önlenmesi bakımından önemli olan bu ilkelerin ikincisi, AİHS'nin, 'Hakların Kısıtlanmasının Sınırları' başlıklı 18. maddesinde, 'bu Sözleşmenin hükümleri gereğince, sözü edilen hak ve hürriyetlere getirilen sınırlamalar ancak öngörülen amaçlar için uygulanabilir' şeklinde ifade edilmiştir[653].

2.2. Avrupa İnsan Hakları Mahkemesi (AİHM) İçtihatlarına Göre Haberleşme Özgürlüğü ve Sınırlandırılması

2.2.1. AİHM İçtihatlarında Yer Alan Kavramlar

2.2.1.1.Özel Hayat Kavramı

Devlet de dahil olmak üzere başkalarının giremeyeceği bir alan oluşturmak, bu alanda yalnız bırakılmak[654] arzusu gitgide genişleyen bir kavram halini aldığından[655], öte yandan, kamu alanı ile özel hayat arasındaki sınır her olayın özelliklerine göre değiştiğinden, özel hayat kavramının tanımlanması her geçen gün biraz daha güçleşmektedir. Bu hususu kabul eden AİHM, özel hayat kavramının tam anlamıyla tanımlanmasının mümkün olmadığı gibi, gerekli de olmadığını ifade etmektedir.[656]

---

[653] OVEY/WHITE, s. 199. Owey ve White, bu ilkeyi 'restrictions expressly authorized by the Convention are allowed' şeklinde ifade etmektedirler.

[654] WARREN/ BRANDEIS, "The Right to Privacy".

[655] FOSTER, s. 359.

[656] NIEMETZ-ALMANYA, Pr. 33-34; ALCARAZ, Hubert: "Sonorisation et Ecoutes Téléphonique: La France Se Fait 'Tirer L'Oreille' A Propos Des Arrets Vetter et Mahteron De La Cour Europeenne Des Droits De L'Homme", Revue Trimestrielle Des Droits De L'Homme,Bruylant, dr.h.(66/2005),s.221; Kişiye istediği gibi yaşama garantisi veren özel hayat hakkı, başkalarıyla duygusal, mesleki, vb. alanlarda ilişki geliştirme imkanı sunar. Özel hayat kavramı, nisbilik de arzedebilen bir kavramdır. Gerçekten de, bir hakimin özel

Bununla birlikte, AİHK ve AİHM, bu kavrama ilişkin tanım ve yorum yapmaktan geri durmamışlardır. AİHK, özel hayatın, bedeni ve manevi bütünlük içinde ve 'yabancı gözlerden uzak' bir şekilde hayat sürmekten daha geniş bir alana taalluk ettiğini, kişinin kendi kişiliğini geliştirmek amacıyla başkalarıyla irtibata geçmesinin ve bu irtibatı devam ettirmesinin bu tanımın kapsamına girdiğini ifade etmiş[657], AİHM de, bu kavramı benimsemiştir. Bazı kişilere hakarette bulunduğu iddia edilen bir kişinin kimliğinin tespit edilmesini sağlamak amacıyla bir hukuk bürosunun aranması sorununu Strasbourg'a taşıyan Niemietz-Almanya davasında[658] AİHM, bu kavramın, bireyin kendi hayatını istediği gibi yaşayabileceği bir iç alan olarak sınırlanmasının ve bu alandan, söz konusu alanın içine girmeyen dış dünyanın olduğu gibi hariç tutulmasının aşırı kısıtlayıcı olacağı tespitini yapmıştır. Özel hayatın net bir tanımını yapmamak ve sessiz duruşuyla, bu alanı olabildiğince geniş yorumlamak gibi bir tercih yapan[659] Mahkemeye göre, bilim ve teknolojinin gelişmesiyle her geçen gün daha da önem kazanan bu hak[660], belirli bir düzeye kadar diğer insanlarla ilişki kurmayı ve bu ilişkileri devam ettirmeyi de içine almalıdır[661]. Bu bağlamda; özel hayat, 'efradını cami, ağyarını mani' bir tanımı yapılamayacak kadar geniş bir kavramdır. Cinsiyet belirleme, isim verme, cinsel tercih gibi şahsi hayata taalluk eden durumlar 8. maddenin korumasına giren konulardır. Bu madde; ayrıca, kimlik ve kişisel gelişim hakkını, başka insanlarla ve dış dünyayla ilişkiler kurma ve bu ilişkileri geliştirme hakkını da kapsamaktadır. Bu bağlamda, meslek veya işle ilgili faaliyetlerin de özel hayat kapsamına girdiğini ifade eden Mahkemeye göre, bir bireyin başkalarıyla kurduğu ilişkilerin bir kısmı, kamusal bağlamda yapılsa bile, özel hayat kapsamına girebilir[662].

Mahkemeye göre kamuya açık bilgiler, yetkililer tarafından düzenli ve sistematik olarak toplanıp muhafaza altına alındığı takdirde de, özel hayat kapsamında değerlendirilecektir. İlgilinin geçmişine ait bilgilerin toplanması halinde de, bu durum geçerli olacaktır. Rotaru davasında Mahkeme, 50 yıldan daha da önce toplanmış olan

---

hayat anlayışı ve sınırlama algılayışı ile başka bir insanın bu kavramı tanımlaması farklılık gösterebilecektir. (ERGEÇ, s. 241).

[657] ANAYURT, Avrupa İnsan Hakları Hukukunda Kişisel Başvuru Yolu, s. 115.

[658] DUTERTRE, , Gilles: Key case-law extracts : European Court of Human Rights, Council of Europe Publications, Strasbourg, 2003, s. 243.

[659] ALCARAZ, s. 223.

[660] ERGEÇ, s. 240.

[661] NIEMETZ-ALMANYA, Pr. 33-34.; ANAYURT, Avrupa İnsan Hakları Hukukunda Kişisel Başvuru Yolu, s. 115.

[662] P.G. ve J.H.- Birleşik krallık (Pr.56-60)(künye); ANAYURT, Avrupa İnsan Hakları Hukukunda Kişisel Başvuru Yolu, s. 115.

ve başvurucunun hayatıyla, özellikle de eğitimi, siyasi faaliyetleri ve adli sicili ile ilgili bilgilerin devlet yetkilileri tarafından saklanması işleminin 8/1. madde bağlamında özel hayat kapsamına girdiği kanaatindedir[663]. Benzer bir yaklaşımın sergilendiği P.G. ve J.H.-Birleşik Krallık kararında, kamusal alandaki davranışların kayıt cihazları ile kaydedilmesi ve dosyalanması halinde, bu işlemin, gizli veya müdahaleci bir yöntemle yapılmamış olsa bile, 8. madde'nin ihlali anlamına geldiği vurgulanmıştır[664]. Yine, Amman–İsviçre kararında, yetkililer tarafından kullanılmaksızın dosyalanan, hassas nitelikte olmayan bilgilerin özel hayatın gizliliğini ihlal edeceği ifade edilmiştir[665].

AİHM, özel hayatla ilgili bazı başvurularda[666], 1 Ekim 1985 tarihinde yürürlüğe girmiş olan ve kişilerin haklarına ve temel hürriyetlerine, özellikle de bireye ait şahsi verilerin otomatik olarak işlenmesi konusunda mahremiyetine saygı gösterilmesini sağlamayı amaçlayan 'Şahsi Verilerin Otomatik Olarak İşlenmesi Konusunda Bireylerin Korunması'[667] isimli Avrupa Konseyi Sözleşmesi ile getirilen hükümlere atıf yapmaktadır. Mahkeme, kişilerin haklarına ve temel hürriyetlerine ilişkin bilgilerin, özellikle de bireye ait şahsi verilerin[668] otomatik işlenmesi hususunda, özel hayata saygı gösterilmesini sağlamayı hedefleyen bahse konu sözleşmenin yorumuyla kendi yorumu arasında bir uygunluk (correspondance) bulunduğunu ifade etmektedir[669].

Görüldüğü gibi, dinamik bir yapıda olan özel hayatın korunması kavramı, günün koşulları ve toplumsal gelişmelerle yüklenen anlamlar çerçevesinde yorumlanmaya muhtaçtır. Bu nedenle, bu kavram, sadece hakkın belirtilmesi suretiyle ortaya konulmuş, hakkın kapsamı ile ilgili açık ve ayrıntılı tanım verilmesi cihetine gidilmemiş, sürekli genişleyen kapsamın belirlenmesi Mahkeme içtihatlarına bırakılmıştır[670].

---

[663] ROTARU-ROMANYA, Pr. 42-44.

[664] P.G. ve J.H.-BİRLEŞİK KRALLIK, Pr. 56-60.

[665] DUTERTRE, s. 245-246; Benzer bir olayda, bireyin özel hayatıyla ilgili belgelerin polisin gizli kayıtlarında saklanması, Sözleşmenin ihlali olarak değerlendirilmiştir.(LEANDER-İSVEÇ, Pr.48).

[666] Bk. ROTARU-ROMANYA kararı, Pr. 42-44.

[667] Council Of Europe Convention For The Protection Of Individuals With Regard To Automatic Processing Of Personal Data, 28.I.1981, İET:13.12.2007, http://conventions.coe.int/Treaty/en/Treaties/Word/108.doc .

[668] Kişisel veriler, anılan Sözleşmenin 2. maddesinde teşhis edilmiş(identified) ya da teşhis edilebilir (identifiable) kişilere ilişkin bilgiler olarak tanımlanmıştır. Council Of Europe Convention For The Protection Of Individuals With Regard To Automatic Processing Of Personal Data, 28.I.1981, İET:13.12.2007, http://conventions.coe.int/Treaty/en/Treaties/Word/108.doc.

[669] ROTARU-ROMANYA, Pr. 43.

[670] KAYA, Abdülkadir: Adalete Erişim İçin Sürekli Mesleki Gelişim: İnsan Hakları, Boğaziçi Üniversitesi Avrupa Çalışmaları Merkezi Proje Yayını, İstanbul, 2006, s. 88.; NIEMETZ-ALMANYA, Pr. 33-34.

2.2.1.2.Haberleşme Kavramı

AİHM, haberleşme kavramının kapsamını belirlerken geniş bir bakış açısı tercih etmiştir. Mahkeme, haberleşme kavramını, teknolojik gelişmelere ayak uyduracak ve elektronik posta gibi diğer yöntemleri de içerecek şekilde geniş tutma eğilimindedir[671]. Bu bağlamda; Mahkeme, posta yoluyla gönderilen malzemelerin yanı sıra, telefonla iletişim ve teleksin de, 8. maddenin 1. paragrafında ifadesini bulan 'özel hayat' ve 'iletişim' kapsamına girdiğine karar vermiştir[672].

Soyut bir formatta bulunan bu hakların somut kapsamını ortaya koymak amacıyla hareket eden AİHM'ye göre, özel haberleşmeye müdahale amacıyla ve gizli olarak, birtakım teknolojik aletlerin kullanılması, geniş anlamda özel hayat ve spesifik anlamda da haberleşme hürriyetinin ihlaline neden olur[673]. Nitekim, haberleşmeye saygı gösterilmesi hakkı, kesinti ya da sansüre maruz kalmadan başkalarıyla iletişim kurma hakkını kapsar[674]. AİHS'nin 8. maddesiyle korunan mahremiyet hakkı, hem yazılı iletişim hem de telefon yoluyla yapılan iletişimi kapsamına aldığından dolayı[675] bu koruma, içeriğine bakılmaksızın her iletişime sağlanmıştır. A-Fransa başvurusunda verilen karara göre, bir cinayet planlamasıyla ilgili görüşmelerin kaydedilmesi, kamu çıkarını ilgilendirmesine rağmen, görüşmenin özel olma niteliğini kaybetmesine neden olmayacaktır. Benzer bir genel bakış, Halford - Birleşik Krallık davasında da korunmuş, işe ya da özel hayata taalluk ettiğine bakılmaksızın bütün telefon görüşmeleri, 8. madde kapsamında kabul edilmiştir[676].

AİHM, haberleşme hakkını, özel hayattan bağımsız olarak algılamanın[677] yanı sıra, zaman içinde, özel hayat kavramını daha da geniş yorumlayan kararlar da verilmiştir. Bu cümleden olarak, AİHM, evden ve işyerinden yapılan iletişimin de özel hayat

---

[671] KILKELLY Ursula, Özel Hayata ve Aile Hayatına Saygı Gösterilmesi Hakkı, İnsan Hakları El Kitabı, No 1, Strasbourg, 2001, s. 20.

[672] KLASS-ALMANYA. Pr.41.; Doktrinde bu tanım daha da genişletilerek; elektrik, radyoelektrik, pnömatik (pneumatique), enformatik vb. kavramlar da bu kapsama alınmaktadır. Bk. ERGEÇ, s. 256.

[673] ÇOKSEZEN, Atakan: "5271 Sayılı Ceza Muhakemesi Kanunu Ve Avrupa İnsan Hakları Sözleşmesi Çerçevesinde Ceza Muhakemesi Tedbiri Olarak İletişimin Dinlenmesi", İstanbul, 2006, s. 4.

[674] UZGÖREN, Orhan:"Özel Hayat, Aile Hayatı, Konut, Haberleşme" Türkiye Barolar Birliği İnsan Hakları Avrupa Sözleşmesi ve Adli Yargı Sempozyumu, Ankara 2004, s. 477; KILKELLY, s. 19.

[675] YILDIRIM, Gülşen: "Özel Hayat, Aile Hayatı, Haberleşme ve Mesken, İnsan Hakları Avrupa Mahkemesinin 8. Maddenin Genişletilmiş Yorumu İle Sağlanan Koruma", Türkiye Barolar Birliği İnsan Hakları Avrupa Sözleşmesi ve Adli Yargı Sempozyumu, Ankara 2004, s. 408.

[676] KILKELLY, s. 11; ÇOKSEZEN, s. 4.

[677] YILDIRIM, s. 408.

kapsamında olduğuna karar vermiştir[678]. Görüldüğü gibi telekomünikasyon yoluyla yapılan haberleşmelerin tümü Sözleşmenin koruması altındadır.

2.2.1.3.AİHM'ye Göre Haberleşmeye Müdahale Kavramı

2.2.1.3.1.Genel Olarak

Son zamanlarda artan terör suçları ve bazı diğer ağır suçlarla mücadelenin haklılığı AİHM tarafından kabul edilmekte ve önemsenmektedir. Mahkeme, Birleşik Krallık Hükümetinin, Malone davasındaki savunmasında yer bazı argümanlara bu anlamda hak vermektedir. Hükümetin konuyla ilgili raporunda (white paper) yer alan ve suçların, özellikle de organize suçların artışı ve suçluların daha da gelişmiş yöntemler kullanması hususlarını not eden Mahkeme, telefon dinlenmesinin ağır suçların önlenmesi ve araştırılması hususunda mutlak olarak kullanılması gerekli olan bir yöntem olduğunu kabul etmektedir. Bununla birlikte, bu tür tedbirlerin doğasında var olan gizlilik nedeniyle suiistimal tehlikesine dikkat çekmektedir[679].

Taraf ülkelerin bu suçlarla mücadele konusunda gerekli önleyici tedbirleri almak hakkına sahip oldukları belirtilmekle birlikte, AİHS ile tanınan hakların yok edilmesinin de önlenmesi gerektiği vurgulanmaktadır. Başka bir ifadeyle, devletler tarafından alınan tedbirler, AİHS'nin lafzına ve özüne uygun olmak kaydıyla hayata geçirilebilir[680]. Bu anlayışı ifade eden Hakim Pettiti, Malone kararında yazdığı çoğunluk görüşünde, AİHS'nin, insan toplumunu koruyan bir metin olduğunu vurgulamaktadır. Pettiti'ye göre Sözleşme, bireyin kendi kimliğini korumasını amaçlar ve toplumun topyekün

---

[678] SCHMID, Gerhard : "Rapport, Sur le Projet de Résolution du Conseil Relative à L'interception Légale Des Télécommunications Compte Tenu Des Nouvelles Technologies, Commission Des Libertés Publiques et Des Affaires Intérieures", 23 Avril 1999, s. 6 (İET :19.09.2007) (http://www.europarl. europa. eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A4-1999-0243+0+DOC+XML+V0//FR).; HALFORD-BIRLEŞIK KRALLIK, 25.7.1997, 20605/92, Pr.44 '… telephone calls made from business premises as well as from the home may be covered by the notions of "private life" and "correspondence" within the meaning of Article 8 Pr. 1' .

[679] MALONE-BİRLEŞİK KRALLIK, 24.8.1984, 8691/79, Pr. 81.

[680] Mahkeme bu bağlamda; Klass Almanya kararında, istihbarî amaçla yapılan dinlemenin ihlal oluşturmadığına karar vermiş, HUVIG ve Kruslin Fransa davalarında ise, Fransız mevzuatında iletişimin denetlenmesi hususunda keyfiliği önleyici mekanizmalar olmadığı gerekçesiyle ihlal kararı vermiştir. Malone-Birleşik Krallık davasında ise, davaya konu olayın gerçekleştiği tarihte İngiltere kanunlarında iletişimin dinlenmesi düzenlenmediğinden dolayı Birleşik Krallığı mahkum etmiştir. (TEZCAN-ERDEM-SANCAKTAR, s.237). Ülkemizin mahkum edildiği Ağaoğlu kararında ise, 1412 sayılı CMUK'nun 91 ve 92. maddelerine dayanılarak gerçekleştirilen iletişimin denetlenmesi tedbirinin AİHS'ye aykırılığına hükmedilmiştir. Mahkemeye göre, anılan madde hükümlerinden iletişimin denetlenmesi yetkisinin çıkarılması mümkün değildir. Çünkü, devlete bu yetkiyi veren hükümler açık olmalıdır. DİNÇ, Güney: "Sorularla Avrupa İnsan Hakları Sözleşmesi", Türkiye Barolar Birliği, Mayıs, 2006, s. 430.

şeffaflığa doğru kaymasına karşı çıkar. Bu tavır, bireyin mahremiyetinin korunması bakımından gereklidir[681].

2.2.1.3.2. AİHM'ye Göre Müdahalenin Kapsamı ve Tespiti

AİHM, önüne getirilmiş bir başvuruda; AİHS'ye aykırılık iddiası ile ilgili inceleme yaparken, müdahalenin var olup olmadığı, müdahale konusu olayın Sözleşmeyle korunan bir hakka ilişkin olup olmadığı, müdahalenin yasal bir düzenlemeye dayanıp dayanmadığı, müdahalenin meşru bir amacının olup olmadığı ve müdahalenin demokratik bir toplumda gerekli olup olmadığı hususlarına ilişkin bir araştırma yapmaktadır[682]. Bilindiği gibi haberleşme özgürlüğü AİHS'nin 8. maddesi ile koruma altına alınmış bir haktır. 'Herkes özel ve aile hayatına, konutuna ve haberleşmesine saygı gösterilmesi hakkına sahiptir.' şeklinde düzenlenen maddede 'haberleşme' ifadesine özellikle yer verilmiş olması, başka bir ifadeyle, sözleşmenin lafzıyla bu hakkın garanti altına alınmış olması önemlidir.

Bir eylemin AİHS bağlamında müdahale sayılabilmesi için, devlet organları ya da resmi sıfatla hareket eden görevliler tarafından gerçekleştirilmesi ve devlete isnat edilebilir nitelikte olması gerekir[683]. Müdahalenin varlığının kabul edilebilmesi için, bu eylemin bir kimseyi etkileyecek, onu mağdur statüsüne koyacak bireysel bir kararın varlığı gerekmektedir. Böyle bir bireysel karar bulunmamakla birlikte, salt kanun metninin varlığı bazı hallerde müdahaleye neden olabilir. Bir formalite, şart, sınırlama veya yaptırım şeklinde gerçekleşebilen müdahale, bastırıcı ya da önleyici rejim altında alınmış önlemler formatında ortaya çıkabilir[684]. Bu çerçevede, iletişime yapılacak her türlü engelleme ve kaydetme, Sözleşme'nin 8. maddesinin birinci fıkrasında korunan hakka bir müdahale oluşturmaktadır[685].

---

[681] Hakim PETTITI'nin çoğunluk görüşü, MALONE, BİRLEŞİK KRALLIK.

[682] KILKELLY, s. 7.

[683] Hollanda'ya karşı yapılan bir başvuruda, Mahkeme; eşinin avukatı tarafından taciz edilen bir bayanın şikayeti üzerine, polis tarafından ilgilinin kullandığı ev telefonuna dinleme ve kayıt cihazı yerleştirmesini haberleşme özgürlüğüne müdahale olarak kabul etmiş ve müdahale koşullarının denetlenmesi gerektiğine karar vermiştir. Şikayeti yapan bayanın kendisinin de, bu aleti kullanarak telefon konuşmalarını kaydedebileceği ve polisin yaptığının teknik destek vermekten öte bir anlam ifade etmediği iddiası da mahkeme tarafından kabul görmemiş, uygulamanın müdahale olduğu belirtilmiştir. (DİNÇ, s. 427).

[684] YILDIRIM, s. 387.

[685] ALCARAZ, s. 223; KÜNHE, Hans-Heiner: "Avukat Telefonlarının Dinlenmesi", Karşılaştırmalı Güncel Ceza Hukuku Serisi 3", Çev. Hakan Hakeri, Ankara 2004., s. 99; KILKELLY, s. 47; YILDIRIM, s. 409: ARSLAN, Gülay: "Avrupa İnsan Hakları Mahkemesinin Özel Yaşam Hakkına Müdahaleyle Elde Edilmiş Deliller Hakkındaki Güncel Kararlarının İlgili Paragrafları", Özel Yaşam Medya ve Ceza Hukuku, Ankara 2007, s. 465.

AİHM'ye göre, sadece kanun hükmünün varlığı, kanun kapsamında kalan herkesin hakkına müdahale edildiği anlamına gelmez, bireyin özel hayatına yapılmış bir müdahale olması gerekir. Bununla birlikte, bir kanun, özel bir uygulama olmamasına rağmen, bireyi doğrudan etkiliyorsa, kanunun varlığı, bizatihi bireyin haklarını ihlal edebilir[686]. Klass-Almanya davasında AİHM, salt gizli önlemler veya gizli önlemlere izin veren kanunların varlığını, hak ihlali iddiası için yeterli bulmuştur[687].

Bireyin özel hayatına, rızası hilafına ve hukuka uygunluk nedeni olmaksızın girmek, Sözleşme tarafından korunmayan bir müdahaledir. Kişinin, başkası tarafından girilmeye müsait hale getirdiği bir ortak paylaşım alanı oluşturması halinde ise, bu alan Sözleşme ile korunma hüviyetini kaybedecektir. Bu bağlamda, sivil havacılıkta kullanılan bir radyo kanalı aracılığıyla yapılan bir haberleşme, başka kullanıcıların da erişebileceği bir dalga boyunda yapıldığı için AİHM tarafından özel haberleşme olarak nitelendirilmemiş ve bu eylem özel hayata müdahale sayılmamıştır[688].

Müdahalenin tespiti ve ispatı sorunu, Mahkeme tarafından müddeiye, yani başvurana yüklenmiştir[689]. Bununla birlikte, iletişimin denetlenmesi, mahiyeti itibariyle gizli bir tedbir olduğu için iletişimin denetlenmesi tedbirine tabi olanların bir çoğu, söz konusu müdahalenin farkında olamazlar. Bazen de, hakkında bu tedbire başvurulan kişi, böyle bir uygulamaya maruz kaldığı konusunda şüphelenmesine rağmen yeterli kanıt bulamadığı için bu iddiasını ispatlayamaz[690]. Bu gibi hallerde, yani müdahalenin varlığını ispatlamanın mümkün olmadığı durumlarda, müdahalenin gerçekleşmiş olma ihtimalini ispatlamak da yeterli olacaktır[691].

Müdahalenin ispatı sorunu devletin pozitif sorumluluğu bakımından da önem taşımaktadır. Özel hayata müdahalenin, devletin aktif ya da pasif bir tutumundan kaynaklandığı gerçeğinden hareketle, AİHM, devletin müdahalesinin yanı sıra

---

[686] DOĞRU, Osman: İnsan Hakları Avrupa Mahkemesi İçtihatları, Cilt 1, İstanbul, 2002., s. 245-253; Klass Almanya Kararı, Pr.41 '…Furthermore, in the mere existence of the legislation itself there is involved, for all those to whom the legisation could be applied, a menance of surveillance; this menace necessarily strikes at freedom of communication between users of the postal and telecommunication services and thereby constitutes an "interference by a public authority" with the exercise of the applicants' right to respect for private and family life and for correspondence…'

[687] KILKELLY, s. 24.

[688] ÇOKSEZEN, s. 4.

[689] KILKELLY, s.23.

[690] KILKELLY, s. 24.

[691] KAYA, s. 92; TEZCAN -ERDEM - SANCAKTAR, s. 238. ;KILKELLY, s. 23.

müdahaleden imtina etmesinin de müdahale etkisini doğurduğunu vurgulamaktadır[692]. Bu bağlamda Mahkeme, bir kararda, başvuranın özel veya aile hayatına yapılmış bir müdahalenin varlığından bahsetmenin mümkün olduğunu ifade ederek, şikayete konu olayın devletin bir eylemi değil eylemsizliği olduğunu vurgulamıştır. 8. madde, bireyi kamunun keyfi müdahalelerine karşı korumayı amaçlamış olsa da, devleti, sadece bu tür müdahalelerden menetmekle kalmaz, bu negatif taahhüde ek olarak, başvuranın özel hayatı ve aile hayatına saygının sağlanmasını sağlamak amacıyla bazı pozitif yükümlülüklere zorlar[693].

2.2.1.3.3. AİHM'ye Göre Müdahale ve Takdir Yetkisi İlişkisi

Belirli bir anda, belirli bir yerde, bir sözleşme hakkı bağlamında bir kişinin hak veya özgürlüğüne konulacak sınırlamanın değerlendirilmesi[694], sözleşmenin aradığı şartların mevcut olup olmadığı ve sınırlamanın meşru olup olmadığı hususu, devletlerin takdirine bırakılmıştır. AİHM, ortak ve medeni ihtiyaçların günden güne artması ve devletin görevleriyle ilgili anlayışların değişmesi karşısında[695], sınırlamaya ilişkin koşulların oluşup oluşmadığı ve sınırlamanın gerekip gerekmediği konusunda üye devletlere bir takdir alanı bırakmaktadır[696]. Takdir hakkı, mahiyeti itibariyle, başkalarının denetimine mahal bırakılmaksızın yetkililerin kendi düşünceleri ve vicdani kanaatlerine uygun olarak hareket etme ve tasarrufta bulunabilmelerinin sağlanmasıdır[697].

Mahkeme, takdir hakkının sınırlarını sağlıklı bir şekilde belirleyebilmek, bu hususta dengeli bir politika izleyebilmeyi başarmak amacıyla, takdir hakkının sınırlarını belirlerken somut şartların yanı sıra, olayın geçmişini de dikkate almaktadır[698]. Her olayın şartlarını dikkate alma, sözleşme haklarının kısıtlanmasına ilişkin tasarrufun her olayda ayrı ayrı gerekçelendirilmesi ilkesi, adaletin tecellisi bakımından çok önemlidir. AİHM, bu şekildeki bir 'daraltıcı' yorum ile, müdahaleyi daha ayrıntılı olarak denetleme imkanını kendi uhdesinde tutmayı tercih etmektedir. Bu bağlamda, AİHM'nin sözleşme haklarına getirilmiş istisnalarla ilgili değerlendirmelerde daraltıcı bir yorum yaparak, bu

---

[692] DUTERTRE, s. 241.

[693] AIREY-İRLANDA, 9.10.197, Pr. 32-33.

[694] SUDRE, F: Droit Européen et International des Droits de l'Homme, Presses Universitaires de France, 7. Baskı, 2005, s.209.

[695] KALABALIK, Halil: " İdare Hukukunda Takdir Yetkisi Kavramı Ve Benzer Kurumlarla Karşılaştırılması", GÜHFD, CİLT I - SAYI 2 (9/1997), s.260.

[696] KAYA, s. 88.

[697] KALABALIK, s. 258.

[698] KILKELLY, s. 34.

kısıtlamaları genişletmeme gibi bir tercih yaptığı söylenebilir[699]. Bu yaklaşım da, AİHS haklarının özünü korumak amacıyla konulmuş açık bir garantidir. Aksinin kabulü istisnaların geniş yorumlanması ve takdir sakatlığı[700] denilebilecek suiistimallerin ortaya çıkması anlamına gelirdi[701].

AİHM'ye göre, devletlere tanınan takdir yetkisinin sınırları belirlenirken, devlet adına bu yetkiyi kullanan görevlilerin bu yetkiyi kullanma sıklığı ve derinliği belirlenmiş olmalıdır. Bunun yanı sıra, görevlilere tanınan bu yetkilerin yazılı veya yazısız olarak ve yeterli açıklıkta belirtilmesi gerekmektedir. Mahkemenin İspanya'yı[702] mahkum ettiği Prada Bugallo kararında, İspanyol Kanunu bu bakımdan eleştirilmiştir.[703] Mahkeme, takdir hakkının yalnızca yasal amacın kapsamına ilişkin değil, aynı zamanda müdahaleye de ilişkin olduğunu belirtmektedir[704].

Devletlerin, AİHS ile koruma altına alınmış hakları sınırlandırma gerekçeleri, daha çok önemli suçlarla mücadelenin zorluğudur. Bu bağlamda devletler tarafından en geniş şekilde kullanılmak istenen bu kısıtlamalar hakkında AİHM, haklar açısından genişletici, sınırlandırmalar bakımından da daraltıcı denilebilecek bir yorum getirmektedir[705]. Bununla birlikte, sınırlamalar konusunda devletlere tanınan takdir hakkı bazı suçlar bakımından daraltılmışken, belli suçlar bakımından takdir hakkı geniş tutulmuştur. Gerçekten de, keyfi uygulamalara karşı koruma sağlanmak kaydıyla, kişisel verilerin toplanması ve gizli izleme (surveillance) konularında devletlere geniş takdir yetkisi tanınmıştır[706]. Ancak bu yetki sınırsız değildir. Demokrasiyi koruma adına, yine demokrasinin altını oyacak veya hatta tahrip edebilecek nitelikte tedbirler alınamaz.

---

[699] OVEY/WHITE, s. 201.

[700] KALABALIK, (İdarenin Takdir Yetkisinin Sınırları), s.199.

[701] YARDIMCI, Mehmet Murat, Regulating Telephone Tapping In Turkey: The Influence Of The European Convention on Human Rights, University of Leicester (Faculty of Law),(Basılmamış Yüksek Lisans Tezi), 2005, s. 11.

[702] Mahkeme, benzer bir şekilde İtalya'yı da, ilgili kanunun, yetkili makamlara verilen takdir payının içeriğini ve uygulanma biçimini makul bir açıklıkla belirtmemesi nedeniyle eleştirmektedir. Bk. CALOGERO DIANA-İTALYA, 15/11/1996 , 56/1995/562/648, Pr.32.

[703] PRADA BUGALLO-İSPANYA Kararı, 18.02.2003 , (Başvuru no: 58496/00), Pr.28 '…le droit espagnol, écrit et non écrit, n'indiquait pas avec assez de clarté, au moment des faits, l'étendue et les modalités d'exercice du pouvoir d'appréciation des autorités dans le domaine considéré…' Bk. VALENZUELA CONTRERAS-İSPANYA, Pr. 61.

[704]LEANDER-İSVEÇ, 26.3.1987, 9248/81, Pr.59.

[705] YARDIMCI, s. 8.

[706] FOSTER, s. 360.

Devletler terör ve casuslukla mücadele adına, kendilerinin uygun gördüğü her türlü tedbire başvuramaz[707].

Takdir hakkının sınırsız olması zaten bu kavramın içeriğine ters düşecektir. Nitekim, bütün yetkilerin meşru ve yasal sınırları olduğu gibi, kamu otoritelerine verilen takdir yetkisinin de meşru ve yasal sınırları söz konusudur[708]. Bu bağlamda, devletlere takdir hakkı tanınmış olmasına rağmen, AİHM, bu hakkın kötüye kullanılması tehlikesi karşısında keyfiliği önleyecek tedbirler alınması gerekliliğini vurgulamaktadır. Kamu denetiminin olmayışı ve suiistimallerin doğuracağı tehlikelerin bertaraf edilmesini önlemek bakımından da, bireylere keyfi müdahalelere karşı korunma sağlanması (some protection to the individual against arbitrary interference) gerektiği ifade edilmektedir[709].

Sözleşmeci devletlere tanınan takdir hakkının denetlenmesinde AİHM, ilgili ülke makamlarının yerine geçerek karar verme gibi bir tavır takınmamaktadır. Mahkeme, başvuru konusu olayı bütünsel olarak değerlendirmekte, müdahalenin elde edilmek istenen yasal amaçla orantılı olup olmadığı ve yetkili makamlarca öne sürülen müdahale nedenlerinin yeterli ve olayla ilgili olup olmadığı hususlarında karar vermektedir[710].

---

[707] KLASS-ALMANYA Kararı, Pr.49 'Nevertheless, the Court stresses that this does not mean that the Contracting States enjoy an unlimited discretion to subject persons within their jurisdiction to secret surveillance. The Court, being aware of the danger such a law poses of undermining or even destroying democracy on the ground of defending it, affirms that the Contracting States may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate'.

[708] KALABALIK, Halil: "İdarenin Takdir Yetkisinin Sınırları Ve Yargısal Denetimi", GÜHFD, CİLT I - SAYI 1, (6/1997),s.197 (İdarenin Takdir Yetkisinin Sınırları).

[709] KILKELLY, s. 50.; ÇOKSEZEN, s. 5.; DOERGA-HOLLANDA, 50210/99,27.4.2004, Pr. 45; Bk. Ayrıca HALFORD-BİRLEŞİK KRALLIK, p.49; Keyfilik tehlikesine dikkat çeken AİHM, Leander kararında yeterli düzeyde açık bir kanun ile bu tehlikenin bertaraf edilebileceğini vurgulamaktadır. Mahkemeye göre kanun, devletin bu gizli ve potansiyel olarak tehlikeli tedbire hangi şartlar altında başvurabileceğini (the circumstances in which and the conditions on which the public authorities are empowered to resort to this kind of secret and potentially dangerous interference with private life) yeterince açık bir şekilde ifade etmelidir. (LEANDER-İSVEÇ, Pr. 51).

[710] HERTEL-İSVİÇRE, 25.8. 1998, 59/1997/843/1049, Pr. 46(iii).

2.2.2. AİHM İçtihatlarına Göre İletişimin Denetlenmesi

2.2.2.1. Geniş Anlamda İletişimin Denetlenmesi

İletişimin denetlenmesi ile ilgili olarak gerek AİHK'ye, gerekse AİHM'ye birçok başvuru[711] yapılmıştır. Konu, AİHM önüne ilk olarak 1978 tarihinde, Klass başvurusu ile getirilmiş[712]; Mahkeme, bu tedbirin 8. maddenin 2. paragrafı anlamında yasallığını (licéité) tasdik etmiştir[713]. AİHM, iletişim kavramını belli bir iletişim aracı belirtmek suretiyle daraltmak yerine, geniş bir bakış açısı kabul etmek şeklinde bir tercih yapmıştır. Gerçekten de, 8. maddenin 1. paragrafında açıkça zikredilmemesine rağmen, telefon görüşmelerinin, teleksin ve posta yoluyla gönderilen malzemelerin haberleşmenin kapsamına girdiği kabul edilmektedir. AİHM, haberleşme kavramını, teknolojik gelişmelere ayak uyduracak ve elektronik posta gibi diğer yöntemleri de içerecek şekilde geniş tutma eğilimindedir[714].

Özel hayat kavramının bir parçası niteliğinde klasik bir hak olarak kabul edilen[715] haberleşme hürriyeti, anılan maddede ifadesini bulan 'özel hayat' kavramının kapsamına girmektedir[716]. Milli güvenliği korumak, kamu düzenini sağlamak[717] ve suçların araştırılmasını sağlamak sorumluluğunu üstlenmiş olan devletler[718] bakımından, en kolay denetlenebilen iletişim türü olarak kabul edilen[719] telefon görüşmelerine ve diğer iletişim yöntemlerine uygulanacak tedbirlerin suçlarla mücadele

---

[711] İletişimin denetlenmesi ile ilgili olarak AİHM önüne getirilen davaların, AİHS ile korunan diğer haklara ilişkin davalara kıyasla az olduğu söylenebilir. Bu davaların en önemlileri arasında; KLASS-ALMANYA, MALONE- BİRLEŞİK KRALLIK, HUVIG-FRANSA, KRUSLIN-FRANSA, LAMBERT-FRANSA sayılabilir.

[712] ALCARAZ, s. 224; MOWBRAY, A.; Cases and Materials on the European Convention on Human Rights, Butterworths, 2001,391-392.; Klass kararı AİHM'nin iletişimin denetlenmesi ile ilgili birtakım standartlara atıf yaptığı bir karardır. Sözkonusu tedbirle ilgili Alman mevzuatı ve uygulamasının AİHS bakımından yeterli garantiler içerdiğini ifade eden Mahkeme hakimin kararının denetlenmesine imkan tanıyan bir mekanizmasının arzu edilir olduğunu belirtmesine rağmen varolan yapıyı yeterli bularak ihlale hükmetmemiştir.

[713] CHARRIER, Jean-Loup: Code de la Convention Européen des Droit de l'Homme, Lexis-Nexis, 2005, s. 510; ERGEÇ, s. 205.

[714] KILKELLY, s. 20; RENUCCI, Jean François: Droit Européen Des Droit De L'Homme, İkinci baskı, 2001, s.135.

[715] RENUCCI, s.135.

[716] CHARRIER, s.510; KLASS-ALMANYA. Pr.41.

[717] RENUCCI, s. 135.

[718] FENWICK, s. 670.

[719] CHARRIER, s. 510.

bakımından önemli birer araç oldukları kuşkusuzdur[720]. Bu hususun önemini bildiğini ifade sadedinde AİHM, devletlerin özellikle terör ve organize suçlarla mücadelesine destek vermek anlamında alınan birçok tedbiri mazur görmektedir[721]. Bununla birlikte, varlığı, kişilerin bilgisel özerkliği (informational autonomy) bakımından ciddi bir tehlike oluşturan bu tür tedbirlerin[722] kapsamının ve süresinin belirlenmesi gereklidir. Başka bir ifadeyle, tedbirin uygulanması bağlamında devlete tanınan yetkilerin net bir şekilde ortaya konulması gerekmektedir. Bu tür hususların öngörülmemiş olması, hakkında bu tür tedbirler uygulanacak kişiler bakımından 'öngörülebilme' bağlamında bir eksiklik doğuracaktır[723].

Telefon dinleme tedbiri, hemen hemen telefonun icat edildiği günden beri var olan bir uygulama olmasına rağmen, AİHS'ye taraf olan devletler, iletişimin denetlenmesini yasal bir zemine oturtmak konusunda tereddütlü davranmışlar, bu tereddüdün bir sonucu olarak da yakın zamana kadar birçoğu milli mevzuatında bu hususla ilgili düzenleme yapmaktan kaçınmıştır[724]. Bunun da ötesinde, bazı ülkeler, iletişimin denetlenmesinin düzenlemesi konusunda negatif bir tutum göstermişlerdir. Gerçekten de, Birleşik Krallık'ta[725] bu konuyla ilgili düzenleme yapan 'Interception of Communications Act'in[726] çıkarılması öncesinde, İngiliz Hükümeti, iletişimin

---

[720] ENGUÉLÉGUÉLÉ, S,/LOURDEL, S: " Three Recent Arguments For The Expansion Of Human Rights In French Criminal And Administrative Law", http://www.gonzagajil.org/pdf/volume1/Engueleguele/Engueleguele.pdf (İET:3.12.2007); RENUCCI, s. 35.

[721] Suçla mücadele, özellikle de organize suçla mücadele edebilmek amacıyla örgüt içine yerleştirilen gizli ajanlarla uyuşturucu tacirlerinin yaptığı telefon görüşmelerinin denetlenmesinin 8. maddenin ihlali anlamına gelip gelmediği hususu Lüdi-İsviçre davasına konu olmuştur. Mahkeme bu tür görüşmelerin 8. maddenin ihlalini oluşturmadığına karar vermiştir. Bk. SUDRE F./ MARGUENAUD J.P./ ANDRIANTSIMBAZOVINA J./GOUTTENOIRE A./LEVINET M., Les Grandes Arrêts de la Cour Européenne des Droits de l'Homme, (SUDRE/MARGUENAUD/ ANDRIANTSIMBAZOVINA/GOUTTENOIRE/LEVINET) Themis, yayınları, İkinci baskı, 2003, s. 332.

[722] FENWICK, s. 670.

[723] RENUCCI, s.135.

[724] FENWICK, s. 670.

[725] MALONE-BİRLEŞİK KRALLIK, Pr. 66 Müdahalenin milli hukuktaki yasal bir düzenlemeden kaynaklanması gerektiği ancak o tarihteki Birleşik Krallık'ta iletişimin denetlenmesinin kanunla yapılmadığı ifade edilmiştir. Aslında, bu başvuru konusu uygulama İngiliz hukukuna uygundu ve bu husus gerek Komisyon, gerek Hükümet gerekse başvurucular tarafından kabul edilmekteydi. Sorun bu uygulamanın bir kanun gücünü arkasına almamış olmasındaydı.

[726] Bu kanun 1985 yılında Birleşik Krallığın AİHS'nin 8. maddesi bağlamındaki yükümlülüklerini ihlal ettiğine karar verilmesi sonrasında çıkarılmıştır. (STONE,R: Textbook on Civil Liberties and Human Rights, Oxford University Press, 2004, s. 187); Parlamento, Malone kararlarına atıf yaparak bu kanunu hazırlamıştır. Bu kanunla İngiltere İçişleri Bakanlığı (Home Office) iletişimin denetlenmesi ile ilgili kararları(warrant) çıkarmakla görevlendirilmiş, sürecin yasallığını denetlemek için de ayrıca özel bir mahkeme (tribunal) kurulmuştur. Halford kararı, bu kanunun kamu organlarınca işletilen iç hatlarla ilgili bir düzenleme bulunmadığını tespit ederek yasal bir boşluğu işaret etmiştir. Bu boşluklar, 2000 tarihli RIPA'da doldurulmaya çalışılmıştır. Bu kanunla, kamu ya da özel hatlar marifetiyle yapılan tüm iletişime kasti ve yasal olmayan bir şekilde müdahale suç haline getirilmiştir. Sistemin işletmecisi ya da kontrolörüne,

denetlenmesi ile ilgili o zamanki idari usulleri düzenleyen mevzuatın, bireylerin çıkarlarını korumak bakımından yeterli olduğu ve bu tür yasalar çıkarılmasının gereksiz olduğu kanaatindeydi[727]. Ancak bu tür ihlaller sonrasında, Avrupa Konseyine üye ülkelerin birçoğu, bu hususstaki suiistimalleri önlemek amacıyla kanun çıkarmak zorunda kalmışlardır[728]. Bugün, iletişimin denetlenmesine ilişkin hükümler, birçok devletin mevzuatında yer almakta, organize suçlar ve terörizm suçlarıyla mücadelede etkin bir şekilde kullanılmaktadır[729].

2.2.2.2. AİHM'ye Göre İletişim Bilgilerinin Tespiti

İletişim bilgilerinin tespiti kavramı, herhangi bir iletişim aracı ile iki veya daha çok kişinin iletişim kurması ve kimlerin ne zaman arandığı, iletişimin ne kadar süreyle yapıldığı, telekomünikasyon yoluyla kimlerle iletişim kurulduğu hususlarına ilişkin bilgilerin belirlenmesi anlamına gelir[730].

Aboneye sunulan hizmetin doğru bir şekilde ücretlendirilmesini sağlamak, bunun yanı sıra olabilecek şikayet veya istismarları araştırmak için kullanılan kontör döküm cihazı (meter-comptage) marifetiyle, iletişimin içeriğine müdahale etmeksizin[731], hizmeti sunan bir şirketin meşru olarak edinebileceği bilgiler kayıt altına alınır. Bu cihazla bilgi edinilmesi iletişimin içeriğine müdahale anlamına gelen iletişimin yasadışı denetlenmesinden farklıdır. Bununla birlikte, telefon kayıtlarının hiçbir şekilde 8. maddenin ihlali anlamına gelmeyeceği söylenemez. Çünkü, telefon kayıtları, özellikle de aranan numaraların tespiti, telefon iletişiminin önemli unsurları hakkında bilgi verir. Sonuç olarak, AİHM, bahse konu bilgilerin abonenin rızası olmadan polise verilmesinin 8. madde kapsamında teminat altına alınan hakka bir müdahale olduğuna karar

---

örneğin, servisi sunan özel şirketin sahibine kendi sistemleri üzerinde müdahale hakkı tanınmıştır. Bk.MOWBRAY, s. 393.

[727] TELEPHONE TAPPING AND THE INTERCEPTION OF COMMUNICATIONS ACT 1985, Northern Ireland Legal Quarterly, Vol: 37, No: 2, Heinonline, 37 N.Ir. legal Q , 126, 1986, s.130.

[728] Hakim PETTITI, Çoğunluk Görüşü, MALONE-BİRLEŞİK KRALLIK .

[729] CHARRIER, s. 510.

[730] İletişim bilgilerinin tespiti kavramı, Malone davasında, bir telefondan aranan numaraları ve yapılan görüşmelerin süresini kaydeden bir cihazın (kontör döküm cihazı) kullanılması olarak tanımlanmıştır. (MALONE-BİRLEŞİK KRALLIK, Pr.83); Amerikan hukukunda telefon numarası tespit cihazı (pen register), giden aramalara ilişkin bilgileri , rota tespit cihazı (trap and trace device) ise gelen aramalara ilişkin bilgileri kaydeden cihazlardır. Bk. 18 U.S.C. § 3127(3), (4); Hukukumuzda ise, telefon kayıtlarının tutulması CMK 135. madde ile iletişimin tespiti adı altında düzenlenmiştir.

[731] SUDRE/MARGUENAUD/ ANDRIANTSIMBAZOVINA/GOUTTENOIRE/LEVINET, s. 332.

vermiştir[732]. Mahkeme, başvuru konusu uygulamanın yasayla öngörülmemiş olmasını ihlal nedeni saymıştır[733].

AİHM'nin verdiği karara katılan Hakim Pettiti, iletişim bilgilerinin ayrıntılı dökümünün çıkarılmasının, (comprehensive metering of telephone communications) normal kullanılma alanından farklı bir amaçla kullanıldığında, özel hayatın ihlali anlamına geleceğini ifade etmektedir. Bazen niteliksiz (neutral) bir bilginin işlenmesi, birtakım kritik bilgilere (sensitive data) ulaşılmasını sağladığı için, bu verilerin incelenmesi suretiyle yetkililer, aslında bilmemeleri gereken verilere ulaşmaktadırlar[734]. Öte yandan AİHM, P.G. ve J.H.-Birleşik Krallık başvurusunda ise, benzer bir durumda yapılan müdahalenin, ikinci fıkrada belirlenen şartlara uygun bir kanun uyarınca yapıldığına karar vermiştir[735].

Bu itibarla, iletişimin tespitine ilişkin işlemlerin de AİHM tarafından belirlenen kriterler çerçevesinde yapılması gerekmektedir. İletişimin tespitini de, AİHS'nin koruma şemsiyesi altına alan Mahkeme, bu konuda iletişimin denetlenmesine ilişkin olarak aradığı şartların varlığı halinde bu tür bir tedbire başvurulabileceğini belirtmektedir. Gerçekten de Malone kararında iletişimin tespitinin kanunla düzenlenmemiş olmasını ihlal nedeni sayarken, AİHM, bir kanunun taşıması gereken tüm diğer şartların taraf ülke tarafından kendiliğinden dikkate alınması gerektiğini zımnen vurgulamış olmaktadır.

2.2.2.3.İletişimin Denetlenmesinde İş Hayatı-Özel Hayat ilişkisi

AİHM'ye göre; Sözleşmenin 8. maddesiyle sağlanan teminatın esas amacı, diğer insanlarla olan ilişkisi esnasında, bireyin, kişiliğini geliştirmesini sağlamak ve bu süreçte dışardan müdahale olmasını engellemektir[736].

Bir çok insan bakımından, dış dünyayla ilişki kurma fırsatı, genellikle iş hayatı sırasında ortaya çıktığından mesleki veya iş dünyasıyla ilgili faaliyetleri 'özel hayat' kavramından hariç tutmak AİHM'ye göre doğru değildir. Öte yandan, bir kişinin yaptığı işlerden

---

[732] MALONE-BİRLEŞİK KRALLIK, Pr. 84.

[733] DUTERTRE, s. 260-261.

[734] Hakim PETTITI, MALONE-BİRLEŞİK KRALLIK.

[735] DUTERTRE, s. 261.

[736] BOTTA-İTALYA, 24.2.1998 (153/1996/772/973), Pr.32 (İET:13.12.2007) 'Private life… includes a person's physical and psychological integrity; the guarantee afforded by Article 8 of the Convention is primarily intended to ensure the development, without outside interference, of the personality of each individual in his relations with other human beings.'

hangilerinin meslek veya iş hayatına girdiği, hangilerinin ise bu alanın dışında kaldığını net bir şekilde belirlemek her zaman mümkün değildir. Hele de, serbest çalışan bir kişinin varlığı halinde, kişinin iş hayatı, özel hayattan ayırt edilemeyecek bir boyuta ulaşmış olabilir. Bu durumda, şikayet konusu önlemin sadece mesleki faaliyetlerle ilgili olduğuna dayanarak 8. maddenin kapsamı dışında kaldığını savunmak, icra ettiği mesleğinin onu eşit olmayan bir muameleye maruz bırakması anlamına gelebilir. Mahkeme bu sebepten dolayı, bu tür ayrımlara girmemiş ve hem iş, hem de özel konuşmaların dinlendiği telefon dinleme faaliyetlerinin özel hayata müdahale olduğuna karar vermiştir. Tedbirin sadece işyerine yöneltilmesi halinde de, Mahkeme, işyerinin özel hayat dışında yorumlanması gerektiği gibi bir tavır almamıştır[737].

Halford-Birleşik Krallık davasında Mahkeme, işe[738] ya da özel hayata taalluk ettiğine bakılmaksızın bütün telefon görüşmelerini, 8. madde kapsamında korunan bir hak olarak kabul etmiştir[739]. Mahkemeye göre, özel hayat başkalarıyla belli bir düzeyde ilişki kurmak ve bu ilişkileri geliştirmek hakkını kapsar. Mesleki nitelikteki ilişkiler ve faaliyetlerin bu kapsam dışında tutulmasını makul gösterecek herhangi bir haklı neden bulunmamaktadır[740]. Mahkeme, Kopp-İsviçre davasındaki değerlendirmesinde de; önceki içtihatlara atıfta bulunarak, bir avukatlık bürosu gibi işyerlerinden yapılan görüşmeler bakımından, gelen ve giden aramaların 8/1. madde anlamında özel hayat ve haberleşme kavramlarının kapsamına girebileceğini ifade etmektedir[741].

---

[737] NIEMETZ-ALMANYA, Pr. 33-34; Mahkeme, Huvig Kararına konu olan iletişimin denetlenmesi tedbirini, başvurucunun işyerine tatbik edilmesine (Pr. 8) rağmen özel hayat kapsamı dışında tutmamış; kamu otoritesi tarafından uygulanan tedbirin bir müdahale olduğuna karar vermiş(interference by a public authority) ve bu durumu hem haberleşme hürriyetinin (right to respect for their correspondence) hem de özel hayatın bir ihlali olarak değerlendirmiştir. HUVIG-FRANSA, Pr. 25.

[738] HALFORD davasında, Birleşik Krallık hükümeti yapılan bu denetlemenin özel hayatı ihlal anlamına gelmeyeceğini, işte yapılan görüşmelerin nitelik itibariyle özel olamayacağını savunmuştur. AİHM ise bu iddiayı kabul etmemiştir. (SUDRE/MARGUENAUD/ ANDRIANTSIMBAZOVINA/GOUTTENOIRE/LEVINET, s. 333).

[739] KILKELLY, s. 11; ÇOKSEZEN, s. 4.; SUDRE/MARGUENAUD/ ANDRIANTSIMBAZOVINA/ GOUTTENOIRE/LEVINET, s. 333; HALFORD-BİRLEŞİK KRALLIK, Pr. 44 '… telephone calls made from business premises as well as from the home may be covered by the notions of "private life" and "correspondence" within the meaning of Article 8 Pr. 1'

[740] ROTARU-ROMANYA, 28341/95, 4 May 2000, Pr.43.

[741] KOPP-İSVİÇRE, 13/1997/797/1000, 25.3.1998 Pr. 50, 53; Mason örgütüne üye olan hakimler hakkında disiplin davası açılması sonrasında Mahkeme önüne gelen N.F.–İtalya davasında, ilgililerin bazılarının adlarının basında yayımlanması üzerine Mahkeme, özel alanın, bireyin fiziksel ve psikolojik bütünlüğünü de kapsadığı gözleminde bulunarak, ifşa edilen bilgilerin kolayca erişilebilme özelliğine ve de yapılan basın toplantısının bir zarara neden olmadığı hususuna dikkat çekerek bir ihlal olmadığı sonucuna varmıştır.(DUTERTRE, s. 244).

2.2.3. AİHS'ye ve AİHM İçtihatlarına Göre İletişime Müdahalenin Koşulları

2.2.3.1.Genel Olarak

Hayat hakkı ve vücut bütünlüğü gibi hakların dışındaki tüm sözleşme hakları sınırlandırmaya konu olabilirler. Böylece birey, ceza tehdidi altında başkalarının haklarına ve kamu yararına tecavüzde bulunmamış olur[742]. Hakların sınırlanmasının altındaki temel amaç, olağan dönemlerde demokratik kurumların korunmasının sağlanmasıdır. AİHS iki tür sınırlandırma kategorisi öngörmektedir. Bunlardan ilki hakların kötüye kullanılmasının önüne geçmeyi amaçlar. Daha güçlü olan diğer neden ise, kamu düzenini korumak amacına matuftur[743]. AİHS'de tanınan hakların hangi durumlarda sınırlandırılacağı, sözleşmede yer alan ve ayrıca AİHM tarafından da birtakım prensiplere bağlanan bir hususdur. AİHS'nin 8, 9, 10 ve 11. maddelerinin kaleme alınmasında, ilk etapta hakkın tanımı ve kapsamı, takip eden bölümde de, bu şartların sınırlandırılıp sınırlandırılmayacağı ve hangi durumlarda sınırlandırılacağı bir sistem olarak benimsenmiştir.

Oldukça gelişmiş formdaki suçlar ve suçlular tarafından tehdit edilen devletlere, bu suçlarla mücadele amacıyla gerekli olan imkanların verilmesi gerektiğini, bu bağlamda iletişimin denetlenmesine imkan tanıyan yasal düzenlemelerin varolmasının doğal olduğunu [744]ifade eden AİHM, özel hayat hakkının sınırlarını belirlerken genişletici ve bu hakka ilişkin kısıtlamaları belirlerken de daraltıcı[745] bir yorum yapmıştır[746]. Bu hakçı yorum tarzının bir yansıması, kişilerin durumundan ve olayların doğasından kaynaklanan sınırlamalara gidilip gidilmeyeceği hususunda ortaya çıkmaktadır. Hakların sınırlandırılmasında, Sözleşme'nin lafzıyla ifade edilen sınırlandırmaların yanı sıra kişilerin durumundan veya olayların doğasından kaynaklanan birtakım sınırlandırmaların (inherent limitations) olup olmayacağı konusunda AİHK'nın ilk zamanlardaki ilginç tavrı tartışma konusu olmuştur. Sözleşmede belirtilen sınırlandırılmaların haricinde; mahkum, tutuklu, evsiz barksız serseri (vagrant) kişilerin, içlerinde bulundukları özel durum nedeniyle birtakım sınırlamaya müstahak oldukları görüşü AİHK tarafından ve J. Fawcett gibi bazı yazarlar tarafından kabul görse de bu görüş daha sonra Mahkeme tarafından reddedilmiştir. AİHM'ye göre, sözleşme

[742] ERGEÇ, Ruşen, Protection Européenne et Internationale des Droit de l'Homme, Bruylant, 161.

[743] SUDRE, s.206.

[744] KLASS-ALMANYA, Pr.48.

[745] ERGEÇ, s. 163.

[746] YARDIMCI, s. 8; SUDRE, s. 208.

haklarından birine yine sözleşme tarafından öngörülen sınırlandırılmalar uygulanabilir ve kabul edilen bu sınırlandırmalar dışındakilerin kabul edilmesi mümkün değildir.[747]

Mahkemeye göre, 8. maddenin ikinci paragrafında sınırlamalar net olarak belirtilmiş olup, örtülü sınırlandırmalar(implied limitations) kabul edilemez[748]. Sözleşme haklarına getirilebilecek sınırlamaların tespiti bağlamında, 8. maddenin lafzıyla ve AİHM içtihatları ile belirlenen şartlar, iletişimin denetlenmesine ilişkin sınırları belirlemeleri bakımından önemlidirler. Bu şartların yokluğunda, keyfiliğin ve suiistimallerin artacağı kuşkusuzdur[749]. Keyfi uygulanmaları bertaraf etmeye karşı etkin ve yeterli teminatları barındırmayan bir gizli izleme mekanizmasının da, demokrasiyi korumak adına demokrasiye zarar verebileceği muhakkaktır[750].

8. maddeden kaynaklanan hakka ilişkin bir kısıtlama getirilmek istenmesi halinde, AİHS üçlü bir test uygulamaktadır. Bunlar; müdahalenin yasaya uygunluğu, müdahalenin meşru bir amaç gütmesi ve müdahalenin demokratik bir toplumda zorunlu olmasıdır[751]. Mahkeme, müdahalenin taşıması gerekli şartlar bakımından yaptığı test sonucunda bu üç şarttan herhangi birinin yerine getirilmediğine kanaat getirirse diğer şartların mevcudiyetini incelemez. Bu duruma örnek olarak gösterilebilecek davalardan biri olan MM-Hollanda davasında bu ilkelerden birine aykırılık teşkil eden bir durumun varlığını tespit eden AİHM, 8. maddenin ihlaline hükmetmiştir. Mahkeme daha ileri bir değerlendirme yapmayı gerekli bulmamış ve müdahalenin kanuna uygun olmadığı tespitini yaptıktan sonra, müdahalenin meşru bir amacı hedefleyip hedeflemediği ve demokratik bir toplumda gerekli olup olmadığı hususlarını incelemeye gerek görmemiştir[752].

Sözleşme ile belirlenen sınırlandırma şartları şunlardır:

---

[747] OVEY/WHITE, s.199-200.

[748] Mahkemeye göre, AİHS'de kabul edilen sınırlandırma tarzı, örtülü sınırlandırmalara izin vermemektedir. '…The restrictive formulation used at paragraph 2 (art. 8-2) ("There shall be no interference ... except such as ...") leaves no room for the concept of implied limitations…' GOLDER-BİRLEŞİK KRALLIK, 21.2.1975, ,4451/70, Pr.44.

[749] YARDIMCI, s.10-11; AİHM, bireylerin haklarının kısıtlanması gündeme geldiğinde, sınırları belirleme gibi bir misyon yüklenmektedir. Çünkü, yetkinin kötüye kullanılması riski ihlallere neden olabilmektedir. Mahkeme, 8. maddede belirlenmiş hakkın, keyfi uygulamalar karşısında erozyona uğramamasını sağlamak bakımından bireyin korunması gerektiğini ifade etmektedir.DOERGA-HOLLANDA, Pr. 45.

[750] KILKELLY, s. 37.

[751] OVEY/WHITE, s. 201-202; ERGEÇ, s. 161 ; SUDRE, s. 208; LAMBERT-FRANSA, 24.8.1998, (88/1997/872/1084), Pr.22; SUDRE, s. 208; ŞEN, (İletişimin Denetlenmesi Tedbiri), s. 98; ERRERA, Roger: "Les Origines de la loi Française du 10 Juillet 1991 sur Les Ecoutes Téléphoniques", Revue Trimestrielle Des Droits De L'Homme, Bruylant, dr.h.(55/2003),(85--870),s.859

[752] MM-HOLLANDA, 8.4.2003, 39339/98, Pr. 46.

2.2.3.2.İletişime Müdahalenin Kanunla Yapılması

İletişime yapılan müdahale, bu nitelikte olmayan bir müdahaleden daha tehlikelidir. Çünkü, ilgili, kendisinin bir müdahalenin mağduru olduğunun farkında bile değildir[753]. Bu tehlikenin bertaraf edilebilmesi bakımından, yasal bir sistem dahilinde iletişime yapılacak müdahalenin yasallığını denetleme testi ihdas etmek zorunludur[754]. Bu tutumun sergilenmemesinin alternatifi, keyfiliğe izin verecek bir yasal boşluğa (legal vacuum) müsaade edilmesidir. Bu bağlamda, birtakım tedbirlerin alınması, muhtemel bir boşluğun engellenmesine hizmet edecektir. Bu tedbirler arasında, tedbirin uygulanma tarzı ile ilgili kontrolden sorumlu kurumların belirlenmesi (ex post facto control of the manner of implementation of measures of interception), denetleme tedbirinin sona erdirilmesi ile ilgili sürelerin tayin ve tespiti, müdahale ile elde edilen verilerin imhasına ilişkin yöntemlerin belirlenmesi, mahrem bir alanda ve mahrem bir bağlamda söylenen sözlerin korunması da bulunmaktadır[755].

AİHS, iletişimin sınırlandırılması için kanunun varlığını şart koşmuştur[756]. Bu şart, 8. maddenin ikinci paragrafında 'Bu hakkın kullanılmasına bir kamu otoritesinin müdahalesi,… kanunla öngörülmüş olmak koşuluyla söz konusu olabilir.' denilmekle tartışmaya ve yoruma yer bırakmaksızın açıkça ifade edilmiştir. AİHM de, AİHS'de yer alan bu hükmü verdiği kararlarla desteklemiş, 1983 tarihli Malone kararında[757] Silver and Others kararına[758] da atıf yapılarak o tarihte Birleşik Krallık kanunlarında iletişimin denetlenmesinin kanunla düzenlenmediğini belirterek ihlal kararı vermiştir[759]. Halbuki iletişimin denetlenmesi ile ilgili hükümleri içeren yasal bir düzenlemenin varlığı halinde

---

[753] Hakim PETTITI,(Çoğunluk Görüşü) MALONE-BİRLEŞİK KRALLIK.

[754] KILKELLY, s. 21.; ŞİMŞEK, s. 4.

[755] Hakim PETTITI,(Çoğunluk Görüşü) MALONE-BİRLEŞİK KRALLIK.

[756] ŞEN, (İletişimin Denetlenmesi Tedbiri), s.99.

[757] MALONE-BİRLEŞİK KRALLIK, Pr. 66.

[758] SİLVER VE DİĞERLERİ-BİRLEŞİK KRALLIK, 25 Mart1983, (Başvuru no. 5947/72; 6205/73; 7052/75; 7061/75; 7107/75; 7113/75; 7136/75),Pr.83. Müdahalenin milli hukuktaki yasal bir düzenlemeden kaynaklanması gerektiği ifade edilmiştir. (… the interference in question must have some basis in domestic law…). Aslında bu başvuruya konu olayın olduğu tarihte şikayet konusu uygulama İngiliz hukukuna uygundu ve bu husus gerek Komisyon, gerek Hükümet gerekse başvurucular tarafından kabul edilmekteydi. Sorun bu uygulamanın bir kanun gücünü arkasına almamış olmasındaydı.

[759] KILKELLY, s. 26; TEZCAN/ERDEM/SANCAKTAR, s.237.;Birleşik Krallık'ta iletişimin denetlenmesi ile ilgili yasal düzenleme yapılması öncesinde, bu tedbir gizli birtakım idari emirlerle (secret administrative guidance) yürütülmekteydi. AİHS'nin Birleşik Krallık hukukunun bir parçası sayılabilmesi için gerekli olan yasal düzenleme (1998 Human Rights Act) başvuruya konu olan olay tarihi itibariyle çıkarılmamıştı. Mahkemeler de, iletişimin denetlenmesine ilişkin olarak verilen kararları, herhangi bir hakkı ihlal etmedikleri gerekçesiyle tasdik etmekteydiler. AİHM tarafından verilen bir dizi karar sonrasında, değişik denetleme tekniklerini düzenleyen mevzuat ortaya konuldu ve bu yasal düzenlemeler bugün Regulation of Investigatory Powers Act (RIPA) 2000 denilen bir kanun çatısına alındı. FOSTER, s. 361, 389.

Mahkeme, devletlerin yasal amaçları (legitimate aim) elde etmek maksadıyla uyguladıkları sınırlamaları meşru görmektedir. Nitekim, Klass kararında, iletişimin denetlenmesine ilişkin düzenlemenin bir kanunla öngörüldüğünü, bu kanunun Parlamento tarafından kabul edildiğini ve Federal Anayasa Mahkemesi tarafından değişikliğe uğratıldığını, başvuru konusu tedbirin milli güvenliğin korunması, kamu düzeninin sağlanması ve suç işlenmesinin önlenmesi gibi yasal amaçlarla gerçekleştirildiğini tespit ederek 8. maddenin ihlal edilmediğine karar vermiştir[760].

Mahkemeye göre, iletişimin denetlenmesine ilişkin kanunun varlığı (the mere existence of the legislation itself…) zaten bir izleme ihtimalinin ifadesi olduğundan burada haberleşme özgürlüğünün ihlal edilmesi tehlikesi vardır[761]. İletişimin denetlenmesi ve son zamanlarda artış eğilimi gösteren gizli görüntü kaydının özel hayatı ağır bir şekilde tahrip etmesi nedeniyle Mahkeme, taraf devlet kanununun yeterliliğine özel önem vermektedir[762]. Kanun kavramını dar bir şekilde yorumlamayan Mahkeme, ulusal düzeyde geçerli, uygulanabilir ve erişilebilir hukuk metinlerini kanun[763] olarak kabul etmektedir[764]. Müdahalenin bu formattaki bir kanuna dayanmasını şart koşan AİHM, yapılan müdahalenin yürürlükte olan kanuna uymadığı tespitini yapar yapmaz davayı sonlandırmakta ve müdahalenin ihlal oluşturduğuna karar vermektedir[765].

2.2.3.2.1.Kanunun İçeriği ve Şekli

Müdahalenin kanuna uygunluğu (In accordance with law/prevu par la loi) kriteri ile, Sözleşmeye taraf devletin iletişimin denetlenmesine imkan tanıyan bir mevzuatı düzenlemesi zorunluluğu getirilmiştir. Bununla birlikte, konuyla ilgili milli hukukun varlığı yeterli değildir. Kanunun, AİHS ve AİHM tarafından belirlenen kriterlere uygun olması da önemlidir[766]. Gerçekten de bu ilke ile, milli hukukun birtakım temel özelliklere sahip olması gerektiği vurgulanmış, müdahaleyi mümkün kılan uygulamanın 'hukukun

---

[760] SUDRE/MARGUENAUD/ ANDRIANTSIMBAZOVINA/GOUTTENOIRE/LEVINET, s. 333-334.; ÜNAL, s. 222. ; Bk. ERRERA, s.859.

[761] KLASS- ALMANYA, Pr.41.

[762] LEACH, Philip: Taking A Case to the European Court of Human Rights, Oxford University Press, Second Edition, s.289.

[763] AİHM'nin aradağı kanun, başvuru konusu problemle ilgili salt bir kanun metni değildir. Mahkeme Lambert davasında (Pr. 23) kanunun özelliklerine de atıf yapmakta, erişilebilirlik (accesibility), öngörülebilirlik(foreseebility) ve açıklık(clarity-clarte) şartlarının da varlığını aramaktadır.

[764] DİNÇ, s. 384.

[765] KILKELLY, s. 25.

[766] LAMBERT -FRANSA, Pr. 23.

üstünlüğü' kuralına uygun olması ve milli hukukta bir dayanağının bulunması zorunlu kılınmıştır[767].

İletişim araçları, teknolojinin gelişmesi ile her geçen gün daha girift bir hal aldıklarından dolayı, iletişimin denetlenmesine imkan veren kanunlar da bu gelişme hızından kaynaklanan sorunların ortadan kaldırılması amacıyla açık ve detaylı bir tarzda kaleme alınmalıdırlar[768]. Kanun; belirsizlik ve karmaşıklık içermemeli; bu bağlamda, kanunlarda farklı yorumlara yol açacak ifadelere yer verilmemelidir[769]. Ayrıca, kanun, görevlilere tanınan yetkileri ve bu yetkilerin kapsamını açıkça ifade etmeli, tanınan takdir hakkının sınırları net bir şekilde belirlenmiş olmalıdır. Gerçekten de, yetkilerin gizli olarak kullanıldığı bir yerde, keyfilik (arbitrariness) kaçınılmaz bir risk olarak ortaya çıkmaktadır[770]. Bu bağlamda, milli hukukta keyfi uygulamalara karşı yeterli (adequate)[771] bir yasal koruma sağlanmalıdır[772]. Bir başvuruda, ilgili İngiliz kanununu birçok bakımdan takdir edici ifadelerle takdim eden Mahkemenin detaylara vurgu yapması önemlidir. Nitekim, yasal metinlerdeki belirsizlikler ve boşluklar birtakım keyfi uygulamalara yol açma riskini taşımaktadırlar. Milli hukukun özellikle temel hürriyetlerle ilgili konularda ayrıntılı düzenleme yapması olası keyfi müdahaleleri en aza indirgeyecektir[773].

Kanunun yazılı olması bir zorunluluk olarak belirtilmemiştir, başka bir deyişle kanun, yazılı olmayan bir metin olarak da karşımıza çıkabilir[774]. Cevaplandırılması gerekli olan

---

[767] OVEY/WHITE, s. 201-202; LAMBERT -FRANSA, Pr. 23.

[768] KRUSLIN-FRANSA, 24.4.1990, 11801/85, Pr. 33; Lambert kararında AİHM, Fransız Ceza Usul Kanununda yapılan değişikliklerin, özellikle de bahsekonu kanun metninin açık ve detaylı hükümler içermesi nedeniyle memnuniyet verici olduğunu ifade etmektedir. LAMBERT -FRANSA, Pr. 28.

[769]MALONE-BİRLEŞİK KRALLIK, 24.8.1984, 8691/79, Pr.79 Polisiye amaçlı iletişim denetlenmesine ilişkin İngiliz ve Galler kanunlarını eleştiren AİHM, bu kanunların belirsiz ve değişik yorumlara imkan tanıyan (obscure and open to differing interpretations) bir formatta olduğunu belirtmiştir. AİHM, milli mahkemelerin yetkilerini gasp anlamına gelebilecek amirane bir ifadeden kaçındığını ifade ettiken sonra, 8. maddenin ikinci paragrafında belirlenen standartlar çerçevesinde, milli hukukun, iletişimin denetlenmesi alanında yetkileri makul bir açıklık ve berraklıkla (reasonable clarity)ortaya koymak zorunda olduğunu ifade etmiştir. AİHM, İngiltere ve Galler'deki iletişimin denetlenmesi ile ilgili mevzuatın detaylı bir şekilde hazırlandığını kabul etmekle birlikte, bu alanda hangi yetkilerin yasal kurallara bağlandığını hangilerinin ise yürütmenin takdirine bırakıldığı hususunda yeterli bir açıklığın bulunmadığını dikkate getirmektedir. Bu bağlamda, mahkeme, mevcut mevzuatın demokratik bir toplumda vatandaşların hukukun üstünlüğü ilkesi çerçevesinde hak ettikleri minimum düzeydeki yasal korumayı içermediğine karar vermiştir.(MALONE-BİRLEŞİK KRALLIK)

[770] MALONE-BİRLEŞİK KRALLIK, Pr. 67.

[771] ANDERSON-İSVEÇ- 25 Şubat 1992, Series A No.226-A, 226, 14 E.H.R.R.615 Pr. 75.

[772] KRUSLIN-FRANSA, Pr. 30.

[773] YARDIMCI, s. 14.

[774] ERGEÇ, s.161; DUTERTRE, s. 260; MALONE-BİRLEŞİK KRALLIK, Pr.66; SUNDAY TIMES-BİRLEŞİK KRALLIK, 26.4.1979, (1979-80) Pr.46-47 Sunday Times davasında başvuranlar diğer iddialarının yanı sıra

bir diğer soru da, müdahaleye imkan tanıyan hukuksal düzenlemenin biçimsel anlamda kanun olması zorunluluğunun bulunup bulunmadığıdır. Başka bir ifadeyle, kanunun, yasama organının ürünü olması bir zorunluluk mudur? Bu konuda mevcut olan ilk yaklaşıma göre, önemli işlerin yasama organı, daha az öneme sahip konuların ise diğer organlarca kararlaştırılması gerekir. "Önemlilik teorisi" olarak da adlandırılan bu yaklaşıma göre, düzenlemelerin biçimsel anlamda da kanun formatında olması gerektiği ileri sürülmektedir. Bu teoriye göre, iletişime, örf adet hukuku kapsamında yer aldığı varsayılan bir hükme dayanılarak müdahale edilemez. 8. maddenin 2. paragrafında yer alan şartların karşılanabilmesi bakımından müdahalenin mutlaka yazılı bir kanunla düzenlenmesi gerekir[775]. Müdahalenin kanundan kaynaklanmadığı, idari uygulamalar veya bağlayıcı olmayan rehber kurallara dayalı olarak gerçekleştirildiği haller, AİHS'nin öngördüğü ilkeler çerçevesinde kabul edilebilir değildir[776]. Gerçekten de, Fransa'yla ilgili bir kararda Mahkeme, iletişimin denetlenmesi konusunda yargı içtihatlarına dayanmanın yeterli olamayacağını, bunun da ötesinde bu nitelikte tedbirlerin genel nitelikteki kanunlara da dayandırılamayacağını belirtmiştir. İletişimin denetlenmesini düzenleyen kanunda, koşullar, yöntem, bu tedbirin hangi suçlar için ve kimlerle ilgili olarak uygulanacağı, süre ve sair sınırlamalar gibi konuların ayrıntılı olarak düzenlenmesi gerektiği vurgulanmıştır[777].

İkinci yaklaşım ise, kanun kavramının , daima şekli ya da biçimsel olarak değil, maddi olarak anlaşılmasının ve özellikle yazılı olmayan hukukun da bu kavram kapsamında

---

mahkemeye hakaret (contempt of court) uygulamasının müdahalenin kanuna uygunluğu (In accordance with law/prevu par la loi)kriterine uymadığını, Lordlar Kamarası tarafından va'zedilen bu uygulamanın belirsiz ve tuhaf uygulamaları içerdiğini iddia etmişlerdir. Hükümet, bu uygulamanın ana hatlarıyla bile olsa öngörülebilir (roughly foreseeable) olduğu savunmasını yapmıştır. Bu sorun hakkında değerlendirme yapan AİHM, kanun ifadesinin sadece yazılı olan kuralları içermediğini, yazılı olmayanların da kanun kapsamına girdiğini bu bağlamda, mahkemeye hakaret(contempt of court) uygulamasının bir 'common law' uygulaması olmasının, bu hukuki düzenlemenin kanun olmadığı anlamına gelemeyeceğini ifade etmiştir. Aksinin kabulü, AİHS'yi kaleme alan yasakoyucunun iradesine muhalif bir tavır olur. Gerçekten de, common law kapsamına giren bir müeyyidenin Sözleşmenin kabul ettiği anlamda kanun olarak kabul edilmemesi bu müeyyidenin uygulandığı ülkenin hukuk sistemininin temellerini zedelemek anlamına gelir.

[775] ERDEM, Gizli Soruşturma , s. 187.

[776] KILKELLY, s. 25.

[777] DİNÇ, s. 425.; AİHM, HUVIG ve Kruslin davalarında, Fransız mevzuatında, iletişimin denetlenmesi ile ilgili yeterli garantilerin yer almadığına dikkat çekmiştir. Mahkemeye göre; yargısal bir kararla telefonları dinlenmesi muhtemel insan kategorileri, iletişimin denetlenmesini gerektirecek suçlar, tedbire ilişkin süre, hakime verilecek yetki, tedbir konusu diyalogları içeren özet raporlar, kayıtların silinmesi veya bantların imha edilmesine ilişkin haller, kamu görevlilerine tanınan yetki net bir şekilde belirlenmemiştir. Konuyla ilgili tek metin Ceza Usul Kanunu'nun eski 81. maddesidir ki, bu madde de birtakım belirsiz (vague) ve kesin olmayan (imprécis) hükümler içermemektedir ve öngörülebilirlik koşulunu karşılamamaktadır. Bk. CHARRIER, s.511.

kabul edilmesinin gerektiğini savunmaktadır[778]. Tüzük, yönetmelik, yerleşmiş mahkeme içtihatları, hatta genelgeler bile kanun kapsamında değerlendirilebilir[779].

2.2.3.2.2.Kanunun Özellikleri

AİHM, verdiği kararlarda kanunun özelliklerini belirlemiştir. Mahkeme, öncelikle, milli hukukta özel hayat hakkında müdahale öngören bir mevzuatın olmasını ve kanunun 'hukukun üstünlüğü'[780] ilkesiyle bağdaşır nitelikte olması gerektiğini ifade etmektedir[781]. Bunun yanı sıra kanun, vatandaşların erişimine müsait olmalı ve ilgili kişiye kanunun uygulaması ile ilgili bir öngörme yeteneği sunmalıdır. Başka bir ifadeyle kanun, bir eyleme bağlanabilecek hukuki sonuçları gösterecek şekilde yeterli açıklık ve kesinlikte kaleme alınmalıdır[782]. Mahkeme, kanunun formel yapısının değil ruhunun önemli olduğunu ifade ederek[783], kanunun kalitesine[784] önem vermektedir[785]. Bu bağlamda AİHM, Kruslin kararı öncesinde Fransa'daki telefon dinlenmesi ile ilgili uygulamanın, Fransız Yargıtay'ının Ceza Usul Kanunu'nun bazı maddelerini yorumlaması suretiyle yapıldığını, bu içtihadın kanun olarak değerlendirilebileceğini, başka bir ifadeyle, 8. maddenin ikinci fıkrasında sayılan 'müdahalenin yasaya uygun olarak yapılması ' şartını karşıladığını ifade etmektedir. Bununla birlikte, AİHM, bahse konu 'kanun'nun AİHS'nin aradığı özelliğe (sufficient precision) sahip olmadığını belirterek ihlal kararı vermiştir[786].

Adı kanun olan her düzenlemenin kanun niteliğinde olmadığını belirten Mahkemeye göre bu kavramın bazı unsurları da ihtiva etmesi gerekmektedir[787]. Hakları sınırlayıcı

---

[778] TEZCAN/ERDEM/SANCAKDAR, s. 239; KÜNHE, s. 101.

[779] KAYA, s. 92.

[780] TEZCAN/ERDEM/SANCAKDAR, s. 240.

[781] ALCARAZ, s. 228-229.

[782] LAMBERT-FRANSA, Pr. 23; OVEY/WHITE, s.201-202; ERDEM, Gizli Soruşturma, s. 184.KüNHE, s. 100; AKDENIZ, s. 13.; DUTERTRE, s. 259-260; ERGEÇ, s.162; SUDRE/MARGUENAUD/ ANDRIANTSIMBAZOVINA/GOUTTENOIRE/LEVINET, s. 334; SUDRE, s. 209.

[783] SUDRE, s. 209; ŞEN, (İletişimin Denetlenmesi Tedbiri), s.99.

[784] AİHM, Huvig ve Kruslin kararlarında, Fransa'yı, iletişimin denetlenmesine imkan tanıyan bir yasa bulunmadığı için değil, varolan yasa suiistimalleri önleyecek kalitede ve açıklıkta olmadığı için mahkum etmiştir. (ENGUÉLÉGUÉLÉ, /LOURDEL, "Three Recent Arguments For The Expansion Of Human Rights In French Criminal And Administrative Law").

[785] ERRERA, s. 860.

[786] MOWBRAY, s.394; …interception… must accordingly be based on a "law" that is particularly precise. It is essential to have clear, detailed rules on the subject, especially as the technology available for use is continually becoming more sophisticated" (KRUSLIN-FRANSA, Pr.33).

[787] ALTIPARMAK, Kemal: Büyük Biraderin Gözetiminden Çıkış: Telefonların izlenmesinde Devletin Sorumluluğu, TBB Dergisi, Sayı 63, 2006, s. 37.; Bu bağlamda, bir çok Avrupa ülkesi mevzuatı ,

bir nitelik taşıyan kanun, yetkililerin suiistimallerine karşı etkili garantileri de kapsamalıdır[788]. Nitekim, belirli güvenceler alınmak suretiyle keyfiliği izale edilmemiş tedbir, meşru amaçlara yönelik olsa bile 8. maddeye aykırı olacaktır.

Bu yaklaşımın bir göstergesi olarak AİHM, iletişimin denetlenmesi ile ilgili olarak gelen başvurularda, ilgili milli hukuktaki eksiklikleri çıkarmak suretiyle diğer hukuk sistemlerindeki eksikliklerin tespiti için bir kontrol listesi çıkarmaktadır[789]. Özellikle Kruslin kararında belirlenen eksiklikler, Ülkemizde iletişimin denetlenmesi hususunda bir yol haritası olarak görev yapmıştır. CMK 135 vd. maddeler, anılan kontrol listesi ışığında tanzim edilmiş olan Fransız Ceza Usul Kanunu'nun 100. maddesi kıstas alınarak hazırlanmıştır[790].

2.2.3.2.2.1.Erişilebilme

Özel hayatla ilgili olarak yapılan müdahalenin meşru sınırlar kapsamında kalıp kalmadığının tespiti bakımından söz konusu müdahaleyi mümkün kılan kanunun ilgili kişiler bakımından erişilebilir, başka bir ifadeyle ulaşılabilir olması gerekmektedir[791].

Erişilebilirlik ile ilgili prensipler Khan-Birleşik Krallık davasında ortaya konulmuştur. Başvuruya konu olayın gerçekleştiği dönemde, Birleşik Krallık'ta gizli dinleme cihazlarının kullanımını düzenleyen yasal bir sistem bulunmadığı için, bu cihazların kullanımı İçişleri Bakanlığı tarafından çıkarılmış rehber kuralları tarafından düzenlenmekteydi ve kurallara halkın ulaşması mümkün değildi. AİHM, bu nedeni gerekçe göstermek suretiyle söz konusu kuralların bağlayıcılığının da olamayacağını belirtmiş ve yapılan müdahalenin Sözleşmenin ihlali anlamına geldiğine karar vermiştir[792].

---

telefonların dinlenmesi konusunda sözleşmenin 8. maddesi hükümlerine uymamaktadır. (KUNHE, s. 105.).

[788] ERGEÇ, s. 162.

[789] MOWBRAY, s. 394.

[790] 5271 sayılı kanun gerekçesi, http://www.tbmm. gov.tr/develop/ owa/kanun_tasarisi _sd.onerge_ bilgileri?kanunlar_sira _no=23594

[791] ALCARAZ, s. 229; ERGEÇ, s. 161; ŞEN, (İletişimin Denetlenmesi Tedbiri), s.99; ÇOKSEZEN.s.5; '… the law must be adequately accessible: the citizen must be able to have an indication that is adequate in the circumstances of the legal rules applicable to a given case…(SUNDAY TIMES-BİRLEŞİK KRALLIK, Pr.49).

[792] KILKELLY, s. 26.

2.2.3.2.2.2.Öngörülebilme

AİHM, milli hukukun ilgiliye öngörülebilirlik (foreseebility) imkanı tanıması gerektiğini ifade etmektedir[793]. Bu kriter, kolluk kuvvetlerinin ne zaman iletişime müdahale edebileceği hususunun ilgili tarafından bilinmesi değildir. Böyle bir imkanın ilgilinin eline verilmesi, kişinin davranışlarını bu doğrultuda önceden ayarlaması gibi bir sonuç doğurur ki, bu, suçla mücadele bakımından olumsuz sonuçlara neden olur ve hayata geçirilmesi istenen tedbiri baştan hükümsüz bir hale getirir[794]. AİHM'nin amacı, insan hakları ihlallerine neden olabilecek keyfiyetteki müphem ifadelerin ortadan kaldırılmasını sağlamaktır. Bu bağlamda, kanun muhtemel şartları açıklamalı[795] ve gizli hedefler içermemelidir[796]. Başka bir ifadeyle kanun, kanun koyucunun amaçladığından farklı hedeflere kapalı olmalı, o hukuka tabi olanlar kendi haklarının ve sorumluluklarının sınırlarını bilmelidir[797].

Öngörülebilirlik ilkesine, tahmin edilebilirlik de denilmektedir[798] 'Foreseebility/previsibilité' kavramını karşılamak bakımından, tahmin edilebilirlik yerine öngörülebilirlik kelimesinin kullanılmasının daha yerinde olduğunu düşünmekteyiz. Nitekim, Türk Dil Kurumu sözlüğünde tahmin etmek; 'yaklaşık olarak değerlendirmek, oranlamak' olarak ifade edilmekteyken, öngörmek ise 'ileride olması gerekeni göstermek, önceden kararlaştırmak, ilerisi için düşünmek, göz önünde tutmak, derpiş etmek' olarak tanımlanmıştır. Bu bağlamda, öngörülebilirlik kelimesi daha doğrudur[799].

Mahkemeye göre, mutlak anlamda öngörülebilirliğin sağlanması gerekli değildir. Öte yandan, tecrübeler de bunun ulaşılamayan bir hedef olduğunu göstermiştir. Kanunlarda sarahat çok arzu edilen bir özellik olmasına rağmen, bu durum beraberinde aşırı sertlik de getirebilecektir. Halbuki kanunlar değişen şartlara ayak uydurabilecek formatta

---

[793] ALCARAZ, s. 229; ŞEN, (İletişimin Denetlenmesi Tedbiri), s.99.

[794] AİHM, Leander kararında, İsveç polisinin, milli güvenliğin korunması ile ilgili faaliyetlerinde kendisi bakımından ne tür kontroller yapabileceğini öngörme ve bilme hakkının ilgiliye verilmesinin mümkün olmadığına karar vermiştir. '…it cannot mean that an individual should be enabled to foresee precisely what checks will be made in his regard by the Swedish special police…' (LEANDER-İSVEÇ, Pr. 51).

[795] AKDENİZ, s. 13; KAYA. S. 92.

[796] YARDIMCI: 2005, s.15.

[797] YARDIMCI: 2005, s.15.; ALTIPARMAK, s. 39.

[798] ÇOKSEZEN, s. 5.

[799] Türk Dil Kurumu Sözlüğü, http://www.tdk.org.tr/TR/SozBul (İET:10.12.2007)518CA.

olmalıdır. Bu nedenle, hemen tüm kanunlar bir miktar muğlaklık ve müphemiyeti ihtiva edecek şekilde hazırlanırlar ve kanunların yorumu uygulamaya bırakılır[800].

Öngörülebilir olma ile kastedilen, uygulanan tedbirin mutlaka ilgilisine haber verilmesini sağlamak değildir. Bu bağlamda, önleme amaçlı iletişimin dinlenmesine ilişkin öngörülebilirlik, bu işlemin ilgilisine haber verilmesi zorunluluğu anlamına gelmemektedir. Bununla birlikte, yasal düzenlemenin, belirli şartların meydana gelmesi halinde, bu müdahalenin gerçekleştirilebileceği konusunda fikir vermesi gerektiği belirtilmektedir[801]. Öngörülebilirlik kriterinin yerine getirilip getirilmediğini tespit edebilmek bakımından, teknik anlamda kanun sayılmayan genelge (instructions) ve idari uygulamalar(administrative practices) da değerlendirmeye alınabilir. Böylece, ilgililerin bu metinlerin içeriği hakkında yeterli bilgiye sahip olmaları sağlanmalıdır. Kanun uygulamasının birtakım gizli tedbirleri kapsadığı ve bu tedbirlerin bireylerin ve kamunun incelemesine açılmadığı hallerde, kanun metni yetkililere verilen takdir hakkının kapsamını açık bir şekilde (with sufficient clarity) belirtmelidir[802]. Mahkeme, aynı yaklaşımı Malone davasında da göstermiş, kişilerin iletişimlerinin gizli bir şekilde izlenmesinin denetime açık olamaması nedeniyle, idareye verilecek yetkinin sınırsız (unfettered power) bir formatta olmaması gerektiği özellikle vurgulanmıştır. Bu bağlamda kanun, idareye verilen takdir yetkisini yeterli bir açıklıkla ifade etmelidir[803].

Kanunların kendilerine özgü bir dili ve terminolojisinin bulunduğu dikkate alındığında, toplumda yaşayan herkesin, kanunları gerektiği gibi anlamasının mümkün olmadığı açıktır. Bireyin anlamadığı bir kanunun varlığı halinde ise, öngörülebilme şartının yerine getirilmesi bakımından, bireylerin tavsiyeler alması bir çözümdür. Uygun tavsiyeler aldıktan sonra bireyler, mevcut şartlar altında belirli bir hareketin ne tür sonuçlar doğurabileceğini makul bir düzeyde öngörebilir duruma gelirler[804].

---

[800] SUNDAY TIMES-BİRLEŞİK KRALLIK, Pr. 49.

[801] ALTIPARMAK, s. 38.

[802] LEANDER-İSVEÇ.Pr.51; Malone kararına göre kanun; kanuna eşlik eden idari uygulamalardan farklı olarak Sözleşme ile korunan haklara yetkililerin hangi hallerde ve hangi şartlar tahtında müdahale edecekleri hususunu ihtiva etmelidir. Kanunun sarahatı ve vuzuhuna ilişkin seviye(the degree of precision) her olayın özel durumuna göre değişecektir. (MALONE-BİRLEŞİK KRALLIK, Pr.68).

[803] MALONE-BİRLEŞİK KRALLIK, Pr.68.

[804] KILKELLY, s. 26; ÇOKSEZEN, s. 5.

2.2.3.2.2.3.Açıklık

Açıklık ilkesi ile kastedilen, yasal düzenlemede, müdahale şartlarının açık ve net olarak belirtilmesi, öte yandan keyfiliğin ortadan kaldırılmasına matuf hükümlere yer verilmesi zorunluluğudur[805]. Bu itibarla, hangi tür kanun ihlallerinin devletin müdahalesine neden olacağı kanunda belirtilmeli[806], muhtemel müdahalelerin niteliği, kapsamı, süresi, bu tedbirlerin emredilmesi için gerekli sebepler[807], emri vermeye yetkili merci, uygulayan ve denetleyen birimler, izlenecek usul[808], uluslararası ve iç hukuk alanındaki başvuru yolları gibi hususlar da kanunda ayrıntılı olarak düzenlenmelidir[809].

Yasal hükmün yeterince açık olması zorunluluğu, devletlere tanınan takdir yetkisi bakımından da önemlidir. Gerçekten de, açıkça belirtilmeyen hususlarda görevlilerin keyfi uygulamalara başvurmaları ve Sözleşme haklarını, Sözleşmenin belirlediği sınırlar ötesinde kısıtlamaları mümkündür. Bu bağlamda, görevlilere tanınan bu yetkilerin yazılı veya yazısız olarak yeterince açık bir biçimde belirtilmesi gerekmektedir. Mahkeme, bu yetkinin kapsamının ve nasıl kullanılması gerektiğinin açıkça (with sufficient clarity) belirtilmediğini vurgulayarak İspanyol kanununu eleştirmiştir[810]. Kanun hükmünün açık olması aynı zamanda öngörülebilirliği de beraberinde getirmektedir. Böylece, ilgili kişi eylemin kendisini hangi sonuca görürebileceğini böylece öngörebilmiş olmaktadır[811]. Benzer bir karar da ülkemiz aleyhine verilmiştir. Ağaoğlu-Türkiye davasında, AİHM, uyuşturucu kaçakçılığı suçundan yargılanan sanığın, iletişiminin kaydedilerek mahkemede delil olarak kullanılmış olduğunu, bu denetleme kararının, 1412 sayılı CMUK'un 91 ve 92. maddelerinde yer alan düzenlemelere dayanılarak verildiğini, anılan kanunun 91 ve 92. maddelerde yer alan düzenlemenin iletişimin denetlenmesi

---

[805] KAYA, s. 92; TEZCAN/ERDEM/SANCAKTAR, s. 238; KILKELLY, s. 25.; RENUCCI, 135.

[806] ERGEÇ, s. 161.

[807] RENUCCI, s.136.

[808] ÇOKSEZEN, s. 5.

[809] ERGEÇ, s. 205; ROTARU-ROMANYA, Pr.57.

[810] Valenzuela Contreras-İspanya, (58/1997/842/1048), 30 July 1998, Pr. 61. '…Spanish law, both written and unwritten, did not indicate with sufficient clarity at the material time the extent of the authorities' discretion in the domain concerned or the way in which it should be exercised.'

[811] ERGEÇ, s. 162; Fransız kanunu da, Kruslin kararında, tedbire konu olacak yere ve suça ilişkin bilgiler ayrıca suçun işlendiğini veya işlenmekte olduğunu gösterecek bilgiler, tedbirin süresine ve bildirime ilişkin hususlar vb. düzenlemediği gerekçesiyle eleştirilmiştir. Bu eksiklikler, bu karar sonrasında Fransız Ceza Usul Kanunu'nda (madde 100) yapılan değişikliklerle giderilmiştir. SUDRE, s. 210.

yetkisini vermediğini, bu nedenle kanunun açıklığı ve öngörülebilirliği ilkeleri bakımından AİHS standartlarında olmadığını belirtmiştir[812].

Kanunun açıklığı sorunu Halford-Birleşik Krallık davasında da incelenmiştir[813]. Kendisine iki telefon tahsis edilen ve bunlardan biri özel kullanımına bırakılan Halford'a, bu telefonlarla ilgili hiçbir sınırlama getirilmemiş ve bu konuda herhangi bir rehberlik bilgisi de verilmemişti. O zamanki Birleşik Krallık kanunlarına göre, bir kamu iletişim aracı ile yapılan görüşmesine müdahale etmek suç sayılmasına rağmen, kamu iletişim araçları dışında yapılan görüşmelere (telecommunications system outside the public network) ilişkin herhangi bir sınırlama bulunmaması AİHM tarafından 8. maddenin ihlali sayılmıştır[814]. Bu karar, keyfiliğe ve kanunların açık olmamasına karşı AİHM'nin tavrını sergilemesi bakımından önemlidir. Mahkeme, yükümlülüklerini yerine getirmeleri bakımından devletlerin gerekli tedbirleri almasına izin vermesine rağmen, müdahalenin açık hükümler içeren bir kanunla yapılması şartını da sıkı bir şekilde uygulamaktadır[815]. Farklı bir tutumun, devletleri Drakon kanunları benzeri birtakım uygulamalara sürükleyeceği muhakkaktır[816]. Bu bağlamda, müdahale sadece sanık ya da şüpheli hakkında uygulanmalı, genel nitelikli sınırlamaya izin veren, müphem ve muğlak yasal düzenleme ve uygulamalardan kaçınılmalıdır[817].

Yasal hükmün açıklığı, ilke olarak dayanağını hukuk devleti, yönetimin kanuniliği, hukuki korunma garantisi ve güçler ayrılığı ilkelerinden almaktadır[818]. Bu çerçevede,

---

[812] DİNÇ, s. 429.

[813] HALFORD-BİRLEŞİK KRALLIK. Bu başvuru, 1983 tarihinde Birleşik Krallık'taki en yüksek rütbeli polis şefi olan Bayan Halford tarafınan AİHM önüne getirilmiştir.

[814] OVEY/WHITE, s. 202-203.

[815] AİHM, bu sıkı tavrını Fransa karşısında net bir şekilde göstermiştir. Huvig ve Kruslin davalarında, anılan ülkeyi 8. maddeyi ihlal ettiği gerekçesiyle mahkum eden Mahkeme, daha sonraki Lambert başvurusunda da yeni bir ihlali tespit etmiştir. Fransa'nın Huvig ve Kruslin davaları sonrasında yaptığı yasal değişiklikleri memnuniyetle karşılayan AİHM, Lambert davasında telefonu dinlenen kişi için yeterli teminatlar içermekle birlikte, söz konusu hatta konuşma yapan üçüncü taraflar için yeterli teminatlar bulunmamasını ihlal nedeni saymaktadır.(SUDRE/MARGUENAUD/ANDRIANTSIMBAZOVINA/GOUTTENOIRE/LEVINET s.335) Söz konusu telefon dinlenmesi ve birkaç görüşmenin kaydı sonrasında telefon hattının sahibini arayan ve hakkında izin alınmamış olan başvurucu çalıntı malların kullanılmasıyla itham edilmiştir. İletişiminin usulune uygun olmadan denetlenmesi nedeniyle elde edilen bilgilerin delil niteliğini taşımadığını iddia eden başvurucunun temyiz başvurusunun reddedilmesiyle, başvuru Mahkeme önüne getirilmiştir. Bk. LAMBERT-FRANSA kararı.

[816] YARDIMCI, s. 15.

[817] RENUCCI, s. 135-136.; Taylor-Sabori davasında da, bir klon (clon) kullanmak suretiyle başvurucunun mesajlarını denetleyen polisin bu eylemi, Birleşik Krallığın mahkumiyetine neden olmuştur. Mahkeme, kolluk görevlilerinin hangi hallerde bu tür yöntemlere başvuracağının belli olmaması, başka bir anlatımla açıklıkla ifade edilmemiş olmasının Sözleşmenin ihlali anlamına geleceğine hükmetmiştir. Mahkeme ayrıca, ilgili kanunun 'hukukun üstünlüğü' ilkesine uygun olması gerektiğini vurgulamaktadır. (TAYLOR SABORI-BİRLEŞİK KRALLIK, 22.10.2002, 47114/99, Pr. 18,19).

[818] ERDEM, Gizli Soruşturma, s. 227.

iletişim hakkındaki denetleme tedbiri hayata geçirilirken, resmi makamların kullanacakları yetkilerin kapsamı, hangi tedbirleri uygulamaya yetkili oldukları, yetkinin kullanım koşulları açıkça belirlenmiş olmalıdır[819]. Teknolojinin hızlı gelişimi karşısında, müdahale şartlarının açık ve ayrıntılı hükümlere bağlanması gereği[820] AİHM tarafından kabul görmüştür. Gerçekten de Kruslin ve Huvig davalarında AİHM, iletişimin denetlenmesi alanındaki hızlı teknolojik gelişmelere atıf yaparak, kanunların, bu gelişmeleri de kuşatacak şekilde açık ve detaylı kurallar içermesi gerektiğini belirtmiştir[821].

2.2.3.3. Müdahalenin Meşru Bir Amaç Gütmesi

8. maddenin ikinci paragrafında, müdahaleyi meşru kılan yasal hedefler belirlenmiş ve yapılan müdahalenin, yani Sözleşmenin 8. maddesinin ikinci fıkrası kapsamındaki sınırlamaların, meşru amaçlar için yapılması gerektiği vurgulanmıştır[822]. Meşru amaçlar ise 2. fıkrada sayılmıştır. Buna göre meşru amaçlar; ulusal güvenlik, kamu emniyeti, ülkenin ekonomik refahı, dirlik ve düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın korunması ve başkalarının hak ve hürriyetlerin korunması nedenlerinden biri ya da bir kaçı olabilir[823].

Demokratik devletler, kendilerini terörizmin bir hayli gelişmiş türlerinin ve diğer problemlerin tehdidi altında gördüklerinden dolayı, bu tür tehditlerle başa çıkmak amacıyla iletişimin denetlenmesi yoluna başvurmaktadırlar[824]. AİHM de, yasal bir hedef gütmek şartıyla bu tür denetime izin vermektedir[825]. Müdahalenin meşru amaç gütmesi şartı Mahkeme tarafından genellikle daha kolay kabul edilmektedir[826]. Devletin uygun bir amaca yönelik hareket etmiş olduğu kabul edilerek, devletçe belirtilen meşru amaç veya amaçlar neredeyse hiç reddedilmemektedir[827]. Bu kavramların içerikleri itibariyle

---

[819] KÜNHE, s. 102; AKDENIZ, s. 13.

[820] TEZCAN/ERDEM/SANCAKTAR, s. 239; KÜNHE, s. 103.

[821] KILKELLY, s. 28.; ÇOKSEZEN, s. 11.

[822] ŞEN, (İletişimin Denetlenmesi Tedbiri), s.99.

[823] ERGEÇ, s. 162.

[824] OVEY/WHITE, 204-205.

[825] KLASS-ALMANYA, Pr. 48.

[826] KILKELLY, s. 31. ; DUTERTRE, 2003:290

[827] KILKELLY, s. 31.

belirsizlik arz ettiği, bu nedenle, suiistimallere neden olabileceği muhakkak olmakla birlikte, bu sınırlamaların dar bir şekilde yorumlandığı söylenebilir[828].

Şimdiye kadar verilen kararların incelenmesiyle, iletişimin denetlenmesine ilişkin değişik yöntemlerin, AİHM tarafından, kamu yetkililerinin uyuşturucu kaçakçılığı gibi modern suç türlerine karşı mücadelede etkin bir yol kabul edildiği görülmektedir. Mahkeme, özellikle organize suçların vahameti karşısında haberleşme özgürlüğüne müdahalenin haklı ve meşru kabul edilebileceğini belirtmektedir[829]. Bu bağlamda AİHM, Lambert davasında, müdahaleye cezai soruşturma ile ilgili delillerin ortaya çıkarılması amacıyla başvurulduğunu ifade ederek, bu tedbirleri kamu düzeninin sağlanması amacına uygun yöntemler olarak yorumlamıştır[830]. 8. maddenin ikinci paragrafında sayılan diğer haller de, Mahkemenin değişik kararlarında atıflara konu olmuş ve Mahkeme, genellikle bu haller gerekçe gösterilerek başvurulan tedbirlerin meşru bir amaca hizmet ettiğine karar vermiştir.

2.2.3.4. İletişime Müdahalenin Demokratik Bir Toplumda Gerekli Olması

Müdahale demokratik bir toplumda gerekli midir? Ya da diğer bir ifadeyle, haberleşmenin kontrol edilmesi zorunlu mudur? soruları AİHS'nin sözleşme haklarına ilişkin sınırlamaların tespiti ve bu sınırlamaların varacağı hudutların belirlenmesi açısından önem taşımaktadır[831]. Demokratik bir toplumda zorunlu olma şartı, bir Sözleşme hakkına yapılacak müdahalenin meşru ve makul olduğunu ispat bakımından önemlidir. Bu şart, keyfiliğe ve kamu görevlilerinin aşırı güç kullanmalarına karşı bireylere bir koruma sağlamaktadır[832].

AİHM, 'demokratik bir toplum' kavramını tartışmak, bu kavrama ilişkin bir detay vermek şeklinde bir tercihte bulunmamıştır. Mahkemenin, çoğulculuk, tolerans, geniş fikirlilik (broadmindedness), eşitlik, hürriyet kavramlarını demokratik bir toplumun nitelikleri olarak tanımladığı açıktır[833]. Mahkeme, demokratik bir toplum kavramını tartışmaktan

---

[828] ERGEÇ, s. 162-163.

[829] OVEY/WHITE, s. 205.; TEZCAN/ERDEM/SANCAKDAR, s. 237; Bk. PRADA BUGALLO-İSPANYA

[830] LAMBERT-FRANSA, Pr. 29.

[831] DUTERTRE, s, 290; ŞEN, (İletişimin Denetlenmesi Tedbiri), s.99.

[832] United Kingdom Parliament, Joint Committee on Human Rights First Report, http://www.publications.parliament.uk/pa/jt200001/jtselect/jtrights/69/6917.htm#n123 ,(İET:19.12.2007).

[833] OVEY/WHITE, 210; Mahkeme Handyside kararında 'pluralism(çoğulculuk), tolerance(tolerans) and broadmindedness(geniş fikirlilik)' kavramlarını demokrasinin olmazsa olmaz şartlarından biri olarak tanımlamıştır. Mahkemeye göre, bu alanda empoze edilen her formalite (formality), her şart (condition), her

imtina etmiş olmakla birlikte, gerekli anlamına gelen 'necessary' sıfatının anlamını ve kapsamını ortaya koyabilmek için bir değerlendirme yapmıştır. Mahkemeye göre, 'necessary' sıfatı, mutlak anlamda gerekli, zaruri, zorunlu anlamına gelen 'indispensable' sıfatı ile eş anlamlı değildir. Bununla birlikte, 'admissible' (kabul edilebilir), 'ordinary' (sıradan, alalade) 'reasonable' (makul) ya da' desirable' (arzu edilir, cazip) sıfatlarının taşıdığı esnekliği de taşımadığı muhakkaktır. Bu bağlamda, 'gereklilik' (necessity) ifadesinin işaret ettiği acil sosyal ihtiyacın (pressing social need) belirlenmesi taraf devletlere bırakılmıştır[834].

Demokratik toplumda gerekli olma ifadesinde iki önemli unsur bulunmaktadır. Bunlardan ilki, acil bir sosyal ihtiyacı karşılama zorunluluğudur. Diğer unsur ise, uygulanacak tedbirin elde edilmek istenen yasal hedefle orantılı olmasıdır[835]. AİHM, bu yetkinin kullanılmasında devletlere bir takdir hakkı tanımış olmakla birlikte, bu takdir hakkının makul bir şekilde kullanılıp kullanılmadığı hususunda devletler üzerinde bir denetleme görevi üstlenmiştir. Bu kapsamda, sözleşmeci taraf hem kanunu hem de uygulaması itibariyle, AİHM denetimine tabidir[836]. Mahkeme, bu denetimi gerçekleştirirken 'hukukun üstünlüğü' gibi ilkeleri mihenk taşı olarak kabul eder. Devletin yürütme organlarının, bireylerin haklarına ilişkin olarak yaptıkları müdahaleler etkin bir denetime tabi kılınmalıdır[837]. Bu bağlamda, uygulanan tedbirin demokratik bir toplumda gerekli olduğunu ispatlama zorunluluğu, özellikle çok kişi tarafından işlenen suçlar ya da organize suçlar bakımından bu tedbirin gerekli olduğunu iddia eden devlete aittir[838].

Mahkeme, başvuru konusu olayı bütün olarak değerlendirmekte, müdahalenin elde edilmek istenen yasal amaçla orantılılılığı, yetkili makamlarca öne sürülen müdahale nedenlerinin yeterli olup olmadığı ve olayla ilgili olup olmadığı hususlarına bakarak değerlendirme yapmaktadır[839]. Çoğunlukla devletin menfaati ile kişinin özel hayatı

---

sınırlama (restriction) ya da ceza (penalty) elde edilmek istenen amaçla orantılı olmalıdır.(HANDYSIDE-BİRLEŞİK KRALLIK, Pr. 48-49.)

[834] HANDYSIDE-BİRLEŞİK KRALLIK, Pr. 48-49.

[835] HANDYSIDE-BİRLEŞİK KRALLIK, Pr. 48-49.

[836] LAMBERT- FRANSA, Pr. 30.

[837] KRUSLIN-FRANSA, Pr. 55; 8. maddenin ikinci paragrafında belirlenen sınırların aşılmaması bakımından, demokratik bir toplumun değerleri denetim süreci çerçevesinde sıkı bir şekilde takip edilmelidir.

[838] LAMBERT –FRANSA, , Pr. 33.

[839] Hertel v. Switzerland, (59/1997/843/1049) 25 August 1998, 46(iii); '…what the Court has to do is to look at the interference complained of in the light of the case as a whole and determine whether it was

arasındaki dengeyi sağlamak misyonu olarak ortaya çıkan bu zor oyun, bazen de iki sözleşme hakkının birbiriyle yarıştığı halde karşımıza çıkmaktadır ki, bu hal, oyunun en karmaşık aşamasıdır. İfade özgürlüğü ile özel hayat hakkı çatıştığında, ifade özgürlüğü ile din özgürlüğü çatıştığında hangisine üstünlük tanınacağı sorunu bu karmaşık oyuna bir örnek olarak gösterilebilir [840].

AİHM, demokratik toplumların karmaşık suçların tehdidi altında olduklarını, bunun sonucu olarak da devletlerin bu tür tehditlere etkin biçimde karşı çıkabilmek için kendi yetki alanı içinde hareket eden yıkıcı unsurlara karşı gizli izleme yöntemleri uygulamak zorunda olduklarını kabul etmektedir. Bu bağlamda, posta ve telekomünikasyon konularında gizli gözetim yapma yetkisi veren bazı kanunların olmasını, bu kanunlar çerçevesinde istisnai durumlarda milli güvenliği ya da kamu düzenini korumak veya suç işlenmesini önlemek için bazı tedbirlere başvurulmasını makul görmektedir[841]. Mahkeme, suçun önlenmesini hedefleyen kurumların demokratik bir toplumda meşru olarak var olabileceğini kabul etmekle beraber, vatandaşların gizli gözetimi konusundaki yetkinin sadece demokratik kurumları korumak için mutlaka gerekli olduğu durumlarda sözleşme kapsamında kabul edilebileceğini açıkça belirtmiştir[842]. Bu gereklilik kavramı, müdahalenin acil bir toplumsal ihtiyacı karşıladığını ve özellikle de elde edilmek istenen meşru amaçla orantılı olduğunu ifade eder. Demokratik bir toplumda gerekli olma kriteri belirlenirken devletin takdir yetkisi dikkate alınmalıdır. Nitekim, devletler, ülkelerindeki önemli güçlerle doğrudan ve sürekli ilişki halinde olmaları nedeniyle ulusal düzeydeki hassas veya karmaşık konuları daha yakından değerlendirebilirler ve uluslararası hâkimlere kıyasla bir hakkın sınırlandırılması veya bir cezanın uygulanmasının gerekliliği konusunda daha iyi karar verebilecek durumdadırlar. Bu bağlamda gereklilik kavramında ifade edilen acil toplumsal ihtiyacın gerçeklik düzeyi konusunda ilk değerlendirmeyi ulusal yetkililer yapmalıdır. Bununla birlikte, devletlere verilen bu takdirin sınırsız olmadığı da muhakkaktır[843].

---

proportionate to the legitimate aim pursued and whether the reasons adduced by the national authorities to justify it are relevant and sufficient'

[840] ERGEÇ, s.163. Mahkemenin haklar arasında tercih yapmak durumunda kaldığı başvurular arasında en meşhurlardan birisi Jersild-Danimarka davasıdır.

[841] KILKELLY, s. 50.

[842] KILKELLY, s. 49.

[843] KILKELLY, s. 5.

2.2.3.5. İletişime Müdahalenin Orantılı Olması

Hukuk devleti ilkesine saygılı bir devlet, suçları önleme ve aydınlatma görevinin yanı sıra, bireylerin temel hak ve hürriyetlerine saygı gösterme ve onları koruma görevini de üstlenmiştir. Bu görevlerin ihmal edilmesi hukuki ve sosyal barışı bozabilir[844]. Devletin bu görevlerini yerine getirirken birtakım sınırlamalar yapma yetkisi de gündeme geleceğinden, bu yetki sınırsız kılınmamıştır. Takdir yetkisinin sınırlandırılmasında[845] orantılılık ilkesi önemli rol oynamaktadır[846]. Orantılılık ilkesi bazı yazarlar tarafından ölçülülük ilkesi olarak adlandırılmaktadır. AİHM kararlarında kullanılan 'proportionate to the aim pursued'[847] ifadesindeki 'proportionate' kelimesinin orantılılık olarak ifade edilmesinin daha uygun olacağını düşünmekteyiz.

Eşitlik ilkesi, keyfilik yasağı, hukuk devleti ilkesi gibi kavramlar orantılılık ilkesinin hukuki temelini açıklamak için ortaya atılan temel hukuk ilkeleri arasında yer almaktadır[848]. İnsan haklarının mutlak olmadığını, hakların kullanılmasının her zaman genel kamu yararı ile dengelenmesi gerektiğini belirleyen, ayrıca kendisi bizatihi söz konusu dengenin sağlanması araçlarından olan[849] orantılılık ilkesi, sözleşme haklarına müdahale etme öncesinde gerekli değerlendirmeyi yapma sorumluluğu ve zorunluluğunu karar sürecine katılan yetkililere yükler. Böylece, müdahalenin şiddeti ile bu tedbiri gerektiren acil sosyal ihtiyaç arasında bir denge kurulmuş olacaktır[850]. Bu ilke marifetiyle, temel hakların somut olarak sınırlandırılması belli rasyonel prensiplere bağlanmakta ve hukuk devletinin özünü oluşturan hukuka bağlılık ve güven duygusu güçlendirilmektedir. Bu ilke ayrıca, devlete karşı temel hak ve hürriyetler kavramının somutlaşmasına hizmet etmektedir[851].

Hukukun genel ilkelerinden biri olarak kabul edilen orantılılık ilkesi, milli hukukta öngörülen sınırlama ile elde edilmek istenen amaç arasında bir orantının olmasını

---

[844] ERDEM, Gizli Soruşturma, s. 223.

[845] MARGUENAUD, s. 53.

[846] ŞEN, (İletişimin Denetlenmesi Tedbiri), s.99.

[847] Bk. HERTEL-İSVİÇRE, 25.8.1998, (59/1997/843/1049), Pr. 46(iii).

[848] SAĞLAM, s. 117-118.

[849]KILKELLY, s. 32.

[850] KILKELLY, s. 33.

[851] SAĞLAM, s.118.

aramaktadır[852]. Başka bir ifadeyle, orantılılık ilkesi, kamu yararının oluşturduğu talepler ile bireyin temel haklarının korunması gereği arasında adil bir denge oluşturma çabasıdır[853]. Bu husus Klass kararında, 8. maddenin 1. fıkrasındaki hakkın birey tarafından kullanılması ile, anılan maddenin ikinci fıkrası uyarınca demokratik toplumun korunması amacıyla iletişimin denetlenmesi tedbirinin uygulanmasına olan ihtiyaç arasında denge olarak ifade edilmiştir[854].

Orantılılık ilkesi ve bu ifadenin altında yer alan gereklilik, elverişlilik ve ölçülülük ilkeleri sınırlamanın amacı ile bu amacı gerçekleştirmek üzere kullanılan araçlar arasındaki ilişki temelinde birleşmektedir. Burada kullanılan araç, Anayasal güvence altındaki temel hakkın sağladığı bireysel hukuki statünün sınırlanış biçimini ifade etmektedir[855].

Orantılılık ilkesinin uygulanmasında, seçenekler daraltılmalı, başvurulan tedbir yasal amacın elde edilebilmesi bakımından tek tedbir (le seul moyen apte à atteindre) olmalıdır. Bunun yanı sıra, bu tedbirin başvurulabilecek olanlar arasında en az kısıtlayıcı olmasına dikkat edilmelidir[856]. Bu bağlamda, ikinci derecede uygulanabilirlik olarak da ifade edilebilecek olan orantılılık, haberleşme özgürlüğüne ağır müdahale oluşturan iletişimin denetlenmesi tedbiri bakımından bir süzgeç niteliği görmektedir. Bu derecelendirme ile, aynı amaca hizmet eden iki tedbir arasında öncelik-sonralık ilişkisi gözetilir ve bu süreç, aynı suçu aydınlatmak üzere başvurulabilecek birden fazla tedbir arasında karşılaştırma yapılmasını ve bunlardan en ılımlısının ya da en az zarar verecek olanın[857] seçilmesini gerektirir[858].

---

[852] DÜLGER, Murat Volkan, "Avrupa İnsan Hakları Mahkemesi Kararlarında Organize Suçla Mücadelede Özel Koruma Tedbirleri", (http//www.hukukcu.com/bilimsel/kitaplar /aihmd_organizesuc.htm). (İET:15.09.2007), s. 6.; YILDIRIM, s. 389.;

[853] KILKELLY, s. 33.

[854] KLASS-ALMANYAKararı, Pr. 59. Benzer bir yaklaşım AİHS'nin başlangıç kısmında vurgulanmıştır. Başlangıç kısmında, insan hakları ile temel hürriyetlerin korunması ve geliştirilmesinin, bir yandan demokratik bir siyasal rejime, diğer yandan da insan hakları konusunda ortak bir anlayış ve ortaklaşa saygı esasına bağlı olan bu temel hürriyetlerle sağlanacağı belirtilmiştir.

[855] SAĞLAM, Fazıl, Temel Hakların Sınırlanması ve Özü, Ankara Üniversitesi Siyasal Bilgiler Fakültesi Yayınları, 1982, s.112-113.

856 ERGEÇ, s. 163.

857 KAYA, s. 93.

858 ERDEM, 5271 Sayılı Ceza Muhakemesi Kanunu'nda İletişimin Denetlenmesi, s. 100.; Amerikan hukukunda, son çare prensibinin açıklandığı 18 & U.S.C. 2518(3) nolu maddeye göre, iletişimin denetlenmesine başvurulabilmesi için, bu tedbir dışındaki soruşturma yöntemlerinin kullanılmış olması ancak bu yöntemlerin başarısızlıkla sonuçlanması gerekmektedir. İletişimin denetlenmesi dışındaki yöntemlerin kullanılması durumunda başarı elde edilemeyeceğine ilişkin bir kanaat olması ya da bu tedbir dışındaki yöntemlerin kullanılmasının çok tehlikeli olması da bu tedbirin kullanılmasını mazur hale getirir.

Müdahalenin üstün bir sosyal ihtiyaca cevap vermesini ve izlenen meşru amaçla orantılı kalmasını şart koşan[859] AİHM'nin orantılılık ilkesini ilk defa kullanması 23.07.1992 tarihli Belçika Linguistic davasıyla olmuştur. Bu kavram, 23.09.1982 tarihli Sporrong/Lönnroth-İsveç kararlarıyla "genel çıkar ve bireyin çıkarları arasında adil bir denge"nin kurulması[860] olarak tanımlanmıştır. AİHM'ye göre, böyle bir dengenin gözetilmesi AİHS'nin doğasından kaynaklanmaktadır (inherent in the whole of the Convention). AİHM içtihatları ile kabul görmüş durumda olan bu ilke ile, Sözleşme ile korunan haklara müdahale konusunda devletlere verilen takdir hakları denetlenebilmektedir[861].

Orantılılık ilkesi, Handyside[862] ve Olsson gibi AİHM kararlarında bağımsız bir şart olarak tanımlanmamış, demokratik toplum düzeninin gereğinin sonucu olarak değerlendirilmiştir. Bu bağlamda Mahkeme, orantılılık ilkesini, "demokratik toplumda zorunluluk" ilkesinden türetmektedir[863]. Bu bağlamda, müdahale, yasal amacın yerine getirilmesi için gerekli olandan fazla olmamalıdır. Bu şart, müdahalenin kapsamı hakkında bir değerlendirme yapmayı gerektirdiği gibi, bu yasal amaca başkaca yollarla ulaşmanın mümkün olup olmadığı konusunda araştırma yapmayı da zorunlu kılmaktadır[864]. Bu bağlamda, devletin, korunmasında acil bir sosyal ihtiyaç gördüğü değere ya da kuruma yönelik gerçek bir tehdit olduğunu gösteren yeterli olgusal temel bulunmalıdır[865].

Sosyal bir yarar sağlamak amacıyla belirli bir kişi ya da grup üzerine açık bir şekilde ağır yük yükleyen tedbir orantısız bir tedbirdir. Tedbirin orantısız olarak nitelendirilebileceği bir diğer hal de, tedbirin uygulanmasını gerektiren suçun şartları

---

859 YILDIRIM, s. 389.

860 SPORRONG/LÖNNROTH-İSVEÇ, 23.9.1982, 7151/75; 7152/75, Pr. 69 '…whether a fair balance was struck between the demands of the general interest of the community and the requirements of the protection of the individual's fundamental rights'. Ayrıca Bk. BELGIAN LINGUISTIC-BELÇİKA, 23.7.1968, Pr. 5.

861 MARGUENAUD, s. 53.

862 Sözleşme ile korunan hakka getirilecek her türlü formalite (formality), şart (condition), sınırlama (restriction) ya da müeyyidenin (penalty) hedeflenen meşru amaçla orantılı olması gerekmektedir. HANDYSIDE-BİRLEŞİK KRALLIK, Pr. 49

863 METİN, s. 83.

864 United Kingdom Parliament, Joint Committee on Human Rights First Report http://www. publications. parliament.uk/pa/jt200001/jtselect/jtrights/69/6917.htm#n123

865 VEREİNİGUNG DEMOKRATİSCHER SOLDATEN ÖSTERREİCHS AND GUBİ-AVUSTURYA(1995) 20 EHRR 56. Avusturya hükümetinin disiplinin sağlanabilmesi bakımından gerekli gördüğü ve bu yüzden askerlere dağıtmadığı bir süreli yayının yasaklanması hakkında AİHM, bu yasağın orantısız olduğu gerekçesiyle ihlal kararı vermiştir. Nitekim, Mahkeme, sözkonusu süreli yayının disiplini bozduğu konusunda tatmin olamamıştır.

dikkate alındığında, aşırı sayılabilecek cezaların uygulanmasıdır. Tedbir hakkında uygulanacak yasal kontrolün etkinliği ve bu tedbirden mağdur olan kişiler hakkındaki yasal çözümlerin yeterliliği de müdahalenin orantılılığı hakkında değerlendirme yapılmasına yardım edecektir. Orantılılığa ilişkin tespit yapılırken her olay kendi bağlamında değerlendirilmeli ve şartlar değiştiğinde bu değerlendirme yenilenmelidir[866].

Yasal metinlerde doğrudan yer almasa da[867] orantılılık ilkesinin birtakım unsurlarının olduğu kabul edilmektedir[868]. Orantılılık ilkesi, temel hak ve hürriyetlere müdahale edilmesi ile izlenen amaca ulaşmak için elverişli, gerekli ve ölçülü araçlara başvurulması gerektiği anlamını taşımaktadır[869].

2.2.3.5.1.Elverişlilik

Elverişlilik ilkesi[870], uygulanan tedbirin istenen sonucun elde edilmesine uygun olması anlamına gelir. Sınırlamayı oluşturan tedbirin, hedeflenen sonuca bir katkı sağlaması olarak[871] da tanımlanan bu ilke, araçla amaç arasındaki ilişkinin değerlendirilmesi, amaçtan araca doğru bir yol bulunması ve bu yolla aracın denetlenmesidir. Başvurulan bir tedbir yardımıyla istenilen neticeye yaklaşılabiliyorsa araç elverişli, buna karşılık kullanılan araç amaca ulaşmayı zorlaştırıyor ya da amaca erişme bakımından hiçbir etki göstermiyorsa araç elverişsizdir[872]. Amaçtan yola çıkılarak aracın denetlenmesi, yani aracın amacı gerçekleştirmek için uygun olup olmadığının denetlenmesi bu süreci elinde tutan otoritenin bir takdir yetkisiyle donatılmasını gerektirir. Bu süreci denetleyen

---

[866] United Kingdom Parliament, Joint Committee on Human Rights First Report http://www.publications.parliament.uk/pa/jt200001/jtselect/jtrights/69/6917.htm#n123

[867] MARGUENAUD, s. 53.

[868] ERGEÇ, s. 163; United Kingdom Parliament, Joint Committee on Human Rights First Report http ://www.publications.parliament.uk/pa/jt200001/jtselect/jtrights/69/6917.htm#n123 ,(İET:19.12.2007);Bk .D. J. Harris, M. O'Boyle and C. Warbrick, Law of the European Convention on Human Rights (London: Butterworths, 1995), 290-301

[869] SAĞLAM, s. 114; ERDEM, Gizli Soruşturma, s. 191.

[870] Elverişlilik ilkesi Amerikan hukukundaki makul sebep(probable cause) ilkesiyle benzerlik göstermektedir. 1968 tarihli Teknik Dinleme Kanunu'nun 18 U.S.C. § 2518(3) sayılı maddesine göre, hakim, başvuruda belirtilen olgulara ilişkin bir değerlendirme yaparken iletişimi denetlenecek kişinin 18 U.S.C. § 2516 sayılı maddede belirtilen suçlardan birini işlediğini, işlemekte olduğunu veya işlemek üzere olduğunu gösteren makul sebeplerin olup olmadığını araştırır. Bunun yanısıra hakim, bu tedbir marifetiyle soruşturma konusu suçlar hakkında belli delillerin elde edileceğine ilişkin makul sebeplerin bulunup bulunmadığını da irdelemelidir. Bu bağlamda araştırılacak diğer bir husus da, son çare prensibinin tüketilip tüketilmediğini yani diğer soruşturma yöntemlerine başvurulup başvurulmadığının tespit edilmesidir. DONOHUE, s.8; DEPARTMENT OF JUSTICE:2002,Interception Authorized by a Title III Order; AN OVERVIEW OF ELECTRONIC SURVEILLANCE: History and Current Status, D.1.2,; SCHWARTZ:2007,A.1; EFF ANALYSIS OF PATRIOT ACT; DEMPSEY:1997; EHRLICH, s. 8.

[871] SAĞLAM, s.114

[872] METİN, 26.

kişinin başka türlü karar verme ya da karar vermekten imtina etme gibi bir seçeneği olmalıdır ki araç-amaç ilişkisi sağlıklı bir şekilde çalıştırılabilsin[873].

Elverişlilik denetiminde iki alanda sorun yaşanmaktadır. Bunlardan ilki, kanun koyucunun düzenleme yaparken kanunun amacını net olarak belirlememiş olması halidir. İkinci sorun da, aracın elverişlilik derecesiyle ilgilidir. Bu bağlamda amaca kısmen ulaşmayı sağlayan araçların da elverişli olduğu kabul edilmektedir[874].

Tehdit altındaki hukuki değer, bir araç yardımıyla etkili olarak korunabiliyorsa bu takdirde araç elverişlidir. Bununla birlikte, tedbire başvurulduğunda işlenen suçla ilgili delil elde edilebilmesinde veya suçların işlenmesinin önlenmesinde etkinliğin fiilen artıp artmayacağı araştırılmalıdır. Kullanılan araç, yani iletişimin denetlenmesine imkan veren tedbir, kolluk görevlilerine, başka türlü elde edemeyecekleri bilgilere ulaşma olanağı veriyorsa elverişlidir[875]. Her ne kadar bazı yazarlar, bu tür gizli soruşturma tedbirlerinin organize suçlarda elverişliliğe sahip olmadığını iddia etseler de, organize suçlarla mücadele hususunda bu tür tedbirlerin elverişliliği izahtan varestedir. Bu tür tedbirler "kör bir kılıç" benzetmesiyle karşı karşıya kalmakta, bu tedbirlerin kullanılabilmesinin çok sayıda personel, emek ve mesai gerektirdiği, elde edilen kayıtların çok az bir kısmının değerlendirilebildiği de ileri sürülmektedir. Bu tedbirlerin, ancak bilinen kişilere karşı yürütülmesi halinde başarılı olabileceği belirtilmektedir. Oysa ki bu tür suçlarla açık koruma tedbirleri ile bugünkü koşulların zorluğu altında mücadele etmek neredeyse imkansızdır. Organize suçluluğun özel yapısı, suçluların profesyonelliği ve dışa karşı geliştirilen koruma mekanizması nedeniyle geleneksel nitelikteki tedbirlerle bu tür suçların aydınlatılması mümkün değildir[876].

2.2.3.5.2.Gereklilik

Gereklilik ilkesi, sınırlamayla elde edilmek istenen amaca ulaşmak için aynı derecede elverişli birçok araç arasından temel haklara en az müdahalede bulunan ya da en

---

[873] METİN, 24-25; SAĞLAM, s. 115

[874] SAĞLAM, s.114; Alman Anayasa Mahkemesi, temel haklara sınırlama getiren kanunların amaca ulaşmak için bütünüyle elverişli olmasını aramamaktadır. Sınırlama getiren kanunun bütünüyle elverişsiz olup olmadığını araştıran mahkeme aracın yardımıyla istenilen sonuca yaklaşılabilmesi halinde aracın elverişli olduğu kanaatindedir. (METİN, s. 27)

[875] ERDEM, Gizli Soruşturma, s. 191; METİN, s. 28.; Bu bağlamda, Alman Anayasa Mahkemesi tarafından verilen bir kararda, daha başlangıçta amacı gerçekleştirmeye elverişli gözükmeyen yasal tedbirler Anayasaya uygun görülmemiştir. Örneğin bir şehirden başka bir şehre giden özel araçlara yol masraflarını paylaşacak müşterilen bulan komisyoncu merkezlerini(Mitfahrerzentrale) 'trafiğin güvenliği' ve 'birlikte seyehat eden kişinin korunması' gibi amaçlarla yasaklayan kanun hükmü Anayasaya aykırı bulunmuştur. Bk. SAĞLAM, s. 115-115

[876] ERDEM, Gizli Soruşturma, s.193

yumuşak nitelikteki araçla erişmeyi ve onu kullanmayı ifade eder. Bir çok mümkün ve elverişli araç arasından bireylere ve kamuya en az zarar verecek olan aracın seçilmesi gerekir. Hakkı daha az sınırlayan başka bir müdahale ile aynı veya daha iyi bir sonuç elde edilebilecekse, bu halde kullanılan araç gereklidir[877].

Gereklilik ifadesiyle kastedilen, aynı ölçüde veya daha ılımlı başka araçlarla aynı amaca ulaşılıp ulaşılamayacağının değerlendirilmesidir. Başka bir anlatımla, temel hak ve hürriyetlere müdahalenin gerekli kabul edilebilmesi için, izlenen amaca ulaşmada daha ılımlı başka bir aracın bulunmaması zorunluluğudur[878].

ABD hukukunda[879], "son çare" prensibi olarak adlandırılan ilke, en hafif tedbirden[880] daha ağır tedbirlere doğru aşamalı bir geçişin yapılmasını zorunlu kılar. Bir tehlikenin önlenmesi amacına matuf olmak üzere, polisin basit kuşkularının hürriyetin ciddi anlamda kısıtlanması anlamına gelen bu tedbirin ikame edilmesi için yeterli olmayacağı gerçeği de akılda tutularak, öncelikle daha hafif tedbirlerin denenmesi, doğrudan doğruya genel bir yasaklama ve ağır bir müdahale yoluna başvurulmasından

---

[877] SAĞLAM, s.115; METİN, s. 30.; DİNÇ, s. 384.

[878] METİN, s.31; İletişimin denetlenmesinin de içinde olduğu soruşturma tedbirleri, bazı yazarlar tarafından, gereklilik ilkesine uygun olmadığı gerekçesiyle kabul edilmemektedir. Bu düşünce savunucuları, temel hak ve hürriyetlere bu denli ağır müdahalenin yapılabilmesi için muhtemel tüm tedbirlerin alınması gerektiğini ifade etmektedirler. Bu bağlamda, suç öncesi araştırmanın derinleştirilmesi, sosyo-politik mücadele stratejilerinin ve uluslararası işbirliğinin geliştirilmesi, uzmanlaşma ve örgütlenmenin artırılması gibi birtakım usullerin tüketilmesi sonrasında bu tür soruşturma tedbirlerine başvurulabileceğini dile getirmekle birlikte bu tür tezler hayatın gerçekleriyle uyuşmayan düşünceler olarak değerlendirilmektedir. Ancak başlangıç şüphesinin bulunması durumunda başvurulabilecek olan bu tür tedbirler yerine suç öncesi araştırmaların ikame edilmesi kabul edilebilir bir tez değildir. Sosyo-politik mücadele stratejileri ve uluslararası işbirliğinin geliştirilmesi de doğası itibariyle zaman gerektiren ve doğası itibariyle bu tür tedbirleri tamamlayıcı bir fonksiyon eda edebilecek nitelikte çözümlerdir. Üstelik her suçun uluslararası boyut taşımadığı gerçeği de meselenin ayrı bir boyutunu teşkil etmektedir. Uzmanlaşma ve örgütlenme de son iki çözüm iddiası gibi zaman gerektiren, bizatihi sorun çözme kabiliyeti olmayan ve başka formüllerle birlikte kullanıldığında sonuca götürücü etkileri barındıran bir yol olabilir. ERDEM, Gizli Soruşturma, s. 205.

[879] İletişimin denetlenmesi tedbirinin kullanılacagı olay sayısını azaltmak ve mahremiyete yönelik riskleri minimize etmeyi amaçlayan son çare prensibi uygulanması için aranacak şartların varlığı ve bu şartların oluştuğunun göstergesi olan makul sebebin tespiti ortam ve amaca göre değişmekle birlikte, Teknik Dinleme Kanununda, makul desteğe dayanmayan kanaatlerin son çare prensibinin uygulanması için yeterli bulunmadığı vurgulanmıştır. Kolluk güçleri, bir soruşturma kapsamında elde ettikleri bilginin daha fazlasına ihtiyaç duyduklarında, bunu elde etmek için iletişimin denetlenmesine ihtiyaç duymaktadırlar. Yani aslında, başka yöntemlerle elde edilmiş bilgi ve belgelerin yeterli bulunmadığı koşullarda iletişimin denetlenmesine ihtiyaç duyulabilir.[879] 18 U.S.C. § 2518(3); DONOHUE,s .8; Overview of Electronic Surveillance: History and Current Status, D.1.2; EHRLICH,s. 8; ÖZDOĞAN, (2004), s. 35; DEMPSEY, "Communications Privacy In The Digital Age: Revitalizing The Federal Wiretap Laws To Enhance Privacy";

[880] SAĞLAM, s.115; METİN,s. 30.; ERDEM, Gizli Soruşturma, s. 205.

kaçınılması gerekmektedir[881]. Aksi takdirde, "gereklilik" ve dolayısıyla üst kavram olarak da "orantılılık ilkesi" ihlal edilmiş olur[882].

Gereklilik ilkesi denetiminde, amaca ulaşmak için hangi aracın daha elverişli olduğunun tespiti bakımından, araçların birbirleriyle mukayese edilmesi ve karşılaştırmayı yaparken bazı verilerin belirlenmesi gerekmektedir. Bu bağlamda, uygulanan tedbirin ilgililere ve kamuya dezavantajlar getirip getirmediği, başka elverişli tedbirlerin mevcut olup olmadığı ve bunların dezavantajları araştırılmalıdır. Böylece, mukayese konusu araçların dezavantajları karşılaştırılarak bireylere ve kamuya en az zarar veren aracın hangisi olduğu anlaşılabilir[883]. Bununla birlikte, bu mukayese doğası itibariyle bir varsayıma ya da bir deneme-yanılma sürecine dayalı bir karar verme zorunluluğunu içermektedir[884].

2.2.3.5.3.Ölçülülük (Dar Anlamda Orantılılık)

Aracın, ulaşılmak istenen amaç ile açık bir orantısızlık içinde olmaması, ilgililere ölçüsüz yükümlülükler getirmemesi, ilgililer için katlanılabilir olması şeklinde ifade edilen ölçülülük ilkesi[885], devlet ve bireyin çatışan menfaatleri arasında bir denge kurma çabasıdır. Çatışan bu çıkarlar arasındaki ilişkiyi, haksız bir şekilde daha az değer taşıyan bir amaç lehine yorumlamak, daha yüksek değerdeki bireyin özgürlüğüne ilişkin menfaatin feda edilmesini gerektirecek bir adım atmak bu ölçülülük ilkesinin ihlali anlamına gelecektir[886].

Gereklilik ilkesinde sabit bir amaçla araç ya da araçlar arasındaki ilişki söz konusu iken, ölçülülük ilkesinde iki değişken arasındaki karşılıklılık karşımıza çıkmaktadır[887]. Ölçülülüğün sağlanabilmesi bakımından, amaç ve araç arasındaki oranın ölçülü olması[888] ayrıca, aracın ilgililere ölçüsüz yükümlülükler getirmemesi, aracın ilgililer için katlanılabilir olması gerekmektedir[889]. Gereklilik ilkesi gibi göreceli bir ilke olan [890]

[881] METİN, s. 31.; SAĞLAM, s.115

[882] METİN, s. 31.

[883] METİN, s. 31.

[884] ERDEM, Gizli Soruşturma, s. 205.

[885] METİN, s. 36.

[886] ERDEM, Gizli Soruşturma, s. 218.

[887] SAĞLAM, s.116

[888] SAĞLAM, s.11; METİN, s. 36.

[889] METİN, s. 36.

[890] METİN, s. 37.

ölçülülük ilkesi bakımından yapılacak denetimde, daima somut olayın özellikleri dikkate alınmalı, çatışan menfaatlerin makul bir denge içinde olup olmadığı araştırılmalıdır[891]. Bu dengenin belirlenmesi, her olayın niteliğine, ağırlığına göre farklılık arz eder. Hürriyete yapılan müdahalenin yoğunluğu bu anlamda önem kazanır. Müdahale ne kadar kapsamlı ve şiddetli ise, söz konusu müdahaleyi haklı çıkartmak için ortaya konulması gereken nedenlerin de o kadar güçlü olması gerekir[892].

Hakka ilişkin olarak yapılan müdahalenin gerekenden fazla olmaması, müdahalenin amaca ulaşmak için gerekli olan ve olabildiğince asgari düzeyde tutulması gerekmektedir[893]. Böylece müdahalenin ağırlığı ile müdahaleyi meşrulaştıran nedenlerin önemi ve zorunluluğu arasında makul bir denge tesis edilmiş olur[894]. Müdahalenin ölçülülüğü, amaca ulaşmak için gerekli düzeyde müdahaleye müsamaha edilmesi hususunda benzer bir yaklaşım ABD hukukunda da mevcuttur. Müdahalenin en aza indirilmesi prensibi olarak da adlandırılan bu yaklaşımla, iletişimin denetlenmesi tedbiriyle özel hayata yapılacak müdahale riskini en aza çekmek hedeflenmektedir[895]. İlgili kanun hükmü[896] uyarınca, iletişimin dinlenmesi esnasında mahkeme kararında belirtilen sınırların dışına çıkılmaması bakımından elden gelen gayret gösterilmelidir. Nitekim, iletişimin denetlenmesi tedbiri, fiziksel aramaya kıyasla özel hayat bakımından daha ciddi riskler barındırmaktadır[897]. Doğası itibariyle gelişigüzel (inherentle indiscriminate) [898] bir tedbir olarak nitelendirilen iletişimin denetlenmesinin sağlanması amacıyla kullanılan cihazlara titizlikle ve ayırt edici koşullar altında başvurulması gerektiği Amerikan Yüksek Mahkemesi kararlarında vurgulanmıştır. Bu hususa dikkat edilmesi, hususilik ilkesi (particularity principle) denilen ve tedbirin sadece suç unsuru taşıyan hususlara hasredilmesi ilkesinin de gereğidir[899]. Bu tedbir, doğası itibariyle müdahaleden bağışık olması gerekli olan bir alanda sürekli bir müdahale

---

[891] ERDEM, Gizli Soruşturma, s. 225 METİN, s. 38.

[892] KILKELLY, s. 33

[893] ERDEM, Gizli Soruşturma, s. 226.

[894] METİN, s. 38.

[895] AN OVERVIEW OF ELECTRONIC SURVEILLANCE: History and Current Status, D.1.2,;EHRLICH,s. 8;

[896] 18 U.S.C. & 2518(5).

[897] BERGER-NEW YORK kararında, Mahkeme, iletişimin denetlenmesi amacıyla gelişigüzel kullanılan cihazların Amerikan Anayasası'nın Dördüncü ve Beşinci maddelerinin ciddi anlamda ihlali anlamına geldiği vurgulanmaktadır. BERGER-NEW YORK, 388 u.s. 41-56 http://supreme. justia. com/ us/ 388/ 41/ case.html .

[898] LOPEZ-ABD, 373 U.S. 427, 463 (1963), 26.11.2007 http://supreme.justia.com/ us/373/427/ case.html.

[899] OSBORN-ABD, 385 U.S. 323 (1966), (İET:26.11.2007) http://supreme. justia.com/us/385/ 323/ case html#T7 .

barındırmaktadır. Bu özellik de fiziksel aramadan daha riskli bir noktaya temas etmektedir. Günlerce bazen aylarca süren iletişimin denetlenmesi tedbiri özel hayatın sürekli bir ihlaline yol açabilmektedir[900].

Bununla birlikte, bahsedilen sınırlar içinde kalmak mevcut teknolojilerle pek mümkün değildir. Başka bir ifadeyle, en aza indirgenme prensibi, olması gereken ölçüde sıkı uygulanabilmiş değildir[901] ve de iletişimin denetlenmesi esnasında denetleme amacıyla ilgisi olmayan bilgilerin de ilgililerin bilgisi kapsamına girmesi muhtemeldir. Örneğin, hakkında dinleme kararı alınan bir kişinin konuşmalarından sadece suç unsuru bulunanlarının dinlenmesi diğerlerinin ise ayıklanması sonucunu verecek bir filtrelemenin yapılması teknolojik olarak pek mümkün değildir. Bu hususta uygulayıcıların yaşadığı zorlukları hafifletmek amacıyla ABD Yüksek Mahkemesi, Scott davasında en-aza indirme prensibini uygulamak hususunda dinlemeyi yapan memurun değerlendirmesine atıf yapmıştır. Bu bağlamda, dinlemeyi yapan memur, dinledikleri arasında suç unsuru olmayan konuşmaları kayıttan çıkarırsa veya yazılı metin haline getirmezse veyahut kimseye bildirmezse bu prensibi hayata geçirmiş olur denilmektedir[902]. Özel hayatın özüne müdahaleyi içeren bir tedbiri objektif ve denetime açık bir değerlendirmeye tabi tutmak gerekliliği karşısında, anılan mahkeme kararıyla, ölçülülük ilkesinin ihlal edildiği söylenebilir.

2.2.4. İletişimin Denetlenmesiyle İlgili Diğer Kriterler

İletişimin denetlenmesi kavramının tanımının yapılmasında ve sınırlarının tespitinde, hürriyetleri koruma eğilimi gösteren ve sınırlamalar hususunda daraltıcı bir yorum

---

[900] DEMPSEY, "Communications Privacy In The Digital Age: Revitalizing The Federal Wiretap Laws To Enhance Privacy".

[901] DEMPSEY, "Communications Privacy In The Digital Age: Revitalizing The Federal Wiretap Laws To Enhance Privacy".

[902] Gruda, 2000; AN OVERVIEW OF ELECTRONIC SURVEILLANCE: History and Current Status, D.1.2, 1978'deki Scott v. United States davasında mahkeme, Teknik Dinleme Kanunu'nun temel taşlarından biri olan hakkında dinleme kararı verilen kişinin suç unsuru teşkil etmeyen konuşmalarının dinlenilmesinin en aza indirilmesini (minimization requirement) dinlemeyi yapan devlet görevlisinin takdirine bırakmıştır. Gerçekten de, telefon dinlenmesi suretiyle elde edilen deliller doğrultusunda mahkum edilen Frank Scott, dinlenilen telefon görüsmelerinin sadece % 40'ının suç içerigi taşıdığını, geri kalanının ise normal ve meşru yasamıyla ilgili olduğunu vurgulamış, bu bağlamda dinlemenin en aza indirilmesi için gereken gayretin gösterilmesi prensibinin ihlal edildiğini iddia etmiştir. Scott'a göre konuşmalarının % 60'sı suç unsuru içermemektedir. Mahkeme, Scott'un iddiasını reddetmistir. Mahkemeye göre, dinlemenin en aza indirilmesi prensibi dinlemeyi yapan devlet görevlisinin görevi esnasındaki "iyi niyeti" ile ilgilidir ve dava konusu olayda dinleme yapan görevlinin iyi niyet göstermedigine dair hiçbir emare bulunmamaktadır. SCOTT-ABD, 436 U.S. 128 (1978), 142-143 27.11.2007, http://supreme. justia.com/ us/ 436/ 128/ case.html ; ÖZDOĞAN, (2004), s. 19, 38

tarzını benimseyen[903] AİHM, Sözleşme ile korunan hakların sınırlandırılması anlamına gelen iletişimin denetlenmesi tedbirine başvurulabilmesi için birtakım şartların oluşması gerektiğini uzun bir zaman dilimine yayılan kararlarıyla ifade etmiştir. Belirlenen bu güvenceler hayati önemi haizdir.

8. maddenin ikinci paragrafında belirlenen kriterlerin, yani, müdahalenin kanunla yapılması, meşru amaçlar gütmesi ve demokratik bir toplumda gerekli olması kriterlerinin yanı sıra zaman içinde belirlenmiş olan ek birtakım kriterler marifetiyle AİHM, iletişimin denetlenmesi tedbirini hassas bir hukuki süzgeçten geçirmektedir. Bu kriterlerin barındırdığı güvenceler devletlerin iletişimin engellenmesi hususundaki sınırlarını belirlemektedir. Bu güvencelerin olmaması halinde keyfilik artacak ve görevlilere tanınmış olan yetkiler kötüye kullanılabilecektir. Mahkemenin burada yapmayı istediği şey, bireylerin haklarının kısıtlanması gündeme geldiğinde, bu kısıtlamanın sınırlarının belli edilmesidir. Bu yüzden, AİHM, 8. maddede tanınmış hakların keyfi müdahalelere karşı korunmasını sağlamak bakımından milli hukukta güvencelere ihtiyaç duyulduğunu vurgulamaktadır[904].

Mahkeme, bu hususta üye ülkelerin sahip olmaları gerekli olan güvenceleri Huvig-Fransa[905] davasında belirlemiştir[906]. Bu güvenceler şunlardır[907]:

---

[903] PRIVACY AND HUMAN RIGHTS, http://www.gilc.org/privacy/survey/intro.html#fnlnk0023 (İET:3 .8. 2007).

[904] DOERGA-HOLLANDA kararı, Pr.45.

[905] AİHM, KRUSLIN-FRANSA davasında da benzer ifadelerle bu güvenceleri ifade etmiştir.

[906] HUVIG kararıyla AİHM'nin üstlendiği yol göstericilik misyonu ABD Yüksek Mahkemesi tarafından da üstlenilmiş, 1967 yılında verilen Berger kararında belirlenen şartlar, 1968 yılında çıkarılan Teknik Dinleme Kanunu'nun(Omnibus Crime Control and Safe Streets Act-Title III) oluşturulmasında önemli rol oynamıştır. Berger kararında eleştiri alan ilgili ABD mevzuatındaki eksiklikler, HUVIG ve Kruslin kararlarında belirlenen eksikliklere uymaktadır. Bu eksiklikler şunlardır: İletişiminin denetlenmesi tedbirine konu olacak yere ve suça ilişkin ayrıca suçun işlendiğini veya işlenmekte olduğunu gösterecek yeterli açıklama bulunmamaktadır. Aramayı genel olmaktan çıkaracak sınırlandırmalar bulunmamaktadır. İletişimin ne kadar bir süre zarfında denetleneceği, tedbirin bitiş tarihi belirtilmemiştir, tedbirin bitirilmesi kolluk görevlisine bırakılmıştır. Mahkeme kararının bir an önce yerine getirilmesi öngörülmüş değildir. Mahkeme kararınına ilişkin sürenin uzatılması için sadece 'kamu yararı' yeterli sayılmış, tedbirin uzatılması için makul sebeplerin bulunduğu izah edilmemiştir. Tedbirin ilgiliye bildirimine ilişkin bir düzenleme bulunmadığı gibi, birtakım zorlayıcı nedenlerin (exigent circumstances) varlığı nedeniyle bu kurumun hayata geçirilemediği hususu da belirtilmemiştir. Gizlilik gerekçesiyle bildirimin öngörülmediği hallerde de, bu eksiklik zorlayıcı nedenlerin belirtilmesi suretiyle bertaraf edilmemiştir. Denetleme süreci ve sonuçları hakkında yargıya rapor verme zorunluluğu bulunmamaktadır, böylece yargı iletişimin denetlenmesi tedbirine ilişkin kontrolu yeterince yapamamaktadır. Kanunda, iletişimin denetlenmesi tedbirinin kullanılabilecegi suç tipi için "yeterli sebep" sartı bulunmamaktadır. Kanuna göre, (aynı süphelinin) mahkeme kararında belirtilmeyen suçları için de aynı Mahkeme kararı ile dinleme yapılabilmektedir. Yani, mahkeme kararında belirtilmeyen durumlar için, bu mahkeme kararı kullanılarak dinleme yapılabilmektedir.

[907] HUVIG-FRANSA, Pr. 34,35. Bu karar Fransız Ceza Usul Kanunu'nun bugünkü şeklini almasına neden olan kararlardan biridir. Bu karar yargı kararlarının uygulamaya yol göstermesi örneklerinden biridir. Gerçekten de mahkemenin verdiği karar sonrasında revize edilen kanun maddesi mahkemenin eleştirdiği

Yargısal bir kararla telefonları dinlenmesi muhtemel insan kategorileri belirlenmelidir. (…the categories of people liable to have their telephones tapped by judicial order …)

İletişimin denetlenmesini gerektirecek suçlar tanımlanmalıdır.

Telefon dinlemeye ilişkin süre belirli olmalıdır. Bu bağlamda, hakime sınırsız yetki verilmemelidir.

Dinlemeye alınmış diyalogları içeren özet raporlar tanzim edilmelidir.(…drawing up the summary reports containing intercepted conversations)

Kayıtların silinmesi veya bantların imha edilmesi gerekli olan haller belirlenmelidir. Bu, özellikle de sanığın hukuki takibattan kurtulduğu veya beraat ettiği hallerde mutlaka yapılmalıdır.

Kanun, yazılı olsun veya olmasın, kamu görevlilerine tanınan yetki alanını net bir şekilde belirlemiş olmalıdır.

AİHM içtihatları doğrultusunda belirlenen iletişimin denetlenmesi ile ilgili diğer kriterler şunlardır:

2.2.4.1.Suç ve İnsan Kategorilerinin Belirlenmesi

AİHM, iletişimin denetlenmesi tedbirinin hangi suçlar hakkında uygulanacağına ilişkin bir kategori yapmaktan kaçınmış, genel kriterler belirlemek, bu kriterlerin içinin doldurulmasında da devletlere bir takdir yetkisi tanımak yolunu seçmiştir.

Suç kategorisi ile kişi kategorisi arasında varolan yakın bağlantı nedeniyle, yasal düzenlemeler marifetiyle iletişimin denetlenmesi kararı verilebilecek kişilerle ilgili sınırlamalara yer verilmesi, keyfiliği önlemesi bakımından önemlidir[908]. Keyfiliği önlemek düşüncesinin bir tezahürü anlamında Mahkeme, bir suçla ilişkisi olduğu düşünülen tüm bireylerle ilgili toplu izinlerin verilemeyeceğini, ancak şüpheli veya bu kişiyle bağlantısı olduğu tahmin edilen kişiler hakkında bu tedbire başvurulabileceğini vurgulamaktadır. Mahkeme genel bir izlemeye imkan vermeyen bir formatta kaleme alındığı için Alman G 10 Kanunu'nun kriterlere uygun olduğunu belirtmektedir.

---

hususlardan arındırılmış ve AİHS ve AİHM kriterlerine uygun bir hale getirilmiştir. Ayrıca Bk. ALTIPARMAK, s. 35; TEZCAN-ERDEM-SANCAKTAR, s.237.

[908] KÜNHE, s. 105.

Bununla birlikte, hürriyetlerin sınırlandırılması, sosyal bir gereksinimin karşılanması gerekçesiyle yapılması halinde mazur görüldüğü için, her türlü suçun önlenmesi amacıyla iletişimin dinlenmesi yoluna başvurulamayacaktır [909]. Bu bağlamda AİHM, Erdem-Almanya davasında Alman ceza hukukunda haberleşmesine müdahale edilecek kişilerin kategorisinin belirlenmesini takdirle karşılamıştır. Gerçekten de söz konusu kararda Mahkeme 'haberleşmesinin izlenmesi gerekli olan kişiler' belirlendiği için, diğer bir ifadeyle Alman Ceza Kanununun 129. maddesine göre bir terör örgütüne üye olduğundan şüphelenilen kişilerin kategorisi belirlendiği için bahse konu hükmün çok kesin bir biçimde hazırlandığı gözlemlenmiştir' ifadesini kullanmaktadır[910]. Bu cümleden olarak, hangi suçlar için tedbire başvurulacağı hususunda bir kategorizasyon yapılmış olması Mahkeme kriterlerine göre olumlu bulunmaktadır.

Sosyal bir ihtiyaç bağlamında, her türlü suçla ilgili olarak bu tedbire başvurulması yerine, organize suçlar[911] gibi belli bir ağırlık ihtiva eden suçların varlığı halinde bu tercihe gidilmektedir. AİHM, bu sosyal ihtiyaç kriterinin (pressing social need) devletler açısından öneminin farkında olarak, iletişimin denetlenmesi tedbirine başvuran devletlerin gerekçelerini belli bir düzeye kadar haklı görmektedir. Örneğin, Birleşik Krallık Hükümeti'nin, Malone davasına ilişkin savunmasındaki bazı argümanlarına bu anlamda iştirak etmektedir. Anılan hükümetin konuyla ilgili raporunda (white paper) yer alan ve suçların özellikle de organize suçların artışı ve suçluların daha da gelişmiş yöntemler kullanması hususlarını not eden Mahkeme, bu tür tedbirlerin doğasında var olan gizlilik nedeniyle suiistimal tehlikesine dikkat çekmekle birlikte, telefon dinlenmesinin ağır suçların önlenmesi ve araştırılması hususunda kaçınılmaz olarak kullanılması gerekli olan enstrümanlar olduğunu kabul etmektedir[912]. Bununla birlikte, Mahkeme, polisin basit kuşkularının bu kararı vermek için yeterli ve tatmin edici olamayacağını belirtmekte, bu tür tedbirlerin belli ağırlıktaki suçlar bakımından ve belli birtakım şartların karşılanması koşuluyla uygulanması gerekliliğini vurgulamaktadır.[913].

Hak ve hürriyetlere müdahale niteliği taşıyan düzenlemelerle ilgili sınırlayıcı koşulların teferruatlı olarak düzenlenmesini yine hakkın korunması için bir koruma olarak

---

[909] DÜLGER, s. 6.

[910] ERDEM-ALMANYA, 5.7.2001, 38321/97 Pr. 64-66.

[911] Amerikan kanun koyucunun iletişimin denetlenmesine ilişkin usul ve esasları içeren Teknik Dinleme Kanununu kaleme almasının asıl nedeni, organize suçlarla mücadele etmek düşüncesidir. Bk. ABD Teknik Dinleme Kanunu bölümü.

[912] MALONE- BİRLEŞİK KRALLIK, Pr. 81.

[913] Bk. PRADA BUGALLO-İSPANYA Pr.

algılayan AİHM, bir kimsenin belirli suçları işlemeyi planladığına, işlemekte olduğuna veya işlediğine dair kuşku duymak için maddi belirtilerin bulunması gerektiğini ifade etmektedir[914]. Şüpheyi somut belirtilerin üzerine kuran Mahkemenin bu tavrı, devletlere tanınan takdir yetkisini daraltan, bireylerin haklarını genişleten bir tavırdır.

2.2.4.2. Tedbire Son Çare Olarak Başvurulabilmesi

İletişimin denetlenmesine ilişkin tedbire, maddi olayların tespitinin başka yöntemlerle mümkün olması halinde başvurulmaması gerekir[915]. Bazı yazarların ikinci derecede uygulanabilirlik olarak[916] adlandırdıkları bu ilkenin amacı, bir kimsenin bir suça ilişkin fiilleri ciddi olarak işlemeyi planladığına ya da işlemekte olduğuna ya da işlediğine dair kuvvetli maddi belirtilerin bulunması halinde ve diğer yöntemlerle bu tür delillerin elde edilmesinin mümkün olmadığı anlaşıldığında iletişimin denetlenmesi tedbirine başvurulmasıdır. Başka yöntemlerle delil elde etmenin mümkün bulunmamasının yanı sıra, bu yöntemlerin çok güç olması halleri de bu tedbire başvurulması için yeterli şartların oluştuğu anlamına gelir[917]. Dinlemenin kullanılacağı dava sayısını azaltmak ve mahremiyete yönelik riskleri en aza indirgemeyi hedefleyen bu ilkeyi[918] AİHM, uygulayıcıların keyfi birtakım uygulamalara yeltenmesinin önlenmesi bakımından da önemli görmektedir[919].

ABD hukukunda, son çare prensibinin açıklandığı Madde 2518(3)'e göre iletişimin denetlenmesi imkanının kullanılabilmesi için, iletişimin denetlenmesi dışındaki soruşturma yöntemlerinin kullanıldığı, ancak bu yöntemlerin başarısız olduğu, bu tedbir dışındaki yöntemlerin kullanılması durumunda başarı elde edilemeyeceğine ilişkin bir kanaat olduğu veya bu tedbir dışındaki yöntemlerin kullanılmasının çok tehlikeli olduğu tespit edilmelidir[920]. Görüldüğü gibi, ABD hukukunda, Strasbourg hukukundan farklı olarak bu tedbire başvurulması için diğer yöntemlerin başarısızlığı ve imkansızlığı kriterlerinin yanı sıra diğer yöntemlerin tehlikeliliği de bu tedbire başvurulmasını mazur gösteren bir haldir.

---

[914] KLASS-ALMANYA, Pr.

[915] KÜNHE, s. 105.

[916] ERDEM, Gizli Soruşturma, s.320

[917] DOĞRU, s. 243.

[918] DONOHUE, s.8; AN OVERVIEW OF ELECTRONIC SURVEILLANCE: History And Current Status, D.1.2; EHRLICH, s. 8

[919] KÜNHE, s. 105.

[920] 18 U.S.C. § 2518(3); DONOHUE,s. 8; AN OVERVIEW OF ELECTRONIC SURVEILLANCE: History And Current Status, D.1.2; ÖZDOĞAN, (2004), s.33; EHRLICH, s. 8;

2.2.4.3. Elde Edilen Verilerin Korunması ve Şartlar Oluştuğunda Yok Edilmesi Zorunluluğu

İletişimin denetlenmesi suretiyle elde edilen bilgiler kural olarak gizli kalmalıdır. Kamuoyunun bilgilenme hakkı ile bu bilgilerin gizliliği arasındaki ilişki ve menfaat dengesi iyi ayarlanmalıdır. Bu bilgilerin kamuoyuna açıklanmasında acil toplumsal bir ihtiyaç olduğunun da ispat edilmesi gerekir[921].

AİHM içtihatlarına göre, iletişimin denetlenmesinin hukuka uygunluğunun sağlanabilmesi bakımından önemli olan hususlardan biri, bu faaliyetlerin sınırı ve bu faaliyetler sırasında bireyin özel hayatının gizliliğine riayet hakkını koruyucu yeterli güvencelerin ve bazı karşı önlemlerin[922] alınması gerekliliğidir[923]. Elde edilen kayıtların zarar görmeden ve bütünlüklerini kaybetmeden (intact and in their entirety) muhafaza edilmesi gerekmektedir. Gerek hakimin, gerekse savunma tarafının bu tür bir koruma mekanizması olmadan davada delil olarak sunulan kayıtların gerçek olup olmadığını ve sonradan müdahaleye uğrayıp uğramadığını anlaması mümkün olmaz[924]. Bu durum da özellikle adaletin tecellisi açısından hayati önemi haizdir. Bu hususun eksikliği adil yargılanma ilkesinin ihlal edildiği iddiasını gündeme getirecektir.

İletişimin denetlenmesi suretiyle elde edilen bilgilerin silinmesi ve imha edilmesi de AİHM'nin yasal düzenlemeye kavuşturulması gerekliliğine vurgu yaptığı hususlar arasındadır. Huvig ve Kruslin kararlarında, iletişimin denetlenmesinden elde edilen kayıtların silinmesi ve imha edilmesine ilişkin şartların belirlenmemiş olması bir eksiklik olarak değerlendirilmiş ve ilgili Fransız mevzuatı eleştirilmiştir[925]. Mahkeme haberleşmeye müdahale sonucu elde edilen bilgilerin ve kayıtların saklanması ve yok edilmesi ile ilgili düzenlemelere yer verilmesinin, keyfiliği önleyici etkileri bakımından önemli olduğunu belirtmektedir[926]. Bireyin korunması, bu bağlamda bu amaca yönelik makul ve etkili garantiler içeren yasal düzenlemelerin öngörülmesi ile sağlanabilecektir.

---

[921] TEZCAN/ERDEM/SANCAKDAR, s. 239.

[922] Hakim PETTITI, MALONE-BİRLEŞİK KRALLIK.

[923] ŞİMŞEK, s. 4.

[924] HUVIG-FRANSA, Pr. 34, KRUSLIN-FRANSA, Pr. 35 .

[925] HUVIG-FRANSA, Pr. 34, KRUSLIN-FRANSA, Pr. 35.

[926] KÜNHE, s. 105.

Aksinin kabulü, Sözleşmenin 8 inci maddesinde belirtilen hakların ihlal edilmesine yol açacaktır[927].

2.2.4.4.Yetkili Merci Kararı ile Tedbire Başvurulabilmesi

Bir suçun işlendiğine ya da işlenmekte olduğuna ilişkin olguların varlığı halinde, bazı tedbirlerin uygulanmasının istenmesi tabiidir. Kuvvetler ayrılığı ilkesinin gereği olarak, bu tedbirlerin bağımsız mahkemeler tarafından alınması gerekmektedir[928]. Bununla birlikte, iletişimin denetlenmesi üzerinde bir yargısal kontrol ihdas edilmesi yalnızca kuvvetler ayrılığından kaynaklanan bir felsefeye dayanmamakta, bu hususla birlikte özel hayatı koruma çabasının bir sonucu olarak ortaya çıkmaktadır[929]. Bu denetim yetkisinin, doğası itibariyle tüm taraflara aynı uzaklıkta bulunan yargıya bırakılması keyfiliğin de önlenebilmesini sağlayan yasal bir güvencedir[930].

İletişimin denetlenmesi hususundaki mevzuatı uygulama ve yorumlama yetkisi esas olarak sözleşmeci devlet mahkemelerine aittir[931]. AİHM, iç hukuku uygulamak ve yorumlamak görevinin öncelikli olarak milli makamlara ve özellikle de mahkemelere ait olduğunu vurgulamaktadır. Bu bağlamda, Fransız Ceza Usul Kanunu'nun 81, 151 ve 152. maddelerinin sorgu hakimi tarafından verilen bir izin tahtında, üst düzey bir polis görevlisi tarafından iletişime müdahale edilmesini makul gördüğü şeklindeki Fransız Yargıtay'ı görüşü hakkında bir değerlendirme yapmamış ve böyle bir değerlendirme yapmanın Sözleşmeci devlet mahkemelerinin görev alanına girmek anlamına geleceğini ifade etmiştir[932]. Önemli olan, makul bir açıklıkla iletişimin denetlenmesine ilişkin yetkilerin nasıl kullanıldığının, hangi yetkilerin idarenin takdirine bırakıldığının izah edilmesidir[933].

---

[927] ŞİMŞEK, s. 4.

[928] Hakim PINHEIRO FARINHA'nın karşı görüşü, MALONE-BİRLEŞİK KRALLIK. Hakim PINHEIRO FARINHA, başvuru konusu Birleşik Krallık uygulamasını eleştirerek, iletişimin denetlenmesi tedbirinin, İçişleri Bakanlığı(Home Office) tarafından kontrol edilse bile, bir polis memuru tarafından yerine getirilmesinin doğru bir uygulama olmadığını ifade etmektedir. Anılan hakime göre, suç konusu şüphenin ve suçluya ilişkin tehlikeliliğin takdirinin polise bırakılması elde edilmek istenen yasal amaca uygun değildir.

[929] Hakim PETTITI,(Çoğunluk Görüşü) MALONE-BİRLEŞİK KRALLIK.

[930] KÜNHE, s. 103.

[931] HUVIG-FRANSA, Pr.28; Bk. Ayrıca MALONE-BİRLEŞİK KRALLİK, Pr. 79; Eriksson-İsveç, 22.7.1989, Pr. 25, 62

[932] HUVIG-FRANSA, Pr. 28

[933] MALONE-BİRLEŞİK KRALLIK, s. 79

İletişimin denetlenmesine ilişkin karar farklı yargı sistemleri içinde farklı merciler tarafından verilebilmektedir. AİHM, bir idari merci tarafından verilen iletişimin denetlenmesi kararını ihlal nedeni saymamaktadır. Burada öne çıkan husus, bu idari nitelikteki kararın yargısal bir denetime tabi tutulması gibi bir güvencenin sağlanmış olmasıdır. Örneğin İngiliz hukukunda iletişimin denetlenmesine ilişkin karar bir mahkeme tarafından verilmemekte, ancak bu karar bir mahkemenin denetimine tabi kılınmaktadır. İçişleri Bakanlığı(Home Office) tarafından iletişimin denetlenmesi ile ilgili olarak verilen kararlar (warrant), sürecin yasallığını denetlemek için kurulmuş özel bir mahkeme (tribunal) tarafından denetlenmektedir[934]. RIPA'nın 65 vd. maddeleri uyarınca kurulan, iletişimin denetlenmesi ile ilgili şikayetleri, örneğin istihbarat memurlarının davranışlarını ya da genel olarak iletişimin denetlenmesi ile ilgili davranışları denetleyen, yüksek yargı mensuplarının üyesi olduğu bu mahkeme, RIPA kapsamında vuku bulan iletişimin denetlenmesi ile ilgili şikayetlerin götürüldüğü bir mercidir[935].

İletişimin denetlenmesi tedbirine karar verecek denetime açık bir merciin varlığı tek başına yeterli olarak görülemez. Bu merciin vereceği kararın kalitesi de önemlidir. AİHM, salt bir kanunun varlığını yetersiz görüp, kanunun kalitesinin de önemli olduğunu vurguladığı gibi, mahkeme kararının da belli bir kaliteye sahip olmasının gerekliliğine işaret etmektedir. Bu itibarla Mahkeme[936], kararların gerekçeli olmasını istismarı ve keyfiliği önleyici bir güvence olarak görmektedir. Kararı verecek olan hâkimi konu üzerinde daha ciddi düşünmeye sevk etmek gibi önemli bir fonksiyon ifa eden gerekçelendirme, verilen kararların denetlenmeye açık bir hüviyet kazanması ve tedbirin uygulanma sebebinin ilgililerce net olarak anlaşılabilmesi gibi faydalar sağlayacaktır.

Gerekçelendirme, karara dayanak bulma işleminin de ötesinde, belirli bir amacın elde edilmesini sağlamalıdır. Hususilik ilkesi[937] olarak da nitelendirebileceğimiz bu yaklaşım marifetiyle, genel bilgi avcılığı amacına yönelik tedbirlerin uygulanması engellenmiş olacaktır[938].

---

[934] MOWBRAY, s. 393

[935] FOSTER, s. 389; RIPA, 65-70., http://www.opsi.gov.uk/Acts/acts2000/ukpga_20000023_en_2#pt1-ch1-pb1-l1g1 ,(İET:19.12.2007);

[936] Kararların gerekçeli olması zorunluluğu ile ilgili olarak Bk. PRADA BUGALLO-İSPANYA kararı.

[937] Bu yaklaşım ABD hukukunda 'particularity principle' olarak adlandırılmaktadır.

[938] KÜNHE, s. 105.

Kararların gerekçelendirilmesinde yetersizlik özellikle AİHM önüne getirilen başvurular bakımından çok eleştiri aldığımız bir husustur. Mahkeme kararların gerekçeli olmamasını daha doğru bir ifadeyle gerekçenin yetersiz oluşunu eleştiri konusu yapmaktadır. Özellikle tutuklama kararlarındaki 'suçun vasfı ve mahiyeti, mevcut delil durumu, delillerin karartılması tehlikesi , sanığın kaçma ihtimalinin bulunması…' gibi basmakalıp (stereotype) ifadeler, hakkımızdaki birçok mahkumiyet kararına gerekçe olmaktadır. Bu eksikliğin karşımıza çıkarıldığı diğer alanlar da, suçluların iadesine ilişkin taleplerimizdir. Görülmekte olan bir dava nedeniyle ya da kesinleşmiş bir ceza mahkumiyetinin infazı amacıyla ülkemize getirilmesi için Suçluların İadesine Dair Avrupa Sözleşmesi hükümleri kapsamında hakkında iade prosedürü başlatılan kişilerle ilgili olarak, anılan Sözleşme gereği talep edilen ülkeye, talep içeriğini ve iade konusu kişiye atılı suçları belirten bir iade talepnamesinin iletilmesi gerekmektedir. Bu gibi taleplerin iletildiği makamlarca iade taleplerimizin reddedilme gerekçelerinin başında kararlarımızın gerekçeli olmaması gösterilmektedir. Kişiyle, kendisine atılı suç arasındaki illiyet bağının net olarak ifade edilmediği kararlar özellikle Anglo-Sakson sistemini benimsemiş ülkelerce iade edilmekte, bu bağlamda birçok kişi başka ülkelerde ceza adalet sisteminden kurtulmuş olarak dolaşmaktadırlar.

2.2.4.5. Tedbirin Süresi

AİHM, iletişimin denetlenmesi tedbirinin uygulanabileceği süre konusunda somut bir zaman dilimi belirlemesi yapmamıştır. Farklı ülkelerden AİHM önüne gelen başvurularda, mahkemenin, iletişimin denetlenmesine ilişkin süreler bakımından bir eleştiri getirmediği görülmektedir[939].

Ancak Mahkemeye göre, haberleşmeye müdahalenin limitinin ilgili kanunlarda belirlenmesi keyfiliğin önlenmesi bakımından önemlidir. Gerçekten de Kruslin ve Huvig kararlarında Mahkeme, telefon dinlenmesi ile ilgili olarak bir zaman limiti öngörülmemiş olmasını ihlal kararının gerekçeleri arasında göstermiştir[940].

2.2.4.6.İlgiliye Bildirimde Bulunma

İletişimin denetlenmesi tedbirinin sonlandırılması sonrasında ilgiliye bildirimde[941] bulunulması, keyfiliği önleyici yasal güvenceler bakımından büyük önem

---

[939] KÜNHE, s. 105.

[940] KRUSLIN-FRANSA, Pr. 35; HUVIG-FRANSA, Pr. 34.

[941] Klass-Federal Almanya kararında, konuyla ilgili terim 'subsequent notification' olarak yer almaktadır. Sözkonusu ifade, kararın Fransızca metninde, 'la notification ultérieure' olarak kullanılmaktadır.

taşımaktadır[942]. Keyfilikten kaynaklanabilecek tehlikelerin önlenmesi amacıyla, AİHM[943], dinleme sona erdiğinde gizli dinlemeye ilişkin olarak ilgiliye sonradan bilgi verilmesi gerekliliğine dikkat çekmiştir. Bununla birlikte, bildirimin yapılması, amacı tehlikeye düşürmemelidir[944]. Bu yaklaşımın altında yatan temel neden, hakkına müdahale edilen bireyin müdahalenin gizliliği nedeniyle müdahalenin hukukiliğini denetleme imkanından yoksun olmasıdır[945].

AİHM anılan tutumunda, yani ilgiliye bildirim sorununu ele alırken, katı bir tutum izlememektedir. Gerçekten de, Mahkeme, Klass Almanya başvurusunda, kanunda gözlem süresinin bitiminde ilgiliye bildirimde bulunma zorunluluğunun bulunmamasını, uygulamanın etkinliğinin ancak bu yolla sağlanabileceği gerekçesiyle Sözleşmenin 8. maddesine aykırı bulmamıştır[946]. İdari yetkilerin gizli olarak kullanılmasının keyfilik riskini artırdığını bu nedenle bildirim kurumunun tesis edilmesi gerekliliğini vurgulayan Mahkeme, bu yaklaşımını dengelemek amacıyla da uygulanan tedbirlerin gizliliğinin sağlanmasının gerekli olduğunu ve bu arada bir dengenin kurulması gerektiğini belirtmiştir[947].

AİHM, kararlarında önleyici amaçla yapılan iletişimin denetlenmesi tedbirinin ilgiliye bildirilmesini zorunlu görmemiştir. Keyfiliği önleyici etkin diğer mekanizmaların varlığı halinde, bildirim yapılmamasının tek başına ihlal oluşturmayacağı kabul edilmiştir[948].

ABD hukukunda da benzer bir yaklaşım vardır. Önleme amaçlı denetlemeyi düzenleyen FISA iletişimi denetime tabi tutulan kişiye bildirim zorunluluğu getirmemekte[949] ve bir ABD vatandaşı hakkında iletişime müdahale yoluyla elde edilen bilgi, bu kişinin rızası aranmaksızın kullanılabilmekte ve açıklanabilmektedir. Bununla birlikte, bu yetkinin kullanılabilmesinin yasal amaçlarla (lawful purposes) sınırlı

Subsequent/ ultérieure sıfatları 'sonraki' anlamına geldiği için 'sonradan bildirim' olarak da çevrilen bu kavramın, bildirim ya da 'tedbir sonrası bildirim' ya da sadece 'bildirim' olarak kullanılmasının daha uygun olacağını düşünmekteyiz. Bk. DOĞRU, Osman; İnsan Hakları Avrupa Mahkemesi İçtihatları,C I, Adalet Bakanlığı Eğitim Dairesi Başkanlığı Yayınları, s. (57).

[942] KÜNHE, s. 103.

[943] Bk. KRUSLIN-FRANSA ve HUVIG-FRANSA davaları.

[944] TEZCAN/ERDEM/SANCAKDAR, s. 238.

[945] KLASS-ALMANYA, Pr.; Doğru, s. 243.

[946] BEŞE, s. 185.

[947] DİNÇ, s. 423.

[948] ALTIPARMAK, s. 51.

[949] AN OVERVIEW OF ELECTRONIC SURVEILLANCE: History and Current Status, D.1.3.

tutulması ve bu tedbirin kullanılmasında en aza indirgeme (minimisation) prensibinin uygulanması önemlidir[950]. İletişimin denetlenmesi yoluyla elde edilen bilgilerin mahkemede delil olarak kullanılması öncesinde hükümetin davalıya bu bilgilerin delil sıfatını haiz olmadığını ispatlama hakkı olduğunu bildirme zorunluluğunun olması bu anlamda kişilere tanınmış bir hak olarak gözükse de, milli güvenliğe halel getireceği gerekçesiyle bu hakkın kullanılmasına yasak getirilebilmesi[951] ile bu hakkın uygulamada kullanılamaz hale getirileceği muhakkaktır .

AİHM tarafından belirlenen bu yaklaşım suçlarla mücadelenin etkinliği bakımından isabetlidir. Nitekim, özellikle önleyici amaçlı denetlemelerde kişiye bildirimde bulunmanın şart koşulması halinde organize suç ve terör suçlarıyla mücadeleden sonuç alınamayacaktır. Aylar hatta yıllar süren takip sonucunda elde edilen ipuçlarının resmi ağızdan ilgiliye ihbar edilmesi anlamına gelecek olan bildirim bu tedbiri ve genel olarak suçla mücadeleyi etkisizleştirecektir. Bildirim mekanizmasının kaldırılmasının rasyonel bir adım olmadığı muhakkak olmakla birlikte, bu tedbirin barındırdığı sakıncaların giderilmesi bakımından denetim sisteminin güçlendirilmesi bildirimle elde edilmek istenen hukuki faydadan daha fazlasını ilgiliye ve tüm kamuoyuna verecektir.

2.2.4.7. Etkin Denetim

Demokratik sistemlerin vazgeçilmez bir unsuru olan hukukun üstünlüğü ilkesi, idari makamlarca kişi hak ve hürriyetlerine ilişkin olarak yapılan müdahalelerin, normal şartlar altında yargı tarafından sağlanması gerekli olan etkin bir kontrole (effective control) tabi tutulmasını gerektirmektedir. Mahkemeye göre, bu sağlanamadığı takdirde en son çare olarak, müdahale, bağımsızlık, tarafsızlık ve makul bir usul güvencelerini sunan bir yargısal denetime tabi kılınmalıdır Bu denetimin normal şartlar altında yargısal mercilere bırakılmış olması (an effective control which should normally be assured by the judiciary) bu denetimin yargı tarafından deruhte edilmesininin sine qua non bir şart olduğu anlamına gelmemelidir. Gerçekten de Mahkeme, anılan karara konu olayın gerçekleştiği tarihte Federal Almanya'da yargısal denetim mekanizmasının bulunmayışını, bu görevin Parlamento Heyeti ve G 10 komisyonunca yapılmasını demokratik bir toplumda gerekli görülen sınırın aşılması olarak yorumlamamıştır. Anılan organların, iletişimin denetlenmesini yapan kişilerden farklı olmasını, bağımsız

[950] WONG, 3.4.10.

[951] WONG, 3.4.11.

olmalarını, görevlerini etkili ve sürekli bir şekilde yapmak için yeterli güç ve yetkilere sahip olmalarını yeterli görmüştür[952].

Denetime ilişkin ilkeler AİHM tarafından belirlenmiştir. Mahkeme'ye göre, iletişimin denetlenmesi işleminin denetimi bu tedbir ilk olarak başlatıldığında ilk emredildiğinde, sürdürülürken ve işlem sona erdikten sonra (when the surveillance is first ordered, while it is being carried out, or after it has been terminated) yapılabilir. İletişimin denetlenmesi tedbirinin doğası gereği, ilk iki aşamaya ilişkin, yani denetimin başlatılması ve devam ettirilmesine taalluk eden aşamalarda, hem tedbirin kendisi hem de bu tedbirin denetlenmesine ilişkin usul ilgilinin bilgisi dışında gerçekleştirilmelidir. Giz içeren işlemin ilk iki aşamasında, hakkında tedbir başlatılan kişinin denetim mekanizmasını başlatamayacağı gerçeğinden hareketle tedbire ilişkin garantilerin sözleşmeci devlet tarafından alınması gerekmektedir. Bu bağlamda, iletişimin denetlenmesi tedbiri, bireyin haklarının korunmasına ilişkin yeterli ve eşdeğer garantiler (adequate and equivalent guarantees) sağlamalıdır[953].

Fransa'nın, iletişimin denetlenmesini düzenleyen kanununda (Ceza Usul Kanunu) bu tedbirin denetlenmesine izin veren ve suiistimali önleyecek bir garanti maddesinin bulunmayışı yeni bir ihlale neden olmuştur. AİHM'ye göre, Fransa Kanunu'nun, kimin telefonunun dinlendiği konusunda ayrım yapmaması, vatandaşların hakkı olan 'etkin kontrol'(effective control) kurumunu devre dışı bırakmaktadır ve bu durum 8. Madde ihlaline neden olmaktadır[954].

Denetimi yapacak merciin takdiri hususu da Mahkeme tarafından ele alınmıştır. Mahkeme, denetleyici kurum veya kişilerin bağımsız davranabilme yetkisi konusunda, keyfiliği önleyici mekanizmaların bulunması bakımından, sistemin düzgün işleyişinin kontrolünün parlamentoya, adalet bakanlığına, parlamento ombudsmanı ve meclis adalet komitesi gibi bağımsız kurumlara verilmiş olmasına çok önem verdiğini belirtmiştir[955]. Leander-İsveç kararında, başvuru konusu olay tarihinde İsveç'te bulunan ve denetim görevi üstlenmiş Milli Polis Kurulu'ndaki (National Police Board) parlamenter varlığı AİHM tarafından takdir edilmekte, Adalet Bakanlığı, Parlamento Ombudsmanı ve Meclis Adalet Komitesinin bu bağlamdaki görevleri

[952] KLASS- ALMANYA, Pr. 55; KILKELLY, s. 50.

[953] KLASS- ALMANYA,Pr. 55.

[954] LAMBERT-FRANSA, Pr.34-41.

[955] KILKELLY, s. 38.; LEANDER-İSVEÇ, Pr.65.

önemsenmektedir. Milli Polis Kurulu'nda muhalefet milletvekillerinin de bulunmasını, bu kişilere veto hakkının verilmiş olması da not edilen diğer hususlardır[956]. Dikkat çeken husus, denetime yapılan vurgudur. Bireyin, niteliği itibariyle kontrolü altında tutamadığı ve denetimden geçirilmesini sağlayamadığı ilk iki aşamada bu tedbirin yani denetimin başlatılması ve devam ettirilmesine taalluk eden aşamalarda, devletin bireyin hakkını koruma görevini üstlenmesi anlamına gelen denetimi kimin yaptığı Mahkeme tarafından fazla önemsenmemektedir. Denetimin içeriği ve kalitesi, kişi haklarının giz içeren tedbire karşı korunması anlamında çok önemlidir.

Denetimsiz ya da yeterli denetimin sağlanamadığı sistemlerde, devletin başvurduğu sınırlama araçları demokrasiyi savunma yerine onun temellerini oyabilir ve hatta demokrasiyi yok edebilir. Aslında vatandaşların gizli olarak izlenmesi "polis devleti"nin en önemli özelliklerinden biri olup, sadece demokratik kurumların korunması açısından kesinlikle gerekli olan durumlarda tolere edilebilir[957].

AİHM, ilgili devletin mevzuatında iletişimin denetlenmesine imkan tanıyan hükmün varlığı halinde bile 8. maddenin ihlali hükmü verilebilmektedir. Bu itibarla, yasal düzenleme, bu tedbiri kullanan kişilere yönelik bir kontrol hükmü getirmelidir. Mahkeme, Halford-Birleşik Krallık davasında Klass davasındaki karara atıf yaparak konuyla ilgili yasal düzenleme hakkında 'söz konusu kanunun varlığı halinde bile, bu kanunun uygulandığı kişiler bakımından bir tehdit ihtiva etmektedir. Bu tehdit, posta ve telekomünikasyon hizmetleri kullanıcıları arasında haberleşme özgürlüğüne mutlak olarak zarar vermektedir. Böylece, başvuruculların aile ve özel hayatına ve haberleşme hürriyetine saygı gösterilmesi hakkına bir kamu otoritesinin müdahalesi gerçekleştirilmiş olmaktadır' şeklinde değerlendirme yapmıştır[958].

[956] LEANDER-İSVEÇ, Pr. 65; TEZCAN/ERDEM/SANCAKDAR, s. 239.

[957] KLASS-ALMANYA, Pr. 42.

[958] HALFORD-BİRLEŞİK KRALLIK, Pr.41.

BÖLÜM 3. TÜRK HUKUKUNDA İLETİŞİMİN DENETLENMESİ

3.1.Türk Hukukunda İletişimin Denetlenmesine İlişkin Tarihsel Süreç

3.1.1. Genel Olarak

Duygu, düşünce veya bilgilerin akla gelebilecek her türlü yolla başkalarına aktarılması[959] ya da kişilerin birbirleriyle ve toplumla ilişki kurması, haber, düşünce ve kanıları öğrenme ve yayması işlemi olan iletişim[960], uluslararası sözleşmeler ve anayasalarla koruma altına alınan haberleşme hürriyetinin en temel unsurudur. Bununla birlikte, kişilerin ve toplumun güvenliğinin sağlanabilmesi bakımından hakların sınırlanması da bir gereklilik olarak belirmiş ve iletişimin denetlenmesi tedbiri de bu çerçevede hukuk dünyasındaki yerini almıştır.

Bugün, hemen tüm devletlerde, ceza muhakemesinde soruşturma ve kovuşturma organlarına telekomünikasyon yoluyla yapılan iletişimin denetlenmesine olanak sağlayan yasal düzenlemelere yer verilmektedir. Türk hukukunda ise, tedbirin temel hak ve hürriyetlere müdahale oluşturduğu ve bunun için de yasal bir dayanağının bulunması zorunluluğu bilinmekle birlikte, bu konuda, CMUK'ta yasal bir düzenleme bulunmamaktaydı[961]. Türk Hukukunda söz konusu tedbir, ilk kez 1999 yılında yürürlüğe giren '4422 sayılı Çıkar Amaçlı Suç Örgütleriyle Mücadele Kanunu' ile yasal düzenlemeye kavuşmuştur. Bu kanunda, iletişimin denetlenmesi tedbirini ifade etmek için "İletişimin dinlenmesi ve tespiti" terimi tercih edilmişti. Ayrıca, öğretide, öteden beri "telefon konuşmalarının koruma tedbiri olarak gizli dinlenmesi"[962], "haberleşme

---

[959] Türk Dil Kurumu Sözlüğü, http://www.tdk.org.tr/TR/SozBul (İET:22.11.2007)

[960] OSKAY, Ünsal: Kitle Haberleşme Teorilerine Giriş, Ankara 1968, s. 94; Ayci, Emrullah: "İletişim Özgürlüğü ve Özel hayatın Gizliliği", Polis Dergisi, S: 45, Temmuz-Ağustos-Eylül 2005, s. 13.

[961] ŞEN, Ersan: Gizli Dinleme ve Görüntüleme Fiillerinin Türk Hukukundaki Yeri Üzerine Bir İnceleme, İBD 1993/7-8-9, s. 527 vd.; ANAYURT, Ömer: "Strasbourg İçtihatlarında, Türk ve Fransız Hukuklarında Telefon Dinlemeleri", MBD C. XXI S. 1997, s.55 ; ÖZTÜRK, Bahri: Ceza Muhakemesi Hukukunda Koğuşturma Mecburiyeti İlkesi (Hazırlık Soruşturması), Ankara 1991, s. 127; TOSUN, Öztekin: Türk Suç Muhakemesi Hukuku Dersleri, C. I Genel Kısım, İstanbul 1984, s. 912; GÖKCEN, Ahmet :Ceza Muhakemesi Hukukunda Basit Elkoyma ve Postada Elkoyma (Özellikle Telefonların Gizlice Denetlenmesi), Ankara 1994, s.172; KUNTER, Nurullah/YENİSEY, Feridun/NUHOĞLU,Ayşe : Ceza Muhakemesi Hukuku, 15. bası, İstanbul 2006, no. 696; YURTCAN, Erdener: Ceza Yargılaması Hukuku, 5. bası, İstanbul 1994, s.350; SÖZÜER, Adem: Türkiye'de ve Karşılaştırmalı Hukukta Telefon, Teleks, Faks ve Benzeri Araçlarla Yapılan Özel Haberleşmenin Bir Ceza Yargılaması Önlemi Olarak Denetlenmesi, İHFM 1997, Türkan Rado'ya Armağan, C.LV, S.3, s. 70 vd.; ZAFER, Hamide, Ceza Hukukunda Terörizm, İstanbul 1999, s. 283.

[962] TOSUN, Öztekin : Ceza Muhakemesinde Koruma Tedbiri Olarak Gizli Dinleme, İÜHFM, C.41, 1976, (Gizli Dinleme), s.76.

araçlarının dinlemeye alınması"[963], "haberleşmenin denetlenmesi"[964], "komünikasyon araçlarıyla yapılan haberleşmenin denetlenmesi"[965], "iletişimin dinlenmesi"[966], "telefon dinlenmesi"[967], "iletişimin izlenmesi"[968], telefon, teleks, faks gibi araçlarla yapılan haberleşmenin denetlenmesi"[969] ve "uzakla haberleşmenin denetlenmesi"[970] terimleri de kullanılmaktaydı[971].

01.06.2005 tarihinde yürürlüğe giren 5271 sayılı Ceza Muhakemesi Kanun'unda (CMK) bu konuda yeni düzenlemelere yer verilmiş ve 5320 sayılı Ceza Muhakemesi Kanununun Yürürlük ve Uygulama Şekli Hakkında Kanun'un 18/d maddesi ile 4422 sayılı Kanun yürürlükten kaldırılmıştır. Bunun yanında, suç işlenmesinin önlenmesi amacıyla da bazı düzenlemelere gidilmiştir. Son olarak 5397 sayılı Kanun'la kolluk güçlerine, önleyici amaçlarla iletişimin dinlenmesi, tespiti, sinyal bilgilerinin değerlendirilmesi, kayda alınması, teknik araçlarla izleme yapılması, kamu kurum ve kuruluşlarının elinde bulunan bilgi ve belgelerden yararlanılması gibi yetkiler tanınmıştır. Yasal düzenlemelerde terim olarak da, isabetli bir şekilde, "iletişimin denetlenmesi" terimi tercih edilmiştir.

3.1.2. 1982 Anayasası ve Haberleşme Hürriyeti

3.1.2.1.Haberleşme Hürriyeti Kavramı

Gerek 1961 Anayasası'nda[972] gerekse 1982 Anayasası'nda koruma altına alınmış olan haberleşme hürriyeti, uluslararası sözleşmeler ve bildirgelerde de koruma altına

---

[963] YURTCAN, Erdener : Ceza Yargılaması Hukuku, 5. Bası, İstanbul 1994, s. 349.

[964] Cihan, EROL/YENİSEY, Feridun : Ceza Muhakemesi Hukuku, 5. Bası, İstanbul 1997, s. 258; CENTEL, Nur: Koruma Tedbirlerinde Gelişmeler, Hukuk Araştırmalar Dergisi, 1995, s.77

[965] ÖZTÜRK, Bahri/ERDEM, M Ruhan/ÖZBEK, Veli Özer : Uygulamalı Ceza Muhakemesi Hukuku,Ankara 2004, s. 794.

[966] KUNTER/YENİSEY/NUHOĞLU , s.696.

[967] CENTEL, Nur/ZAFER, Hamide: Ceza Muhakemesi Hukuku, İstanbul 2003,(2003) s. 268.

[968] DÖNMEZER, Sulhi: Çetelerle Mücadele Amacıyla 4422 Sayılı Kanunla Kabul Edilen Koruma Tedbirleri, Yargı Reformu 2000 Sempozyumu, İzmir 2000, s. 268.

[969]GÖKCEN, Ahmet: Ceza Muhakemesi Hukukunda Basit Elkoyma ve Postada Elkoyma (Özellikle Telefonların Gizlice Dinlenmesi), Ankara 1994, s. 188; SÖZÜER, s. 64.

[970] ERDEM , Mustafa Ruhan/ ÖZBEK, Veli Özer : 4422 Sayılı ÇASÖMK Çerçevesinde Uzakla Haberleşmenin Denetlenmesi , Seyfullah Edis'e Armağan, İzmir 2000, s. 249.

[971] ÖZBEK, Veli Özer : Ceza Muhakemesi Hukuku, Ankara 2006, s.419.

[972] Haberleşme hürriyeti başlıklı 17. madde aşağıdaki gibidir: 'Herkes, haberleşme hürriyetine sahiptir. Haberleşmenin gizliliği esastır. Kanunun gösterdiği hallerde, hakim tarafından kanuna uygun olarak verilmiş bir karar olmadıkça, bu gizliliğe dokunulamaz.'

alınmış temel bir haktır. Anayasamızda[973], temel haklar ve ödevler bölüm başlığı altında 22. maddede düzenlenmiş olan haberleşme hürriyeti; İnsan Hakları Evrensel Bildirgesi'nin 12., Medeni ve Siyasi Haklara İlişkin Birleşmiş Milletler Sözleşmesi'nin 17. ve Avrupa İnsan Hakları Sözleşmesinin 8. maddesiyle koruma altına alınmıştır.

İnsan haklarının gerçekleştirilmesi, adaletin sağlanması, güvenliğin temin edilmesi üzerine inşa edilen hukuk devletinde, bireylere; maddi ve manevi varlıklarını istedikleri gibi geliştirip şekillendirebilecekleri hür bir "hayat alanı" tanınması gerekir. Devletin müdahalesinden korunmuş bulunan ve " bireyin özeli" olarak anılabilecek olan bu alan, temel hak ve hürriyetler ve ülkenin siyasi rejimi bakımından hassas bir göstergedir[974]. Bu özel alanın genişliği ya da darlığı, ülkede mevcut olan siyasi rejimin hürriyetçiliği ve demokratikliği hakkında yanılmaz bir gösterge olarak görülmektedir.

Sosyal bir varlık olan insan hayatı, "genel" ve "özel" iki boyut halinde değerlendirilebilir. İnsan hayatının özel boyutu da, "özel hayat" ve "hayatın gizli alanı" olmak üzere ikiye ayrılır. Hayatın genel yönünün korunacak bir gizliliği olmamasına rağmen, hayatın özel yönü her hukuk devletinde koruma altına alınmıştır. "Özel hayat" nisbi olarak korunurken , "hayatın gizli alanı" mutlak bir şekilde korunur ve dokunulmaz olarak kabul edilir. Bu bağlamda, iletişimin denetlenmesi, Anayasa'nın 20. maddesinde düzenlenen "özel hayatın gizliliği" ve 22. maddesinde düzenlenen "haberleşme hürriyeti" ile yakından ilgilidir.

Anayasa'nın 20. maddesinde herkesin, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahip olduğu, ayrıca özel hayatın ve aile hayatının gizliliğine dokunulamayacağı önemle vurgulanmıştır. Aynı maddenin 2. fıkrasında ise milli güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlakın korunması veya başkalarının hak ve hürriyetlerinin korunması sebeplerinden biri veya birkaçına bağlı olarak, usulüne göre verilmiş hakim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; kimsenin üstünün, özel kağıtlarının ve eşyalarının

---

[973] 1982 Anayasası'na göre, kimsenin özel hayatına ve aile hayatının gizliliğine dokunulamaz (Md.20); kimsenin konutuna dokunulamaz (Md.21); herkes haberleşme hürriyetine sahiptir ve haberleşmenin gizliliği esastır(Md.22). Kanunun açıkça gösterdiği hallerde, usulüne uygun verilmiş hakim kararı olmadıkça, kimsenin üstü , özel kağıtları , eşyası ve konutu aranamaz; bu eşya ile konutta bulunan eşyaya el konulamaz ; haberleşme engellenemez ve gizliliğine dokunulamaz (Md. 20-22)

[974] ACURMAN, Hüseyin: Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi, http:// www. kocaelibarosu.org.tr/dergi/makale (İET: 15.7.2007).

aranamayacağı ve elde edilen bulgulara el konulamayacağı düzenlenmiştir[975]. Fıkranın devamında, yetkili merci kararının yirmi dört saat içinde görevli hakimin onayına sunulacağı ve hakimin, kararını el koymadan itibaren kırk sekiz saat içinde açıklaması gerektiği; aksi takdirde, el koyma işleminin kendiliğinden ortadan kalkacağı vurgulanmıştır.

Anayasa'nın "Haberleşme Hürriyeti" başlığını taşıyan 22. maddesinde ise, yine kişinin özel hayat alanını korumayı amaçlayan bir düzenleme mevcuttur. Anayasa'nın bu düzenlemesine göre; herkesin, haberleşme özgürlüğüne sahip olduğu bunun yanı sıra bu temel hakkın kullanımında gizliliğin esas olduğu belirtilmiştir. Ancak, milli güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlakın korunması veya başkalarının hak ve hürriyetlerinin korunması sebeplerinden biri veya birkaçının varlığı halinde hakim kararı ile, yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri ile kişinin haberleşme hürriyetinin engellenebileceği ve gizliliğine müdahale edileceği belirtilmiştir. Anayasa, temel hak ve hürriyetlerde genel olarak yapılacak yasal müdahalelerde olduğu gibi, burada da "hakim güvencesini" öngörmüş ve hakim dışında yetkili merci tarafından verilen kararın yirmi dört saat içinde görevli hakimin onayına sunulmasının şart olduğu, aksi takdirde haberleşme hürriyetini engelleyen kararın kendiliğinden kalkacağı düzenlenmiştir[976].

3.1.2.2.Haberleşme Hürriyetinin Kapsamı

Anayasa'nın 22. maddesinde kullanılan "haberleşme hürriyeti" kavramı, esasen "haberleşmenin gizliliği" ve "posta dokunulmazlığını" ifade etmektedir. Gazete, televizyon ve radyo gibi araçlarla yapılan kitle haberleşmesine ilişkin hürriyetlerin, burada ele alınan mektup, telgraf, telefon gibi özel haberleşmeye ilişkin hürriyetlerle doğrudan bir ilişkisi bulunmamaktadır. Anayasa'nın "haberleşme" kavramını kullanmış olması sebebiyle kamuya kapalı olarak mektup, telefon, telefaks, telgraf, çağrı cihazı, elektronik posta ve bilgisayar gibi araçlarla yapılan her türlü kişisel iletişim[977] anayasal güvence altına alınmıştır. Yeni teknolojik gelişmeler göz önüne alındığında, Anayasa'da kullanılan "haberleşme" kavramının söz konusu temel hürriyetin

---

[975] Madde, ABD Anayasasının 4. maddesiyle (Fourth Amendment) benzerlik göstermektedir. Kişilerin; üzerlerinde, evlerinde, dökümanlarında ve mallarında ancak şartların varlığı halinde ve mahkeme kararı ile arama yapılabileceği anılan maddede ifade edilmektedir. http://www.lectlaw.com/def/f081.htm) (İET:8.8.2007).

[976] Bk. ŞEN, (İletişimin Denetlenmesi Tedbiri), s.99.

[977] ŞEN, (İletişimin Dinlenmesi Tedbiri), s. 97.

korunmasını, teknik ve bilimsel gelişmelere paralel olarak dinamik bir biçimde sağlamaya uygun olduğu açıktır. Ayrıca, kişisel haberleşmenin gizliliğinin kapsamı bakımından da, söz konusu gizlilik sadece haberleşmenin içeriğini değil, aynı zamanda haberleşmenin gerçekleşme şekli, süresi, zamanı ve yerine ilişkin bilgileri de kapsamaktadır. Anayasa'da koruma altına alınan temel hak ve hürriyetlerin kullanılabilmesi için, insanın duygu, düşünce ve tutumlarını dilediği kişilerle paylaşması ve bu paylaşımı güven içinde yapabilmesi gerekir. Bu nedenle, özel haberleşme hürriyeti ve gizliliği ile; bireyin, çeşitli vasıtalarla kamuya kapalı olarak yürüttüğü duygu, düşünce ve bilgi alışverişinin üçüncü kişilerce okunmasına, dinlenmesine ve kaydedilmesine karşı bir korunma sağlanmak istenmiştir[978].

3.1.2.3.Haberleşme Hürriyetinin Sınırlanması

Küreselleşme ile birlikte hayatın bir çok yönünün (ulaşım, iletişim, ekonomi vb.) hızlanması ve çeşitlenmesinin yanında suç oranları ve nitelikleri de küresel bir boyut kazanmış, bu gelişmeler organize suç dünyasını da canlandırmış ve büyütmüştür[979]. Günümüzde devletler, son derece kompleks yapılı terörist ve organize suç örgütleri ile karşı karşıyadır. Bu düşmana karşı başarılı olabilmek için, geleneksel güvenlik yapılanmalarına yeni ve özel bazı birimlerin eklenmesi gerekmiştir. Bunun yanında suçla mücadelede kullanılan klasik yöntemlerin güçlendirilmesi ve yeni bazı tedbirlerin hayata geçirilmesi zorunluluğu duyulmuştur. Demokrasiler, zayıflık göstermeksizin ve ilkelerinden ödün vermeksizin terörizm ve diğer örgütlü suçlarla daha etkin yollarla mücadele etmek zorundadırlar[980].

Son yıllarda işlenen bazı suç türleriyle ilgili delil elde etmek son derece zor, bazen de imkansız olabilmektedir. Klasik ceza muhakemesi tedbirleri ile, bu nitelikteki suçlarla ve özellikle örgütlü suçlarla etkin mücadele mümkün olamamaktadır. Suçlular veya suç organizasyonları, özellikle başta terör amaçlı olmak üzere örgütlü olarak hareket eden gruplar, bilişim alanındaki teknolojik imkanlardan fazlasıyla faydalanmaktadırlar. Buna karşılık olarak, güvenlik görevlilerinin suçun işlenmesinden öncesini ve işlendikten sonrasını kapsayacak şekilde, suç ve suçlulukla mücadelede çağa uygun yöntemlere başvurmaları gerekmektedir[981]. Artan teknolojik gelişmeler karşısında suçla ve

---

[978] SÖZÜER, s. 72.

[979] GÜVEL, Enver Alper: Organize Suç Ekonomisi ve Hukuk Uygulaması, Ankara 2004,s. 86.

[980] POLAT, Ahmet: Fransa'da Terörizme Karşı Mücadele, Polis Dergisi, Sayı 46 Ekim-Kasım Aralık 2005, s. 204, 205.

[981] BALTACI, Vahit:Yeni TCK ve CMK'da Terör Suçları ve Yargılaması, Ankara 2007, s. 357.

suçlulukla etkin bir mücadele yürütülebilmesi için ceza soruşturmasında kullanılan yöntemlerde yeniliğe gitmek bir zorunluluk olarak ortaya çıkmıştır. Telekomünikasyon yoluyla yapılan iletişimin denetlenmesi, bu çerçevede ortaya çıkmış tedbirlerden birisidir[982]. Teknolojik ve bilimsel gelişmeler, suçların takibi ve suçluların yakalanmasında yeni kapılar açmakta, bilimsel bulgu ve tekniklerle suçların önlenmesi, takibi ve faillerin yakalanması ve cezalandırılması kolaylaşmaktadır[983].

Ulusal ve uluslararası nitelikteki tüm belgelerde yer alan haberleşme hürriyeti ile özel hayatın gizliliği hakkına, demokratik toplumda zorunlu gereksinimler çerçevesinde ve yasal düzenlemelerle birtakım sınırlamaların getirilmesi zorunludur[984]. Anayasamızın, hak ve hürriyetleri sınırlamaya ilişkin genel ilkelerin belirlendiği 13. maddesinde, 03/10/2001 tarih ve 4709 Sayılı Kanunla önemli değişiklikler yapılmıştır. Bu değişiklikten önceki hüküm "Temel hak ve hürriyetler, Devletin ülkesi ve milletiyle bölünmez bütünlüğünün, milli egemenliğin, Cumhuriyetin, milli güvenliğin, kamu düzeninin, genel asayişin, kamu yararının, genel ahlakın ve genel sağlığın korunması amacı ile ve ayrıca Anayasa'nın ilgili maddelerinde öngörülen özel sebeplerle, Anayasa'nın sözüne ve ruhuna uygun olarak kanunla sınırlanabilir. Temel hak ve hürriyetlerle ilgili genel ve özel sınırlamalar demokratik toplum düzeninin gereklerine aykırı olamaz ve öngörüldükleri amaç dışında kullanılamaz. Bu maddede yer alan genel sınırlama sebepleri temel hak ve hürriyetlerin tümü için geçerlidir" şeklindeydi. Yapılan değişiklikle söz konusu madde metni "Temel hak ve hürriyetler, özlerine dokunulmaksızın, yalnızca Anayasa'nın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabilir. Bu sınırlamalar, Anayasa'nın sözüne ve ruhuna, demokratik toplum düzeninin ve laik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamaz" şeklinde düzenlenmiştir.

Yapılan bu değişikliklerin ortaya çıkardığı sonuçlar irdelendiğinde aşağıdaki sonuçlara varılmaktadır:

---

[982] KEKLİK, Ramazan, Ceza Yargılamasında İletişimin Denetlenmesi, Adalet Dergisi, Sayı 25, s. 1.

[983] BAYRAM, Levent: "Ses ve Görüntü Kayıtlarının Türk Hukukundaki Yeri", Polis Bilimleri Dergisi, Cilt 6 (3-4), s. 2.; Avrupa Parlamentosu da 2001/2098(I INI) sayılı raporunda; yasal düzenin devamlılığı ve ulusal güvenliğin sağlanması maksadıyla denetleme faaliyetlerinin yapılabileceğini, organize suçların ve terörist faaliyetlerin eyleme dönüşmeden belirlenebilmesi amacıyla, kişi ve gruplar hakkında bilgi toplanabileceğini kabul etmektedir.

[984] ŞEN , Ersan: "Türk Hukukunda Telefonların Gizlice Dinlenmesi Sebebiyle Gündeme Gelen Hukuka Aykırılık Sorunu ve Kişi Haklarına Keyfi Müdahaleler", Prof. Dr. Sahir Erman'a Armağan, İÜHF Eğitim, Öğretim ve Yardımlaşma Vakfı Yayını No:8 İstanbul 1999,(1999), s. 729; KAYA, Abdulkadir: Adalete Erişim İçin Sürekli Mesleki Gelişim: İnsan Hakları, Boğaziçi Üniversitesi Avrupa Çalışmaları Merkezi, İstanbul 2006, s.93.

1. Bütün hak ve hürriyetler için kabul edilen genel sınırlama nedenleri kaldırılarak sadece o hak ve hürriyet için öngörülen sınırlama nedenlerine bağlılık esası getirilmiştir. Şu halde, örneğin, yerleşme ve seyahat özgürlüğünün sınırlandırılması sebepleri arasında milli güvenlik, kamu düzeni, genel ahlak gibi sebepler sayılmamıştır. Değişiklikten önce bu genel sebeplere dayanılarak da seyahat özgürlüğü sınırlandırılabilmekteyken, artık bu genel sebeplere dayanılarak yerleşme ve seyahat özgürlüğü sınırlandırılmayacak, sadece ilgili maddede belirtilen sebeplerle sınırlandırma yoluna gidilebilecektir. Bu düzenlemeyle sınırlandırma sebeplerinde önemli bir daraltma yapılmıştır.

2. Hak ve hürriyetlerin sınırlandırılması sırasında o hak ve özgürlüğün özüne[985] dokunmama ilkesi benimsenmiştir. Böylece temel hak ve hürriyetlerin kullanılmasını imkansız kılacak derecede sınırlandırmanın yapılamayacağı hüküm altına alınmıştır.

3. Anayasamızın belirlediği bir diğer yeni kriter ise "ölçülülük" ilkesidir. Çalışmamızda orantılılık olarak adlandırdığımız bu ilke; temel hak ve hürriyetlere müdahale edilmesi ile istenen amaca ulaşmak için elverişli, gerekli ve oranlı araçlara başvurulması, başka bir anlatımla, kamu yararının oluşturduğu talepler ile bireyin temel haklarının korunması gereği arasında adil bir denge oluşturulmasıdır[986].

Avrupa İnsan Hakları Sözleşmesi'nin 8. maddesine göre de, özel hayat hakkının sınırlandırılması mümkündür. Mahkemeye göre, demokratik toplumda, ulusal güvenliğin korunması, kamu düzeninin sağlanması, suçların önlenmesi gibi nedenlerle iletişimin gizlice denetlenmesine imkan tanıyan yasal düzenlemelere yer verilebilir[987].

---

[985] AİHM de, hakkın özüne dokunulmaması prensibini kabul etmiştir. Özellikle, kişisel verilerin korunması ve gizli izleme (surveillence) gibi bazı tedbirler hayata geçirilirken, devlete tanınan takdir hakkı oldukça dar tutulmaktadır. Bu yaklaşım hakkın özüne dokunulmaması ilkesinin doğal bir sonucudur.

[986] SAĞLAM, s.112-113; TEZCAN, Durmuş /ERDEM, Mustafa Ruhan/ SANCAKTAR ,Oğuz: Avrupa İnsan Hakları Sözleşmesi Ve Uygulaması, Adalet Bakanlığı Eğitim Dairesi Başkanlığı, Ankara 2004, (AİHS), s. 24.

[987] AİHM, iletişimin tespiti konusunda yapılacak yasal düzenlemelere esas olabilecek ilkeler belirlemiştir. Buna göre, sözkonusu yasal düzenlemelerin özel yaşama ve aile yaşamına saygı gösterilmesi ilkesine bir müdahale niteliği taşıdığı açıktır. Burada asıl sorun, müdahalenin haklı olup olmadığıdır. Bu noktada uygulanacak kriter ise, gizli denetlemenin ancak demokratik kurumların korunması amacı ile zorunlu olmasıdır.Bu aynı zamanda orantılılık ilkesinin bir gereğidir. Yani ulusal güvenliğin korunması, kamu düzeninin sağlanması ve suçların önlenmesine yönelik olarak getirilen sınırlamalar ancak bu amaca ulaşmak için benimsenen araçların demokratik toplum için zorunlu olup olmamasına göre meşruiyet kazanacaktır. Hemen her devlet karmaşık casusluk olayları ve terör tehdidi altında bulunmaktadır. Devletin bunlarla etkin bir şekilde mücadele edebilmesi ülkesinde faaliyette bulunan yıkıcı faaliyetleri gizlice gözetleme yeteneğine sahip olmasına bağlıdır. Bu sebeple demokratik bir toplumda, ulusal güvenliğin korunması, kamu düzeninin sağlanması ve suçların önlenmesi içi haberleşmenin gizlice denetlenmesine olanak veren yasal düzenlemeler bir zorunluluktur. Bununla birlikte devletlere tanınan bu imkan sınırsız değildir. Çünkü demokrasiyi korumak amacıyla çıkarılan ve haberleşme özgürlüğünü sınırlayan böyle bir düzenleme demokrasi

Bu bağlamda, hakka yapılacak müdahalenin koşulları kanun tarafından açıkça belirtilmeli ve yapılacak müdahaleler, meşru bir amacın elde edilmesine yönelik olmalıdır[988]. AİHM, Sözleşmenin 8. maddesinin getirdiği koruma alanını değerlendirirken iki önemli olguya işaret etmiştir. Bunlardan birincisi, casuslukta ve karşı izleme araçlarında meydana gelen teknik ilerlemedir. İkincisi ise, son yıllarda Avrupa'da terörün ilerlemesidir. Demokratik toplumlar, son zamanlarda kendilerini casusluğun ve terörizmin hayli gelişmiş biçimlerinin tehdidi ile karşı karşıya bulmuşlardır. Bu da devletlerin bu tür tehditlere karşı etkin bir şekilde mücadele edebilmek için kendi egemenlik alanı içinde faaliyet gösteren yıkıcı unsurları gizli izlemeye almasını gerektirmiştir[989]. Nitekim, bu tür suçlar, başta hayat hakkı olmak üzere temel hak ve hürriyetlerin yok edilmesine yönelik eylemlerdir[990].

Sözleşme'de geçen yasal düzenleme maddi anlamdadır. Dolayısıyla, kanun kavramına yazılı ve yazılı olmayan tüm hukuk kuralları dahildir[991]. Ancak bu metinlerin kanun niteliğini alabilmeleri için, kişilerin erişimine açık ve ulaşılabilir olmaları gerekmektedir[992]. Ayrıca bu düzenlemelerin kanun niteliğini kazanabilmeleri için iki unsurun daha bulunması gerekmektedir. Bunlardan ilki, bu düzenlemelerin yeterince açık ve kesin hükümler taşımaları gereğidir[993]. Böylelikle, bu tedbirlerin ilgililer tarafından kötüye kullanılmasının önüne geçilecektir. İkincisi ise, öngörülebilirlik[994] unsuru olup, buna göre, kişiler belirli koşullar altında belirli bir hareketin ne tür sonuçlar doğurabileceğini makul bir şekilde kestirebilmelidirler. Yasal düzenlemede; tedbir kapsamında toplanacak bilgilerin nelerden ibaret olduğu ve bunların açıklanması, hakkında bilgi toplanacak kişilerin tanımının yapılması , elde edilecek bilgilerin ne kadar

---

adına tehlikeyi de beraberinde getirmektedir.Bu sebeple haberleşmenin denetlenmesine imkan veren düzenlemelerin yanı sıra bu hususun kötüye koullanılmasını engelleyecek ve aynı şekilde yaptırım altına alan düzenlemelere ihtiyaç vardır. (Bk.KLASS-ALMANYA; ÖZTÜRK/ERDEM/ÖZBEK, s.680; GÖZÜBÜYÜK , A. Şeref: Avrupa İnsan Hakları Komisyonu Kararlarından Seçme Özetler,İHMD, Ocak 1995, C.III, S.1, s. 35; ANAYURT, s. 51; KILKELLY, s. 25-26; TEZCAN/ERDEM/SANCAKTAR, s. 237.)

988 KOYUNCU, Tuğçe: Telekomünikasyon Yoluyla Yapılan İletişimin Tespiti, Hukuk Gündemi Dergisi, CMK Dosyası, s. 77;KAYA, s. 93.

989 DİNÇ, Güney: Sorularla Avrupa İnsan Hakları Sözleşmesi, Türkiye Barolar Birliği, Mayıs, 2006, s. 420.

990 BEŞE, Ertan: Terörizm, Avrupa Birliği ve İnsan Hakları, Ankara 2002, s. 151.

991 ERGEÇ, s. 161; DUTERTRE, s. 260; MALONE-BİRLEŞİK KRALLIK, Pr.66; SUNDAY TIMES-BİRLEŞİK KRALLIK, Pr.46-47.

992 ALCARAZ, s. 229; ERGEÇ, s. 161; ŞEN, (İletişimin Denetlenmesi Tedbiri), s.99; ÇOKSEZEN.s.5; SUNDAY TIMES-BİRLEŞİK KRALLIK, Pr.49.

993 TEZCAN/ERDEM/SANCAKTAR, s. 238; KILKELLY, s. 25.; RENUCCI, 135; KAYA, s. 92.

994 ALCARAZ, s. 229; ŞEN, (İletişimin Denetlenmesi Tedbiri), s.99.

süreyle saklanacağı ve ne amaçla kullanılacağının açıkça belirtilmesi gerekmektedir. Öngörülebilirlikle birlikte kişi, devletin hangi şartlar altında tedbire başvurduğu hakkında fikir sahibi olacaktır. Doğal olarak da her kanun karar merciine belirli oranda takdir yetkisi verecektir. Ancak, takdir yetkisi keyfilik doğurmayacak sınırlar içinde olmalıdır.[995]

Bu ilkeler ışığında, Türk hukukunda iletişimin denetlenmesine ilişkin hükümler hem Anayasa'da hem de 5271 sayılı CMK ve 5397 sayılı kanunda ayrıntılı olarak düzenlenmiş ve bu düzenlemelere paralel yönetmelikler de çıkarılmıştır. Yapılan bu kanunların, AİHS'nin 8. maddesinde yer alan şartı karşılaması bakımından önemli olduğu kanaatindeyiz. Nitekim, iletişimin denetlenmesi konusunun hukukumuzda düzenlenmesi sürecinde AİHS ve AİHM içtihatları dikkate alınmıştır. Diğer ülkelerin negatif tecrübeleri olan ihlal kararlarından pozitif sonuçlar çıkarılması takdire şayandır. Gerçekten de, gerek 5271 sayılı gerekse 5397 sayılı kanunlar, bu konuda daha önce verilmiş AİHM kararlarındaki ilkeler dikkate alınarak hazırlanmıştır. 5271 sayılı CMK hazırlanırken, Fransa Ceza Usul Kanunu'nun iletişimin denetlenmesine ilişkin düzenleme yapan 100. maddesi örnek alınmıştır. Bu tür bir çalışma oldukça yararlı olmuştur. Bu konuda AİHM'nin Ülkemiz aleyhine verdiği kayda değer bir karar bulunmamasına rağmen, AİHS ve AİHM'nin bu hususstaki anlayışının irdelenmiş olması, ileride Strasbourg Mahkemesi'ne götürülebilecek şikayetler bakımından olumlu bir adımdır. Bununla birlikte, teknolojik gelişmeler hususunda Avrupa'dan daha ileri bir noktada olduğu tartışma götürmeyen ABD'nin bu konudaki kanunlarının ve mahkeme kararlarının değerlendirmeye alınmamış olmasının bir eksiklik olduğunu düşünüyoruz. Nitekim, ulusal boyutu da aşarak global düzeyde bilgi toplayan bu ülkenin çalışmalarının dikkate alınması, gelecekte karşımıza çıkacak bazı problemlerin önceden bertaraf edilmesi bakımından yararlı olurdu.

3.1.3.765 Sayılı Türk Ceza Kanunu'nda İletişimin Denetlenmesine İlişkin Hükümler

Mülga 765 sayılı Türk Ceza Kanunu (TCK), kişinin özel hayat hakkı ve ona sıkı sıkıya bağlı diğer temel hak ve hürriyetleri yeterli olarak koruyamamakta ve onlara yönelen tecavüzlere engel olamamaktaydı. Bunun temel sebeplerinden biri , 765 sayılı TCK'nın yürürlüğe giriş tarihinden sonra bilim ve teknolojinin akıl almaz bir şekilde ilerlemiş ve temel hak ve hürriyetlere yönelik saldırıların sayı ve yöntemlerinin artmış olmasıydı. Anılan nedenlerle, 765 sayılı TCK hükümleri ihtiyaca cevap veremez duruma gelmişti.

[995] ALTIPARMAK, s.37-38; KAYA, 93.

Diğer bir sebep ise, bahse konu kanunun 1. maddesinde kabul edilen 'suçta ve cezada kanunilik ilkesi' gereği, ancak kanunda suç olarak düzenlenen fiilerin cezalandırılabilmesiydi[996].

765 sayılı TCK'nın 195. maddesi ve devamındaki hükümler haberleşme hürriyetinin bozulmasını ve gizliliğin ihlalini ve mesleki sırların açıklanmasını birer cürüm olarak düzenlemişti. Bu hükümler, insan hak ve hürriyetlerini karşı karşıya olduğu tehlikelerden korumaya yeterli değildi. Örneğin hükümet karşıtı bir gazeteci veya siyasetçinin telefonlarının gizlice dinlenmesi suretiyle onun hak ve hürriyetlerinin ihlal edilmesi durumunda mevcut yasal düzenlemeler yetersiz kalmaktaydı. Söz konusu eylemlerde bulunan kişilerin kendisine veya başkasına maddi bir çıkar sağlamak için bu eylemleri gerçekleştirdiği somut olarak tespit edilemezse, cezai müeyyidenin uygulanması mümkün değildi[997].

765 sayılı TCK'da bireylerin arasındaki özel konuşmaların, kanunda öngörülen koşullar oluşmadan ve hakim kararı olmaksızın gizlice dinlenip kaydedilmesi suretiyle haberleşme hürriyetine ve kişisel haklara müdahale edilmesi açıkça suç olarak kabul edilmediği için, TCK'nın vazgeçilmez prensibi olan "suçta ve cezada kanunilik ilkesi" nedeniyle, fiil hukuka aykırı olsa bile cezasız kalmaktaydı.

3.1.4.1412 Sayılı Ceza Muhakemesi Usulü Kanunu Döneminde İletişimin Denetlenmesi

Haberleşmenin denetlenmesi yoluyla delil elde edilmesi konusuna Türk hukuk sisteminde ilk açık düzenleme 4422 sayılı Çıkar Amaçlı Suç Örgütleriyle Mücadele Kanununda yer verilmiştir. Bu tarihten önce doğrudan ve açıkça önleme amaçlı iletişimin dinlenmesine ilişkin yetki veren bir hüküm yer almıyordu[998]. 4422 sayılı Kanun yürürlüğe girinceye kadar, arama ve el koymaya ilişkin hükümler kıyas yoluyla uygulanarak telekomünikasyon yoluyla yapılan iletişim denetlenebiliyordu[999]. Mülga 1412 sayılı CMUK'un, özellikle elektronik ve mekanik araçlarla elde edilen delillerin hukuka uygunluklarını belirlemek konusunda oldukça geri olduğu ve yeni düzenlemelere ihtiyaç olduğu dile getiriliyordu. Özellikle haberleşme hürriyeti açısından

---

[996] ŞEN, s. 516.

[997] ŞEN, s. 516.

[998] ÜNVER, Yener/ HAKERİ, Hakan :Sorularla Ceza Muhakemesi Hukuku, TBBD,Ankara Mayıs 2006, s. 188.

[999] KUNTER/ YENİSEY/NUHOĞLU, s. 697.; ŞEN, (İletişimin Denetlenmesi Tedbiri), s. 103.

CMUK'un 91. maddesi ile yetinilmiş ve 1982 Anayasası'nın ortaya koyduğu hükümlere uygulanabilirlik getiren düzenlemelere yer verilmemişti[1000]. Diğer taraftan, iletişimin denetlenmesi hakkında açık bir hüküm bulunmamasından kaynaklanan boşluğun kıyas ya da yorumla doldurulabileceğini savunanlar olduğu gibi, her iki yolun da uygulanamayacağını iddia edenler de bulunmaktaydı.

Bir görüş, 1412 sayılı CMUK'un 91. maddesinde yer alan, postada el koyma ile ilgili hükümlerin kıyas yolu ile telefonla yapılan iletişimin denetimi için de uygulanabileceğini dile getirilmekteydi[1001]. Başka bir görüş ise, iletişimin tespit ve denetimi konusunda CMUK'un 92/2. maddesinde yer alan " sair mersule" kavramından yararlanmaya çalışmaktaydı. Buna göre burada kıyas yolu ile değil ancak geliştirici yorum yapılarak "sair mersule" teriminin, telefon teleks, bilgisayarlı iletişim sistemleri gibi araçlarla yapılan iletişimi de içine alacak bir şekilde yorumlanması gerektiği belirtiliyordu[1002]. Bir diğer görüşe göre ise , mevcut yasal düzenlemeler karşısında telefonla yapılan iletişimin tespiti bakımından ne kıyas ne de genişletici yorum yapılması mümkün değildi. Buna göre, iletişime müdahalenin koşullarını kanun açıkça öngörmeli ve bu temel hakka müdahale devlete ait somut ve belirli bir çıkar için zorunlu olmalıydı. Bu bağlamda farklı görüşlerin hakim olduğu bir dönemde 4422 sayılı kanunun yürürlüğe girmesi isabetli kabul edilmekteydi[1003]. Bununla birlikte, belli birtakım suçlar için öngörülmüş bir yasa olan 4422 sayılı kanun da, o dönemde var olan problemlere çözüm getiren bir yol olamadı.

3.1.5.4422 Sayılı Çıkar Amaçlı Suç Örgütleriyle Mücalele Kanunu'nda (ÇASÖMK) İletişimin Denetlenmesi

Türk hukukunda iç hukuka ilişkin düzenlemelerin AİHS'ye uyumlu hale getirilmesi amacıyla iletişimin denetlenmesi tedbiri ilk olarak, 4422 sayılı Çıkar Amaçlı Suç

[1000] GÖKÇEN, s. 188.

[1001] TOSUN,(Gizli Dinleme), s. 99; Akmanlar, Bülent: Avrupa Konseyi Üyesi Bazı Devletlerde Telefon Konuşmalarının Dinlenmesi ve Telekominikasyonun Kaydedilmesi, YD,1982/4,s.670;YURTCAN, s.350;YENİSEY, Feridun Ceza Muhakemesi Hukukunda Kovuşturma Mecburiyeti, (Hazırlık Soruşturması), Ankara 1991, no.244, s.478; ŞEN, Ersan: Devlet Ve Kitle İletişim Araçları Karşısında Özel Hayatın Gizliliği ve Korunması,İstanbul 1996,(1996) s. 151.

[1002] ÖZTÜRK, (Hazırlık Soruşturması), s.116;GÖKCEN,s. 176.

[1003] Cihan/YENİSEY, s, 258; CENTEL, Nur: Koruma Tedbirlerindeki Gelişmeler, Hukuk Araştırmaları Dergisi 1994, s. 77; KAYMAZ, Seydi: Mevcut Yasal Düzenlemeler Karşısında Telefon İle Yapılan Haberleşmenin Denetlenmesi, İstanbul Barosu Dergisi, Sayı 1, İstanbul 1996, s. 797; ÖZTÜRK/ERDEM/ÖZBEK, s.679.

Örgütleriyle Mücadele Kanunu'nda[1004] açıkça hükme bağlanmıştır. Bu maddede yer alan hükümlerin, Sözleşmenin 8. maddesinde vurgulanan ilkelere yakın bir düzenleme olduğu söylenebilir[1005]. Ancak, bu kanunda da, adli ve önleyici amaçlı iletişimin denetlenmesi ayırımı yeterli ve açık şekilde belirtilmemiştir. Kaldı ki, bu Kanun sadece çıkar amaçlı suç örgütleriyle mücadele amacıyla çıkartılmış olup diğer suçların önlenmesine ilişkin uygulama alanı oldukça sınırlıdır[1006].

4422 sayılı Kanunun 2 . maddesinde; bu kanunda öngörülen suçları işleme, bunlara iştirak, faillere yardım, aracılık ve yataklık etme kuşkusu altında bulunan kişilerin iletişimlerinin dinlenebileceğini hükme bağlanmaktaydı. Bununla beraber, bir süre 4422 sayılı Kanunun 2. maddesine dayanılarak önleme amaçlı iletişimin dinlenmesine de kararlar verilmiştir. Ancak bu hükümlere dayanılarak önleme amaçlı iletişimin dinlenmesine karar verilmesinin, hükmün çok geniş yorumlanması olduğu da muhakkaktır.

3.1.5.1.Tedbire Başvurma Şartları

Türk hukuk sistemi bakımından iletişimin denetim altına alınmasına yönelik ilk düzenleme, 4422 sayılı Çıkar Amaçlı Suç Örgütleriyle Mücadele Kanunu'nun 2.maddesi ile getirilmiştir[1007]. Bu kanundaki yasal düzenlemeye göre iletişimin dinlenmesi ve tespiti için kuvvetli belirtiler ve makul şüphenin var olması ile başka bir tedbir ile faillerin belirlenmesi, ele geçirilmesi veya suç delillerinin elde edilmesinin mümkün olmaması gerekmekteydi[1008]. Hakim kararı bulunmadıkça, elde edilen veriler

---

[1004] Kabul tarihi: 30.07.1999, R.G., 01.08.1999, S. 23773.

[1005] ALTIPARMAK, s. 41.

[1006] 4422 sayılı Kanunun 16. maddesi şu şekildeydi: "Bu Kanunun 2 ila 10 uncu maddeleri, Terörle Mücadele Kanunu kapsamına giren suçlarla, 21/7/1983 tarih ve 2863 sayılı Kültür ve Tabiat Varlıklarını Koruma Kanunu, 10/7/1953 tarih ve 6136 sayılı Ateşli Silahlar ve Bıçaklar ile Diğer Aletler Hakkında Kanun ve Türk Ceza Kanununun 403, 404 ve 406 ncı maddelerinde yer alan suçlar teşekkül halinde işlendiğinde de uygulanır".

[1007] Bu tür yasal düzenlemeler, hemen bütün Avrupa ülkelerinde vardır. Alman Anayasası'nın 10 uncu maddesi "haberleşme özgürlüğü" nün nasıl kısıtlanacağını ayrıntılı olarak düzenlemiştir. Almanya'da ayrıca 'Zur Neuregelung von Beschraenkungen des Brief-Post und Fernmeldegeheimnisses' isimli kanun konu ile ilgili düzenleme yapılmıştır. Fransa da ise, "Telekomünikasyon Yolu ile Yapılan Haberleşmenin Mahremiyetine İlişkin" kanun (10 Temmuz 1991 tarihli ve 91-646 sayılı) terörizm, örgüt suçları gibi suçları ortaya çıkarmak amacı ile telekomünikasyon vasıtası ile yapılan haberleşmeye istisnai olarak müdahale yetkisi vermektedir. (ÖZTÜRK/ERDEM/ÖZBEK, s. 629.; ANAYURT, s. 53).

[1008] YENİSEY, Feridun, "Çıkar Amaçlı Suç Örgütleri İle Mücadele Yöntemleri", Hukuk Kurultayı 2000, Ocak 2000, Ankara,(Kurultay) s.350; MIHÇAK, Muhittin :Çıkar Amaçlı Suç Örgütleri ve Cürüm İşlemek İçin Teşekkül Oluşturmak Suçları, Ankara 2003, s.55;ÇOŞKUN, Atilla: Örgütlü Suçlar Ve Çıkar Amaçlı Suç Örgüleri İle Mücadele Kanunu, Ankara 2002, s. 82-83; ALTIPARMAK, s.42.

hukuka aykırı delil sayılamayacak ve yargılama süresince dikkate alınamayacaktı[1009]. Ancak gecikmesinde sakınca bulunan durumlarda Cumhuriyet savcısı da bu tedbirin uygulanmasına karar verebiliyordu. Hakim kararı olmaksızın verilen bu tedbir kararının yirmi dört saat içinde hakim kararına bağlanması zorunluydu. Söz konusu tedbirde yirmi dört saatlik süresinin dolması veya hakim tarafından aksine bir karar verilmesi halinde, bu tedbir Cumhuriyet savcısı tarafından derhal kaldırılıyordu. 4422 sayılı kanun çerçevesinde iletişimin denetlenmesine karar verecek olan hakim, yetkili Devlet Güvenlik Mahkemesi'nin 1 numaralı dairesinin yedek üyesiydi[1010]. Daha sonra yapılan değişikliklerle Devlet Güvenlik Mahkemeleri'nin yerini geniş yetkili ağır ceza mahkemeleri aldı.

3.1.5.2.Süre

İletişimin tespiti ve dinlenmesine en fazla üç aylık bir süre için karar verilebilirdi. Bu süre en fazla iki defa üç aydan fazla olmamak üzere uzatılabilirdi. Sürenin başlangıcı, kararın kolluğa tebliğ edildiği tarihti. Ancak verilen ek süreler de dahil olmak üzere, söz konusu sürenin kısa olduğu dile getiriliyordu. Uluslararası örgütlerde faaliyet alanı geniş olduğundan verilen süreler yetersiz kalmaktaydı. Bu yetersizlik nedeniyle elde edilen bilgilerdeki kopukluk, delillerin etkisiz kalmasına neden olmaktaydı[1011].

3.1.5.3.Tedbire Konu Olan Suçlar

4422 sayılı kanunda özel tedbire başvurulacak suçlar bakımından katalog tarzı bir çözüm öngörülmediği gibi, suçların ağırlığına göre bir ayrıma da yer verilmemişti. Söz konusu tedbir, 4422 sayılı kanunun 2. maddesinde sadece ilgili kanun kapsamında yer alan örgütlü suçlar bakımından uygulama alanı bulmaktaydı[1012]. Buna karşın, bu kanunda yer almayan suçlar bakımından ise, 1412 sayılı CMK'nın 91 ve 92/2. maddeleri temel alınarak kıyas[1013] ve genişletici yorum[1014] ile bu tedbire

---

[1009] ŞAFAK, Ali: Suç Organizasyonu Ve Kovuşturma Usulü, Temmuz 2003, s.93;YENİSEY, (Kurultay), s.350.

[1010] YENİSEY, (Kurultay), s.350.

[1011] YENİSEY, (Kurultay), s.350; MIHÇAK, s.57.

[1012] ÖZBEK, s.418; ŞAFAK, s.94.

[1013] TOSUN,(Gizli Dinleme), s.99; AKMANLAR, s. 670; YURTCAN, s. 350; ŞEN, (1996), s. 151.

[1014] ÖZTÜRK, (Hazırlık Soruşturması), s.116; GÖKCEN,s.176.

başvurulabileceğinin mümkün olduğunu ileri süren görüşlerin yanı sıra, kıyas ve genişletici yorum yoluyla dinlenmenin hukuka aykırı olduğunu savunanlar da vardı[1015].

3.1.5.4.Tedbire Konu Olan İletişim Araçları

4422 sayılı kanunun 2. maddesinde "bu kanunda öngörülen suçları işleme veya bunlara iştirak yahut işlendikten sonra faillere her ne surette olursa olsun yardım ve aracılık veya yataklık etme kuşkusu altında bulunan kimselerin kullandıkları telefon, faks ve bilgisayar gibi kablolu, kablosuz veya diğer elektromanyetik sistemlerle veya tek yönlü sistemlerle alınan veya iletilen sinyalleri, yazıları, resimleri, görüntü veya sesleri ve diğer nitelikteki bilgileri dinlenebilir veya tespit edilebilir" şeklinde iletişimin denetimi hüküm altına alınmıştı[1016].

4422 sayılı kanun, hangi tür iletişim araçlarının denetlemeye tabi olacağını tek tek sayma yoluna gitmişti. Ayrıca her ne kadar 2. maddede "dinleme ve tespit etme" kavramından söz edilmekte ise de, bunun iletişimin kaydedilmesini de içerip içermediği madde içeriğinden açıkça anlaşılamıyordu. Bundan başka kanunun aynı maddesinin dördüncü fıkrasında "resmi veya özel her türlü iletişim kuruluşlarının tuttukları, iletişimin içeriği dışında kalan kayıtlar hakkında da yukarıdaki hükümler uygulanır " denilmek suretiyle "dış veriler" bakımından da "kuvvetli belirtilerin varlığı" ve başka bir tedbirle failin belirlenmesi, ele geçirilmesi veya suç delillerinin elde edilmesinin mümkün olmaması şartı aranmaktaydı. Kişinin Anayasa ile teminat altına alınan iletişim özgürlüğüne, iletişimin denetlenmesinden daha az önemli sayılamayacak bir müdahale oluşturan dış veriler hakkında, 2. maddenin takip eden fıkralarında yer alan, tedbire kimin karar vereceği, tedbirin süresi,sona ermesi ve elde edilen delillerin yok edilmesine ilişkin hususların uygulanamaması eleştirilmekteydi[1017].

3.1.5.5.Tedbire Konu Kişiler

4422 sayılı kanunla yapılacak iletişimin denetlenmesi tedbirine, kanunda öngörülen suçları işleme şüphesi altında bulunan kişiler bakımından başvurulması kabul edilmişti. Ayrıca, suç işleme şüphesi altındaki şüphelinin yanı sıra, suça iştirak etme, suç işlendikten sonra yardım, aracılık veya yataklık faaliyetlerinde bulunanlar bakımından

---

[1015] CİHAN/YENİSEY, s,258; CENTEL, Nur: Koruma Tedbirlerindeki Gelişmeler, Hukuk Araştırmaları Dergisi 1994, s. 77; ÖZTÜRK/ERDEM/ÖZBEK, s.679 ; KAYMAZ, s. 797-800.

[1016] ÜNVER , Naci : Çıkar Amaçlı Suç Örgütleri ve Cürüm İşlemek İçin Teşekkül Oluşturmak,Ankara 2001, s. 14; KÖROĞLU, Hasan : Örgütlü Suçluluk , Ankara 2001, s. 64; ÇOŞKUN, s. 86.

[1017] ÖZTÜRK/ERDEM/ÖZBEK, s.679;

da bu tedbire başvurulabiliyordu. Ancak hakkında tedbir uygulanamayacak kişilerle ilgili herhangi bir düzenleme bulunmamaktaydı[1018]. Oysa ki, mülga 1412 sayılı CMUK'un 89. maddesinde, el koymaya ilişkin olarak tanıklıktan çekinme hakkına sahip olan kişiler ile sanık arasında yapılan mektuplaşmaların denetlenemeyeceği öngörülmesine karşın buna paralel bir düzenlemenin olmayışı eksiklik olarak görülüyordu[1019].

Diğer yandan, iletişimin denetlenmesi tedbirinin müdafii bakımından uygulanıp uygulanmayacağı hususu da bir başka eleştiri konusuydu. Mülga 1412 sayılı CMUK'un 144. maddesine göre, yakalanan ve tutuklu bulunan kişilerin müdafii ile yazışmaları denetime tabi tutulamıyordu. Bu kapsamda bu maddede yer alan "yazışmalar" tabiri ile aynı maddenin birinci cümlesinde yer alan "yakalanan veya tutuklu bulunan kişi, vekaletname aranmaksızın müdafii ile her zaman ve konuşulanları başkalarının duyamayacağı bir ortamda görüşebilir" hükmü birlikte değerlendirildiğinde müdafii ile bu kişiler arasındaki telefon görüşmelerinin kontrolünün de mümkün olmaması gerektiği dile getiriliyordu[1020].

3.1.6. 5271 Sayılı Ceza Muhakemesi Kanununda İletişimin Denetlenmesi

5271 sayılı Ceza Muhakemesi Kanunu, Türk Hukukunda adli amaçlı iletişimin denetlenmesine ilişkin hükümlerin ihdas edildiği temel kanundur. Çalışmamızın temel kısımlarından biri olan adli amaçlı iletişimin denetlenmesi aşağıda detaylı bir şekilde anlatılacaktır.

3.1.7. 5237 Sayılı Kanunla Getirilen Değişiklikler

5237 sayılı Kanun, Türk Hukukunda önleme amaçlı iletişimin denetlenmesine ilişkin hükümler getirmiştir. Bu bölüm aşağıda detaylı olarak anlatılacaktır.

3.2.Türk Hukukunda Adli Amaçlı İletişimin Denetlenmesi

3.2.1.Genel Olarak

2004 yılında çıkarılan 5271 sayılı Ceza Muhakemesi Kanunu'nun (CMK) 135-138. maddelerinde iletişimin denetlenmesi, bir koruma tedbiri olarak detaylı ve açık olarak düzenlenmiştir. CMK'nın 135. maddesinin 7. fıkrasında bu madde hükümleri dışında

---

[1018] ŞAHİN, Cumhur: Ceza Muhakemesi Şerhi, Ankara 2006, s. 86-87.

[1019] ERDEM/ÖZBEK, s. 272.

[1020] YURTCAN, Erdener: CMUK Ceza Yargılaması Hukuku 1992 Değişiklikleri, İstanbul 1992,(1992), s.29; YENİSEY, Feridun : CMUK Eki, 3842 Sayılı Kanunla Yapılan Değişiklikler ve Zabıtayı İlgilendiren Maddeler , İstanbul 1993, (CMUK Eki), s. 38.

başka bir şekilde iletişimin denetlenmesinin uygulanamayacağı açık şekilde ifade edilmiştir. CMK'da düzenlenen iletişimin denetlenmesi tedbiri, sadece bir suç işlendikten sonra başka yollarla ulaşılamayan delillerin elde edilmesi amacıyla başvurulabilecek bir tedbir olarak yer almıştır[1021].

Adli amaçlarla iletişimin denetlenmesi tedbirine başvurabilmek için gerekli olan şartlar CMK'da düzenlenmiştir. Bu şartlar, anılan kanunun 135. maddesinde, "bir suç dolayısıyla yapılan soruşturma ve kovuşturmada, suç işlendiğine ilişkin kuvvetli şüphe sebeplerinin varlığı ve başka suretle delil elde edilmesi imkânının bulunmaması durumunda, hâkim veya gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısının kararıyla şüpheli veya sanığın telekomünikasyon yoluyla iletişimi tespit edilebilir, dinlenebilir, kayda alınabilir ve sinyal bilgileri değerlendirilebilir" şeklinde ifade edilmiştir.

İletişimin denetlenmesi ile ilgili CMK hükümleri, kişi merkezli bir yaklaşım tespit etmiştir. Son çare olarak başvurulması gerekli olan bir tedbir olması nedeniyle bu tedbirin uygulanması birtakım şartların varlığına bağlanmıştır. Bu şartların varlığı halinde de, şartlara uyan sanık ya da şüphelilerin iletişimlerinin denetlenmesine izin verilmiştir. Bu bağlamda; sabit telefon, mobil telefon, faks, İnternet, teleks gibi iletişim araçlarının yanı sıra[1022] şüpheli veya sanık tarafından kullanılan jetonlu veya ankesörlü telefonlar üzerinden kurulan iletişimin denetlenmesi de mümkündür[1023]. Özel ya da resmi her türlü iletişim kuruluşunca tutulan iletişimin içeriğine ilişkin kayıtlar hakkında da iletişimin denetlenmesi kararı alınabilir. Öte yandan, iletişimin denetlenmesi kararı, kişilerin yurt dışı bağlantılı iletişimini de kapsar[1024]. İletişim aracının şüpheli ya da sanığın evinde veya işyerinde olması tedbirin uygulanması açısından bir önem taşımaz[1025]. İşyeri kavramına, kamu kuruluşları da girmektedir. Başka bir anlatımla, kişinin kamu kuruluşundaki bir vasıta aracılığıyla kurduğu iletişim hakkında da bu tedbir kararı uygulanabilir.[1026] Bununla birlikte, posta ya da telgraf ile yapılan iletişim, niteliği gereği CMK'nın 135 vd. maddelerine göre denetlemeye tabi tutulamaz[1027].

[1021] ŞEN, (İletişimin Denetlenmesi Tedbiri), s. 104.

[1022] ÖZBEK, s. 422.

[1023] KUNTER/YENİSEY/NUHOĞLU, s. 699.

[1024] 14.2.2007 tarihli Yönetmelik.

[1025] CENTEL, Nur/ZAFER, Hamide: Ceza Muhakemesi Hukuku, 4. Bası,İstanbul 2006, s. 365.

[1026] YİĞİT, Nuri, Arama, Elkoyma ve Gizli Koruma Tedbirleri, Adalet Bakanlığı Seminer Notları, Ankara 2005, s. 15, 23 .

[1027] KUNTER/YENİSEY/NUHOĞLU, s. 702.

Hukukumuzdaki bu yaklaşımın AİHM içtihatlarıyla uygunluk arzettiği düşüncesindeyiz. Mahkeme, iletişim kavramını belli bir iletişim aracı belirtmek suretiyle daraltmak yerine, geniş bir bakış açısı kabul etmek şeklinde bir tercih yapmıştır. Nitekim, 8. maddenin 1. paragrafında açıkça zikredilmemesine rağmen, telefon görüşmelerinin, teleksin ve posta yoluyla gönderilen malzemelerin haberleşmenin kapsamına girdiğini kabul eden AİHM, haberleşme kavramını, teknolojik gelişmelere ayak uyduracak ve elektronik posta gibi diğer yöntemleri de içerecek şekilde geniş tutma eğilimindedir[1028].

CMK öncesinde, yani, bu tedbirin kıyas ya da yorumla uygulandığı dönemlerdeki mevzuat ve uygulamamızın AİHS ve AİHM kriterlerine uygun olmadığı aşikardı. Bugünse artık, gerek sözleşme gerekse mahkeme kriterlerine uygun mevzuat[1029] marifetiyle iletişimin denetlenmesi tedbiri uygulanmaktadır. CMK ile getirilen sistemin AİHM kriterlerine genel olarak uygunluk sağladığı söylenebilir. Bununla birlikte, iletişimin denetlenmesi ile ilgili hususları düzenleyen bir kanunun varolması yalnız başına yeterli değildir. Bu görüşün bir ifadesi olarak AİHM, iletişimin denetlenmesine ilişkin bir kanunun varlığını yeterli bulmamış ve Huvig ve Kruslin davalarında Fransa'yı[1030] mahkum etmiştir. Mahkemeye göre, kanunun varlığı kadar niteliği de önemlidir. Birtakım güvenceleri barındırmayan sistemimiz, Strasbourg Mahkemesi tarafından eksiklikle itham edilebilecek niteliktedir. Eksiklik olarak dile getirilebilecek en önemli konu denetim sistemidir. Eleştiri konusu olabilecek eksiklikler ve getirilecek öneriler aşağıda anlatılacaktır.

3.2.2.Kavramlar ve İletişim Türleri

İletişimin denetlenmesi tedbiri konusunda kullanılan kavramların ve türlerin bilinmesi, tedbirin amaç ve kapsamının belirlenmesi bakımından önem taşımaktadır. Çünkü, söz konusu kavramların nasıl yorumlandığı, tedbirin kapsamını daraltıcı ya da aksine genişletici sonuca ulaşılmasına neden olabilir.

[1028] KILKELLY, s. 20; RENUCCI, Jean François: Droit Européen Des Droit De L'Homme, İkinci baskı, 2001, s.135.

[1029] Yapılan son mevzuat değişiklikleri sonrasında, hem adli amaçlı iletişimin denetlenmesine hem de önleme amaçlı iletişimin denetlenmesine ilişkin düzenlemeler AİHM ve AİHS kriterleri anlamında kanun niteliğindeki normlarla düzenlenmiş bulunmaktadır. Aralarında Malone- Birleşik Krallık (Pr. 66) ile Silver ve diğerleri-Birleşik Krallık (Pr .86) davalarının da bulunduğu birçok davada, müdahalenin kaynağını milli hukuktan alması gerektiği ifade edilmektedir.

[1030] Bk.ENGUÉLÉGUÉLÉ, /LOURDEL ("Three Recent Arguments For The Expansion Of Human Rights In French Criminal And Administrative Law")

3.2.2.1.Telekomünikasyon Kavramı

Telekomünikasyon kavramı[1031], 10.11. 2005 tarihli Telekomünikasyon Yoluyla Yapılan İletişimin Tespiti, Dinlenmesi, Sinyal Bilgilerinin Değerlendirilmesi ve Kayda Alınmasına Dair Usul ve Esaslar ile Telekomünikasyon İletişim Başkanlığının Kuruluş, Görev ve Yetkileri Hakkında Yönetmelikte[1032] "Her türlü işaret, sembol, ses ve görüntünün ve elektrik sinyallerine dönüştürülebilen her türlü verinin kablo, telsiz optik, elektrik, manyetik, elektromanyetik, elektro kimyasal, elektro mekanik ve diğer iletim sistemleri vasıtasıyla iletilmesi, gönderilmesi ve alınmasını ifade eder" şeklinde tanımlanmıştır. Bu tanımdan her türlü elektromanyetik iletiden; örneğin, telefon ,İnternet, faks, telsiz ile yapılan göndermeler, bilgi aktarımları, haberleşmeler vs. anlaşılmalıdır[1033].

Telekomünikasyon yoluyla yapılan iletişimin denetlenmesi kavramı ise, araya bir vasıta sokulmak suretiyle gerçekleştirilen her türlü haberleşmenin gizlice dinlenmesi ve buradan elde edilen bilgilerin kaydedilmesi ve değerlendirilmesi olarak tanımlanabilir[1034]. Bir başka tanıma göre ise telekomünikasyon yoluyla yapılan iletişimin denetlenmesi, görüşenlerin bilgisi dışında, görüşmenin dışarıdan uygun teknik araçlarla müdahale edilerek dinlenmesi ve elde edilen bilgilerin kaydedilmesi ile değerlendirilmesidir[1035].

Kanun koyucu, hangi araçlarla yapılan iletişimin denetlenebileceğini açıkça saymamak suretiyle telekomünikasyon aracı olarak nitelendirilebilecek mevcut ve gelecekte ortaya çıkacak tüm iletişim araçlarını bu kapsama dahil etmek istemiştir. Nitekim yönetmelikte de bu üslup korunmuştur[1036]. Hukuk ve iletişimin iç içe geçtiği bir alan olan iletişimin denetlenmesi ile ilgili bir yönetmelikte böyle bir üslubun tercih edilmesinin hak ve

---

[1031] Telekominikasyon terimi Türkçe sözlükte "Haber, yazı, resim veya her çeşit bilginin tel , radyo, optik, ve başka elekromanyetik sistemlerle iletilmesi, bunların yayımı ve alınması" olarak tanımlanmıştır.(www.tdk.gov.tr).(İET:4.8.2007).

[1032] R.G., 04.07.2007, S. 26572.

[1033] KAYA, Abdulkadir: "Avrupa İnsan Hakları Kararları Işığında İletişimin Dinlenmesi Ve Teknik İzleme", Yargı Dünyası, Sayı 129, Eylül 2006,(İletişimin Dinlenmesi), s.11.

[1034] ÖZTÜRK/ERDEM, s. 600; CMK'nun Beşinci Bölüm başlığının "Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi" olmasına karşılık, konunun düzenlendiği 135. madde başlığının "İletişimin tespiti, dinlenmesi ve kayda alınması" olması aynı konuyu ifade etmek üzere iki ayrı terimin kullanılması eleştirilmiştir. Bunun yerine "Uzakla Haberleşmenin Denetlenmesi" teriminin kullanılmasının daha yerinde olacağı belirtilmiştir. (ÖZBEK, s. 420.).

[1035] BALTACI, s. 357.

[1036] KEKLİK, s.228; AİHM uygulamasında da haberleşme kavramının kapsamı belirlenirken geniş bir bakış açısı tercih edilmiştir. Posta yoluyla gönderilen malzemelerin yanı sıra telefonla iletişim ve teleksi de haberleşmenin kapsamına girmektedir. AİHM, haberleşme kavramını, teknolojik gelişmelere ayak uyduracak ve elektronik posta gibi diğer yöntemleri de içerecek şekilde geniş tutma eğilimindedir. KILKELLY. s. 20.

hürriyetlerin korunması bağlamında doğru olmayacağını düşünmekteyiz. İletişim teknolojisinin on yıl sonra ulaşacağı yer bugünden kestirilemese de, bundan on yıl geriye bakıldığında karşımıza çıkan tablo, gelecek adına bizlere bir fikir vermektedir. Gerçekten de, bugün böyle bir tasarrufta bulunmak yarın teknolojinin çok daha gelişeceği günlerde, mutlak surette müdahaleden uzak tutulması gerekli olan birtakım iletişim vasıtalarının da bu kapsama alınması anlamına gelir. Yönetmeliğin konusu hakkın özüne ilişkin bir sınırlama anlamına geldiğinden, bugünü kuşatacak bir üslubun belirlenmesinin, ihtiyaçlar yeni bir düzenlemeyi gerektirdiğinde de yeni bir çalışmaya gidilmesinin uygun olacağını düşünmekteyiz.

Aslında, anılan yönetmelikle izlenen bu usul 1412 sayılı CMUK dönemindeki kıyas ve yorum tartışmasını akla getirmektedir. Bilindiği üzere, bahse konu kanun döneminde iletişimin denetlenmesi açıkça düzenlenmediğinden, anılan Kanunun 91 ve 92/2. maddelerinde yer alan kıyas[1037] ve yorum[1038]usullerinin kullanılması ile soruna çözüm getirilebileceğini savunan yazarlar vardı. Bizim de katıldığımız bir diğer görüşe göre ise, mevcut yasal düzenlemeler karşısında iletişimin denetlenmesi bakımından ne kıyas ne de genişletici yorum yapılması mümkün değildi. Bu görüş sahipleri, iletişime müdahalenin koşullarının açıkça öngörülmesi gerektiğini ifade etmekteydiler[1039]. Kıyas ve yorum yöntemi umulan gereksinimi karşılamadığı içindir ki, kanun koyucu 5271 sayılı CMK' da yeni bir usul ihdas etmiş ve bu tedbire ilişkin açık hükümler öngörmüştür.

Üstelik bu yaklaşım, AİHM'nin kabul ettiği perspektifle de çelişmektedir. Mahkemeye göre, hakkın özüne ilişkin sınırlama getiren bu tedbirle ilgili olarak, önceden belirlenmiş birtakım kategorilendirmelere başvurulmalıdır. Nitekim, Huvig davasında, Mahkeme, hakkında tedbir uygulanacak kişilerin(the categories of people liable to have their telephones tapped by judicial order) belirlenmemiş olmasını ihlal nedenlerinden biri olarak göstermiştir[1040].

[1037] TOSUN,(Gizli Dinleme), s.99; AKMANLAR, s.670;YURTCAN, s.350;YENİSEY, (Hazırlık Soruşturması), s.478; ŞEN, (1996) s.151.

[1038] ÖZTÜRK, (Hazırlık Soruşturması), s.116;GÖKCEN,s.176.

[1039] Cihan/YENİSEY, s,258; CENTEL, Nur: Koruma Tedbirlerindeki Gelişmeler, Hukuk Araştırmaları Dergisi 1994, s. 77; KAYMAZ, s.797; ÖZTÜRK/ERDEM/ÖZBEK, s.679.

[1040] HUVIG-FRANSA, Pr. 34,35.

3.2.2.2. Denetleme Kavramı

Denetleme terimi; bir görevin yolunda yürütülüp yürütülmediğini anlamak için yapılan araştırma, denetim, bakı, teftiş, murakabe, kontrol anlamına gelmektedir[1041]. Çalışmamızda; geniş anlamda, iletişime yapılan müdahale olarak kullanılan 'denetleme' teriminin içeriği, CMK 135. maddesinde tespit, dinleme, kayda alma ve sinyal bilgilerinin değerlendirilmesi olarak belirlenmiştir.

Denetleme kavramı kapsamında en çok başvurulan işlemlerden olan kayda alma ve tespit kelimelerinin CMK'da bir arada kullanılması bu ifadelerin anlamları konusunda tereddüt doğurmaktadır. Çünkü, 4422 sayılı Kanun'da kayda almayı da kapsayacak şekilde tespit kelimesi ve bunun dışında 'dinleme' kelimesinin kullanılması ile yetinilmişti. CMK md. 135'te kayda almanın ayrıca sayılması nedeniyle tespit etme ile ne kastedildiği sorusu gündeme gelmiştir[1042]. Bu konudaki tereddüt ilgili 10.11.2005 tarihli yönetmelikle giderilmeye çalışılmıştır. Bu yönetmelikte, iletişimin dinlenmesi ve kayda alınması, "Telekomünikasyon yoluyla gerçekleştirilmekte olan konuşmalar ile diğer her türlü iletişimin uygun teknik araçlarla dinlenmesi ve kayda alınmasına yönelik işlemleri ifade eder" şeklinde; iletişimin tespiti ise "İletişimin içeriğine müdahâle etmeden iletişim araçlarının diğer iletişim araçları ile kurduğu iletişime ilişkin arama, aranma, yer bilgisi ve kimlik bilgilerinin tespit edilmesine yönelik işlemleri ifade eder" şeklinde tanımlanmıştır[1043].

Bu tanımlarla, en azından uygulamada, tespit ve kayda alma ifadelerinden ne anlaşılacağı büyük oranda şekillenmiştir. Ancak bu kez de yapılan bu tespit tanımı karşısında sinyal bilgilerinin değerlendirilmesi ifadesinin içeriği büyük oranda boşalmış olmaktadır. Öyle ki aynı yönetmelikte sinyal bilgisinin, "Bir şebekede haberleşmenin iletimi veya faturalama amacıyla işlenen her türlü veriyi ifade eder" şeklinde tanımlanmasıyla birlikte bu tanımların içeriğinin, büyük oranda çakışacağı ortadadır.

Öğretide "dış bağlantı verileri" adı verilen ve konuşmaların içeriğine müdahale etmeden kimler arasında ve hangi saatte yapıldığına ilişkin bilgilerin elde edilmesi, CMK'nın 135. maddesi ve devamındaki madde hükümlerine tabi değildir. Özellikle telefonla taciz, hakaret ve telefonla rahatsız etme suçlarının aydınlatılması amacıyla haberleşme hizmeti sunan kurum tarafından, yapılan konuşmaları ücretlendirmek amacıyla tutulan

---

[1041] Türk Dil Kurumu Sözlüğü, http://www.tdk.org.tr/TR/SozBul (İET:22.11.2007)

[1042] KEKLİK, s. 228.

[1043] ŞAHİN, s. 380.

bu bilgilerden yararlanmasına CMK'nın 135. maddesi engel değildir. Nitekim CMK'nın 135/6. maddesinde "dinleme, kayda alma ve sinyal bilgilerinin değerlendirilmesine ilişkin "yetkinin ancak tek tek sayılmak suretiyle gösterilen suçlar bakımından uygulanacağı öngörülmesine karşın "iletişimin tespiti" bakımından böyle bir sınırlamaya yer verilmemiştir[1044].

İletişimin denetlenmesine ilişkin tedbirler, hakkında tedbir uygulanacak kişinin üzerine kayıtlı veya kullanmakta olduğu iletişim araçlarının hepsi hakkında uygulanabilir. Hakkında karar verilen kişi ile iletişim aracının sahibinin farklı kişiler olması halinde bu durumun ilgili talep ve karar içeriğinde açıkça belirtilmesi gerekmektedir. Resmi ve özel her türlü iletişim kuruluşlarının tuttukları, iletişim içeriğine ilişkin kayıtlar hakkında da dinleme ve tespit kararı alınması mümkündür. İletişimin tespiti , dinlenmesi , kayda alınması ve sinyal bilgilerinin değerlendirilmesi tedbiri kişinin yurtdışı bağlantılı iletişimini de kapsar niteliktedir[1045].

3.2.2.3. Sinyal Bilgilerinin Değerlendirilmesi

İletişimin denetlenmesi tedbirinin esaslarını düzenleyen 14.01.2007 tarihli Yönetmelikte sinyal bilgisinin, bir şebekede haberleşmenin iletimi veya faturalama amacıyla işlenen her türlü veriyi ifade edeceği belirtilmiştir. Aynı Yönetmelikte, sinyal bilgilerinin değerlendirilmesi kavramı ise, iletişimin içeriğine müdahale niteliğinde olmayıp yetkili makamdan alınan karar kapsamında sinyal bilgilerinin iletişim sistemleri üzerinde bıraktığı izlerin tespit edilerek anlamlandırılan sonuçlar çıkarmak üzere gerçekleştirilen değerlendirme işlemlerini ifade etmektedir. Sinyal bilgilerinin değerlendirilmesi tedbiri, 5271 sayılı CMK'nın 135/6 maddesindeki açık düzenleme çerçevesinde ancak ve sadece kanunda öngörülen katalog suçlar için başvurulacak bir yöntemdir[1046].

Örnek olarak belirtmek gerekirse, bir mobil telefonun baz istasyonlarına gönderdiği sinyallerin değerlendirilerek, hakkında yakalama emri bulunan kişinin yerinin belirlenmesinde bu bilgilerin kullanılması[1047] CMK hükümleriyle sınırlandırılmış ve yer tespiti olarak tanımlanan bu işlem aslında sinyal bilgilerinin değerlendirilmesi işlemi olduğu için, ancak CMK 135. maddede belirtilen katolog suçlarında uygulanabilmesi öngörülmüştür. Çünkü, sinyal bilgilerinin canlı olarak değerlendirilmesi, ancak,

---

[1044] ÖZTÜRK/ERDEM, s. 601.

[1045] ÇOLAK, Haluk / TAŞKIN, Mustafa :Ceza Muhakemesi Kanunu Şerhi, Ankara 2007, s.624.

[1046] ÇOLAK/TAŞKIN, s. 623.

[1047] ŞAHİN, s.381.

hakkında dinleme kararı bulunan kişiler için ve bir soruşturma veya kovuşturma kapsamında başka yolla delil elde edilmesi mümkün bulunmadığı takdirde mümkün olabilmektedir. Ayrıca sadece şüpheli ve sanığın iletişimi denetlenebileceğinden, bunun dışındaki kimseler için bu tedbir uygulanamaz. Başka bir anlatımla, şüpheli ve sanık sıfatını kaybeden kişi ile ilgili iletişimin tespiti, dinlenmesi, kayda alınması ve sinyal bilgilerinin değerlendirilmesi söz konusu olamaz.

İletişimin tespiti kavramı ile sinyal bilgilerinin değerlendirilmesi kavramları karıştırılmamalıdır. Yer veya adres bilgilerini ihtiva eden iletişimin tespitin katalog dışı suçlar bakımından da uygulanabildiği halde, sinyal bilgilerinin değerlendirilmesi sadece katalog suçlarına münhasır bir uygulamadır. Sinyal bilgilerinin değerlendirilmesinde iletişim kurulmaksızın bir kişinin yerinin tespit edilmesi söz konusudur. Bu işlem, verilerin değerlendirilmesi gibi rafine bir süreci barındırdığından hakların özüne olabilecek müdahale bakımından daha riskli bulunmuş ve katalog suçları dışında bu işleme izin verilmemiştir.

Sinyal bilgisi, bir şebekede haberleşmenin iletimi veya faturalama amacıyla işlenen her türlü veriyi ifade etmektedir. İletişim vasıtalarından biri olan telefon görüşmeleri, içerik bilgisi ve faturalandırma bilgisi olmak üzere iki temel unsurdan oluşmaktadır. Bu temel unsurlardan ilki olan “içerik bilgisi”, iletişimin dinlenmesi ve kayda alınması işleminin konusunu oluşturmaktadır. Diğer bir unsur olan faturalandırma bilgisi ise, verilen iletişim hizmeti karşılığında alınacak ücrete temel teşkil edecek bilgileri kapsamaktadır. Telekomünikasyon firmalarının ülke çapında kurmuş oldukları baz istasyonları belirli bir kapsama alanı meydana getirmektedirler. Kişilerin iletişim hizmeti alabilmeleri için bu kapsama alanı içinde bulunmaları gerekmektedir. Bu kapsama alanı içinde olan telefonlar baz istasyonları ile sinyal alış-verişi yaparak haberleşmekte, bu haberleşme ise telefonun düzenli aralıklarla göndermiş olduğu sinyale , baz istasyonunun vermiş olduğu cevapla sağlanmaktadır. Bu sinyal bilgileri, kişinin telefon numarasını, telefonun seri numarasını, görüşmelerin gerçekleştiği yer bilgisi ve aranan kişilerle ilgili bilgilerden oluşmaktadır. Bu işlemler sırasında meydana gelen eylemlerden ilki, iletişimin içeriğinin, örneğin ses, mesaj ve veri gibi, karşı tarafa alıcı cihaz aracılığı ile aktarılması ve bunların faturalara yansıtılmasıdır. İkincisi ise, bu aktarımı sağlayan cihazların birbirini bulmasını, anlaşmasını ve birbirinden ayrılmasını sağlayan sinyallerin yazılım ve mekanik sistemler yardımıyla gerçekleşmesi eylemidir[1048].

[1048] ŞAHİN, s.380-381.

Bu verilerin herhangi bir işleme tabi tutulmadan kayıt altına alınarak muhafaza edilmesi ve ilgililere aktarılması iletişimin tespitini ifade ederken; bu verilerin fatura , yazılım ve mekanik bilgilerin bir sanal havuza alınarak ikinci bir işlemden geçirildikten sonra farklı bir amaç için değerlendirilmesi ve işlenmesi ise sinyal bilgilerinin değerlendirilmesini ifade eder[1049]. Sinyal bilgilerinin değerlendirilmesi işleminde, kişiler arasındaki iletişim trafiği, görüşmelerin içeriğine başvurulmaksızın takip edilmektedir. Telefon detay kayıtları, fatura bilgileri esas olmak üzere arayan, aranan, kullanılan cihaz ve yer bilgilerini kapsamakta olup , bu kayıtlar konuşma mesaj ve ses bilgileri dışında kalan bilgileri içermektedir. Sinyal bilgileri vasıtasıyla kişi takip edilerek aynı güzergahtan aynı zaman dilimi içerisinde geçmiş olan kişilerin geçmişe dönük olarak yapılan incelemesi ile bazı bilgilere ulaşılmaya çalışılmaktadır[1050].

3.2.2.4. İletişimin Tespiti

CMK'nın 135. maddesiyle 'Bir suç dolayısıyla yapılan soruşturma ve kovuşturmada, suç işlendiğine ilişkin kuvvetli şüphe sebeplerinin varlığı ve başka suretle delil elde edilmesi imkânının bulunmaması durumunda, hâkim veya gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısının kararıyla şüpheli veya sanığın telekomünikasyon yoluyla iletişimi tespit edilebilir…' şeklinde bir düzenleme getirilmiştir. İletişimin tespiti işleminin, kanunla düzenlenmiş olması önemli bir gelişmedir. Nitekim AİHM, Birleşik Krallık'ta iletişimin tespiti işleminin kanunla öngörülmemiş olmasını ihlal nedeni saymıştır[1051].

İletişimin tespiti kavramı, herhangi bir iletişim aracı ile iki veya daha çok kişinin iletişim kurması ve kimlerin ne zaman arandığı, iletişimin ne kadar süreyle yapıldığı, telekomünikasyon yoluyla kimlerle iletişim kurulduğu hususlarının belirlenmesi ya da sanık veya şüphelinin telekomünikasyon yoluyla kimler ile iletişim kurduğunun tespit edilmesi[1052] olarak tanımlanmaktadır. Özel hayata tam bir müdahale olarak yorumlanmadığı için, iletişimin tespitinin, sadece hakim kararı ile ve katalog dışı suçları da kapsayacak şekilde yapılabilmesi uygulaması Yargıtay tarafından kabul görmektedir[1053]. Bu hususta düzenleme yapan, 10.11.2005[1054] ve 14.01.2007[1055] tarihli

---

[1049] ŞEN, (İletişimin Denetlenmesi Tedbiri), s. 104.

[1050] ŞAHİN, s.381.

[1051] DUTERTRE, s. 260-261.

[1052] ÖZBEK, s. 421.

[1053] 5. CD.,2005/14969 E., 2005/20489 K., 03.10.2005

yönetmeliklerde iletişimin tespiti, "İletişimin içeriğine müdahâle etmeden iletişim araçlarının diğer iletişim araçları ile kurduğu iletişime ilişkin arama, aranma, yer bilgisi ve kimlik bilgilerinin tespit edilmesine yönelik işlemleri ifade eder" şeklinde tanımlanmıştır[1056].

İletişimin denetlenmesi tedbiri üst başlığında yer alan iletişimin dinlenmesi, kayda alınması ve sinyal bilgilerinin değerlendirilmesi tedbirlerinin uygulanmasında katalog suç koşulu aranırken, iletişimin tespiti kararının verilmesi için katalog suç şartı bulunmamaktadır[1057]. Bu husus 14.01.2007 tarihli yönetmeliğin 5.maddesinde "Bir suç dolayısıyla yapılan soruşturma ve kovuşturmada, suç işlendiğine ilişkin kuvvetli şüphe sebeplerinin varlığı ve başka suretle delil elde edilmesi imkanının bulunmaması durumunda, şüpheli veya sanığın telekomünikasyon yoluyla iletişimi tespit edilebilir" şeklinde ifade edilmektedir. AİHM içtihatları kapsamında bu nitelikteki detay bilgiler de özel hayat kapsamında korunduğundan[1058] iletişimin tespiti işleminin tüm suçlar için uygulanabilmesinin doğru bir uygulama olmadığını düşünmekteyiz. İletişim bilgilerinin ayrıntılı dökümünün çıkarılmasının, normal kullanılma alanından farklı bir amaçla kullanıldığında, özel hayatın ihlali anlamına geleceği muhakkak olduğundan, başka bir anlatımla, bazen niteliksiz (neutral) bir bilginin işlenmesi, birtakım kritik bilgilere (sensitive data) ulaşılmasını sağladığı için, bu bilgilere uygulanacak rejimin dikkatli seçilmesinde fayda vardır. Nitekim yetkililer, bu verilerin incelenmesi suretiyle, aslında bilmemeleri gereken verilere ulaşmaktadırlar[1059]. Bu bağlamda, özel hayatın özüne ilişkin bu işlem bakımından da katalog uygulamasının getirilmesi uygun olacaktır. Ancak belli bir ceza eşiğinin aşılması halinde bu işleme başvurulması, bu tedbirin son bir çare olması niteliğiyle uyuşacaktır.

Şikayetçinin iletişimin tespiti konusunda varolan boşluk Yargıtay tarafınan doldurulmuştur. Yüksek Mahkeme, şikayetçinin talebi doğrultusunda Cumhuriyet

---

[1054] Telekomünikasyon Yoluyla Yapılan İletişimin Tespiti, Dinlenmesi, Sinyal Bilgilerinin Değerlendirilmesi ve Kayda Alınmasına Dair Usul ve Esaslar ile Telekomünikasyon İletişim Başkanlığının Kuruluş, Görev ve Yetkileri Hakkında Yönetmelik.

[1055] Ceza Muhakemesi Kanununda Öngörülen Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi, Gizli Soruşturmacı Ve Teknik Araçlarla İzleme Tedbirlerinin Uygulanmasına İlişkin Yönetmelik .

[1056] ÇOLAK / TAŞKIN, s.622.

[1057] ŞAHİN, s. 379.

[1058] AİHM, iletişimin tespitine ilişkin bilgilerin abonenin rızası olmadan polise verilmesinin 8. madde kapsamında teminat altına alınan hakka bir müdahale olduğuna karar vermiştir.(MALONE-BİRLEŞİK KRALLIK, Pr. 84); KUNTER/YENİSEY/NUHOĞLU, s. 704.

[1059] Hakim PETTITI, MALONE-BİRLEŞİK KRALLIK.

Savcısı tarafından yapılan iletişimin tespitinin CMK 135 değil, bu kanunun 160-161. maddeleri kapsamında değerlendirilmesi gerektiğini belirtmiştir. 4. Ceza Dairesi konuyla ilgili kararında 'Gerçekten de ileştişimin tesbiti tedbiri, C.Y.Y.'nın 135/6 maddesindeki sınırlamaya bağlı olmaksızın tüm suçlar açısından uygulanabilir. Ancak bu tedbire sadece şüpheli veya sanık için başvuralabilir. Yakınanın veya suçtan zarar görenin iletişiminin tesbitini, kimliği belirtilen yöntem sonucu belirlenebilecek şüpheli veya sanık için aleyhe kanıt oluşturacak sonuca ulaşılsa bile 135. madde kapsamında değil, Cumhuriyet Savcısın 160. ve 161. maddelerde yer alan genel soruşturma ve kanıt toplama yetkisi çerçevesinde değerlendirmek isabetli olacaktır.' şeklinde görüş beyan etmektedir[1060]. Yargıtay'ımızın bu kararının isabetli olduğunu düşünmekteyiz. Nitekim bu hususu şüpheli veya sanık hakkındaki iletişimin tespitinden farklı kılan şey, kişinin kendi iletişiminin tespit edilmesi yönündeki rızasıdır. Bu rıza, Cumhuriyet Savcısının konu ile ilgili muvafakatı ile birleştiğinde tedbir hayata geçirilmektedir.

Yargıtay bu yaklaşımıyla ceza adaletinin sağlanması kaygısını dile getirmektedir. 4. Ceza Dairesi'ne göre, şikayetçinin talebi ile iletişimin tespiti yoluna başvurulmasına izin verilmemesi halinde, telefon yoluyla işlenen ve faili bilinmeyen suçların şüphelisine/şüphelilerine ulaşma imkanı kalmayacak ve ceza yargılamasının maddi gerçeğinin ortaya çıkartılması amacı gerçekleştirilemeyecektir. Daireye göre, şikayetçi, kendisini tehdit eden şüphelinin kimliğini bilmemekte, bu kişinin bulunarak cezalandırılmasını istemektedir. Şüphelinin saptanabilmesi için eldeki en önemli kanıt, yakınanın cep telefonuyla yapılan görüşmelerin tespitidir. Ancak yakınanın iletişiminin tespitine yönelik olarak hakim kararı alınmasına yasal olanak bulunmadığına göre, bu

---

[1060]4.CD., 2006/4669 E., 2006/17007 K., 29.11.2006.; Yakın tarihli bir 'Yasa Yararına Bozma' kararında Daire bu yargısını pekiştirmektedir. 'Açıklanan yasal düzenlemelerden anlaşılacağı üzere, Yönetmeliğin 3. maddesinde tanımlanan iletişimin tespiti işlemi, CYY'nın 135/6. maddesi kapsamında bulunmadığından, anılan 6. fıkrada sayılan suçlarla sınırlı kalınmaksızın 135. madde uyarınca gereken kararlar verilebilecektir. Buna karşın, CYY'nın 135. maddesindeki düzenleme uyarınca, yalnızca şüpheli veya sanığın iletişiminin tespiti, kayda alınması, dinlenilmesi ve sinyal bilgilerinin değerlendirilmesi olanaklı bulunduğundan, yakınan ya da mağdurun iletişimine ilişkin olarak belirtilen işlemlerin yapılabilmesi anılan madde kapsamında görülmemiştir. Nitekim sözü edilen Yönetmeliğin 12. maddesine göre de hakim kararı gerektiren iletişimin tesbiti tedbiri, şüpheli veya sanık tarafından kullanılan telefonlar hakkında uygulanabilir. Anılan düzenlemelerde yakınanın telefonlarına yönelik bir tedbirden bahsedilmemektedir. Bu durumda yakınanın telefonları açısından iletişimin tesbiti uygulamasını Cumhuriyet Savcısının, C.Y.Y.'nın 160. ve 161. maddelerinde öngörülen genel soruşturma yetkisi çerçevesinde değerlendirilerek çözüme kavuşturmak olanaklıdır. Cumhuriyet Savcısı, ilgili kurumdan yakınanın telefonu ile yapılan görüşmelerin kimle, ne zaman ve hangi süreyle yapıldığına ilişkin kayıtları ve görüşen kişiye ilişkin kimlik bilgilerini içeren iletişimin tesbitini isteyebilir. Cumhuriyet savcısının, soruşturma sırasında failin kimliğini belirleyecek kanıtları elde etmek için, C.Y.Y.'da öngörülen yetkisini kullanabileceğini kabulde yarar ve zorunluluk vardır. Aksi takdirde, telefon yoluyla işlenen ve faili bilinmeyen suçların şüphelisine/şüphelilerine ulaşma olanağı kalmayacak ve ceza yargılamasının, maddi gerçeğinin ortaya çıkartılması amacı gerçekleştirilemeyecektir.'(4. CD.,2007/4496E., 2007/5905 K., 20.6.2007)

durumda, Cumhuriyet Savcısınca CMK'nın verdiği yetkiler çerçevesinde ilgili Telekominikasyon kurumuna gönderilecek yazı ile belirtilen tarihlerde yakınanın cep telefonunu arayan ve aranan kişilerin kimlik bilgileriyle birlikte tespiti mümkün olmalıdır[1061].

3.2.2.5. İletişimin Dinlenmesi ve Kayda Alınması

İletişimin dinlenmesi ve kayda alınması, ilgili yönetmeliklerde, "telekomünikasyon yoluyla gerçekleştirilmekte olan konuşmaların dinlenmesi ve kayda alınması ile diğer her türlü iletişimin uygun teknik araçlarla dinlenmesi ve kayda alınmasına yönelik işlemleri" ifade edeceği belirtilmiştir. İletişimin dinlenmesi ve kayda alınması ancak katalog suçlar bakımından uygulanabilecek bir tedbirdir. Dinleme, iletişimin kayda alınması suretiyle ve kesintisiz olarak devam eden bir tedbirdir.

Faks ile yapılan haberleşmelerde veya İnternet üzerinden yapılan yazışmalarda her ne kadar dinleme değil okuma söz konusu ise de, bu durum iletişimin dinlenmesi kapsamında yer almaktadır. Bu sebeple, faksların veya elektronik posta iletilerinin okunması için de CMK'nın 135. maddesindeki usulün uygulanması gerektiği[1062] düşüncesi hak ve hürriyetlerin korunması bakımından isabetlidir.

3.2.2.6. Mobil Telefonun Yerinin Tespiti

Telekomünikasyon yoluyla iletişimin denetlenmesini düzenleyen CMK'nın 135. maddesi aynı zamanda mobil telefonun yerinin tespitini de düzenlemektedir. Burada mobil telefonla yapılan iletişimin içeriğinin tespitine ilişkin bir tedbir söz konusu değildir. Bu tedbir ile mobil telefonun yeri belirlenerek, şüpheli veya sanığın bulunduğu yerin tespit edilmesi amaçlanmaktadır. Bu tedbirin uygulanması ile şüpheli veya sanığın yanında ya da yakınında bulunan mobil telefonuna sinyal gönderilerek sinyallerin geri alındığı baz istasyonu tespit edilecektir. Kolluk görevlileri de baz istasyonu çevresinde yapacakları araştırmalarla şüpheli veya sanığın yeri ile ilgili verileri değerlendireceklerdir. Bu tedbir katalog suçlar açısından yapılabilmektedir. Ancak sinyal bilgilerinin değerlendirilmesi sonucu yapılan yer tespiti ile iletişimin tespiti kapsamında belirlenen yer tespiti birbirine karıştırılmamalıdır. Her iki işlemde de yer belirlenmekte, ancak sinyal bilgilerinin değerlendirilmesinde herhangi bir iletişim kurulmadan da yer belirlenebilirken (katalog suçlarda), iletişimin tespiti kapsamında yer

---

[1061] 4. CD.,2007/4496E., 2007/5905 K., 20.6.2007.; Bk. Ayrıca 4. CD.,2007/1398 E.,2007/2879 K., 28.3.2007

[1062] KUNTER/ YENİSEY/NUHOĞLU, s. 706.

tespitinde ise kurulan iletişimin sonrasında yer belirlenmektedir. (katalog suçu ve diğer suçlarda)

CMK'nın 135/4. maddesi uyarınca şüpheli veya sanığın yerinin tespit edilebilmesi için, mobil telefonun yeri, hâkim veya gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısının kararına istinaden tespit edilebilir[1063]. Mobil telefonun yerinin tespitine ilişkin karar, iletişimin içeriğine bir müdahale oluşturmamaktadır. Bu nedenle Cumhuriyet savcısının da acele hallerde bu kararı verebilmesi kabul edilmiştir. Ayrıca şüpheli veya sanığın yerinin belirlenmesi, her zaman gecikmesinde sakınca olabilecek bir durumdur. Her an şüpheli veya sanığın yer değiştirmesi, kaçması, telefonunu değiştirmesi mümkündür. Bu nedenle gecikmesinde sakınca bulunan hal gerekçesi ile Cumhuriyet savcısı da bu kararı verebilecektir[1064]. Ancak Cumhuriyet savcısının verdiği mobil telefonun yerinin tespitine ilişkin karar hakim onayına sunulmak zorunda değildir[1065]şeklindeki görüşlerin isabetli olmadığı kanaatindeyiz. Çünkü CMK 135. maddenin genelinde hakim kararının asıl, savcılık talebinin ise istisna olarak düzenlendiği bilinmektedir. Mobil telefonun yerinin tespiti için verilecek kararda, mobil telefon numarası ve tespit işleminin süresi belirtilmek zorundadır. Bu tedbirin uygulanmasında, sinyal bilgilerinin değerlendirilmesi açısından katalog suç sınırlaması söz konusu iken, iletişimin tespiti sonucu yapılan yer tespiti bakımından katalog suç uygulaması zorunlu kılınmamıştır. Dolayısıyla, her suç bakımından sinyal bilgilerinin değerlendirilmesi suretiyle şüpheli veya sanığın yakalanması amacıyla bu yola başvurulabilir[1066] düşüncesi isabetli değildir. Bu durum, iletişimin tespiti sırasında yapılan yer tespitinde geçerlidir. Düzenlemeye göre hükümlünün yakalanması amacıyla da bu tedbir uygulanamaz.

Öte yandan, sanık ve şüphelinin yanı sıra hükümlülerin hakkında da bu tedbirin uygulanması gerektiği şeklindeki görüşünün isabetli olduğunu düşünüyoruz[1067]. Bununla birlikte, bu tedbirin ancak kişinin yakalanması amacıyla uygulanması gerektiği muhakkaktır. Ayrıca, hükümlüler için bu tedbirin uygulanması halinde, bu tedbirin uygulama alanının daraltılması gerekir. Gerçekten de, bu hükmün tüm

---

[1063] TURHAN, Faruk :Ceza Muhakemesi Hukuku, Ankara 2006, s. 270; ÖZBEK, s. 422; CENTEL/ZAFER, s. 365.

[1064] ÖZTÜRK/ERDEM, s. 607.

[1065] YİĞİT, s. 26.

[1066] ÖZBEK, s. 424; ŞAHİN, s. 379.; ŞAHİN, Ceza Muhakemesi Hukuku, s.271

[1067] TAŞKIN, Mustafa: Adli Ve İstihbari Amaçlı İletişimin Denetlenmesi, Seçkin Yayıncılık, 2008, s.82.

hükümlülere uygulanması halinde, bu tedbirin amacını aşması ihtimali de vardır. Bu itibarla, mahkumiyetin niteliği(para cezası, hapis cezası), kişinin adaletten kaçma durumu(cezanın ertelenmiş olması vs.) gibi durumların dikkate alınması gerekir.

3.2.2.7. Diğer İletişim Bilgilerinin İstenmesi

İletişim dinlenmesi ve kaydedilmesi, iletişime ilişkin sinyal bilgilerinin değerlendirilmesi ve iletişimin tespitine ilişkin bilgilerinin dışında yer alan abone, kimlik veya kütük bilgilerinden de ceza soruşturması ve kovuşturmasında yararlanılmaktadır. Bu bilgilere "diğer iletişim bilgileri " ya da "iletişim dışı detay bilgiler" denilmesi kavram karışıklığını engellemek için uygun olacaktır. Yukarıda sayılan dinleme, kaydetme, sinyal bilgilerini değerlendirme ve tespit işlemleri dışında kalan abone bilgileri, telefon numarası, elektronik cihaz bilgileri veya iletişim bağlantısının tespitine imkân veren kod gibi iletişimin tespiti kapsamı dışındaki bilgiler de bir suç dolayısıyla yapılan soruşturma ve kovuşturma kapsamında işletmecilerden, servis sağlayıcılardan talep edilmelidir.

Abone ismi , abone adresi, abone kimlik bilgileri, telefon numarası, IMEI numarası sorgusu veya eşleştirmesi, (IMEI numarasından kullanıcı, kullanım tarihi, kimlik ve adres bilgisi araştırması), IP sorgusu bilgileri, sim kart bilgisi ve eşleştirmesi, İmsi bilgisi, Puk numarası bilgisi, kontör kartları bilgisi ve eşleştirmesi, roaming bilgisi, telefonun açık olup olmadığı bilgisi diğer iletişim bilgileri ya da iletişim dışı detay bilgileri olarak adlandırılan bilgilerdir.

3.2.3.Türk Hukukunda Adli Amaçlı İletişimin Denetlenmesinin Koşulları

3.2.3.1.Katalog Suçlardan Birinin Bulunması

3.2.3.1.1.Genel Olarak

Türk hukukunda katalog[1068] suç uygulaması kabul edilmiştir. Kanun koyucu bu tedbirin uygulanabileceği suçları bir katalog halinde belirlemiştir. İşlenen suç ile verilen zarar ne kadar ağır olursa olsun burada belirtilen suçlar dışındaki suçlar bakımından iletişimin denetlenmesi tedbirine başvurulamayacak[1069] ve denetleme tedbiri hangi

---

[1068]İletişimin denetlenmesinin uygulanacağı suçların belirlenmesi bakımından, suçun niteliği kıstas alınarak üç ayrı model kabul edilmektedir. Bunlardan ilki, belirli suçları içine alan bir suç katalogu oluşturup bu fiiller sebebiyle tedbire karar verilmesidir. İkincisi, failin işlediği suç dikkate alınarak, verilmesi mümkün olan ceza miktarına göre tedbire karar verilmesi ve üçüncüsü ise, fiilin ağırlığına göre tedbire karar verilmesi olarak sıralanabilir.(GÖKCEN, s. 189.).

[1069] TURHAN, s. 267; ÇOLAK/TAŞKIN, s. 633; MALKOÇ,İsmail/YÜKSEKTEPE,Mert:Ceza Muhakemesi Kanunu, Ankara 2005, s. 371; KARAYAZGAN, Mehmet: "Yeni TCK İle İletişimin Tespiti, Dinlenmesi Ve Kayda Alınması", Polis Dergisi,Sayı 44, Nisan-Mayıs-Haziran 2005, s. 55.

suçla ilgili olarak verilmişse, sadece o suçtan dolayı ve karara konu iletişim vasıtası hakkında bu tedbir uygulanabilecektir[1070]. Bu kapsamda CMK, sınırlı sayıda suç için bu tedbire izin vermiştir. Bu suçlar, belirli ağırlıkta olan ve işleniş şekilleri itibari ile, iletişimin denetlenmesi tedbirine en çok ihtiyaç duyulacak suçlar olarak belirlenmiştir . Katalog tespiti suretiyle, kapsam dışındaki suçlarla ilgili olarak bu tedbire başvurulması engellenmiştir[1071]. Kanun tarafından denetleme tedbirine tabi suçların kıyas suretiyle genişletilmesi mümkün değildir. Her ne kadar ceza muhakemesi hukukunda kıyas yapılabilse de, temel hakları sınırlayıcı kıyas mümkün değildir. Bu sebeple, kapsam dışında kalan diğer suçlarda iletişimin denetlenmesine başvurulması hukuka aykırı olacaktır[1072].

AİHM, iletişimin denetlenmesi tedbirinin hangi suçlar hakkında uygulanacağına ilişkin bir kategori yapmaktan kaçınmış, bunun yerine genel kriterler belirlemek ve bu kriterlerin içinin doldurulmasında da devletlere bir takdir yetkisi tanımak yolunu seçmiştir. Takdir hakkının suiistimali ihtimali karşısında, belli kategorizasyonların öngörülmesi, keyfilik tehlikesine karşı önlem olması anlamında önemlidir[1073]. Bu düşüncenin sonucu olarak Mahkeme, polisin basit kuşkularının bu kararı vermek için yeterli ve tatmin edici olamayacağını[1074], bir suçla ilişkisi olduğu düşünülen tüm bireylerle ilgili toplu izinlerin verilemeyeceğini, şüpheli veya bu kişiyle bağlantısı olduğu tahmin edilen kişiler hakkında bu tedbire başvurulabileceğini vurgulamaktadır[1075]. Mahkeme, her türlü suçun önlenmesi amacıyla iletişimin dinlenmesi yoluna başvurulamayacağını[1076], acil sosyal ihtiyaçların karşılanması bağlamında, organize suçlar gibi belli bir ağırlık ihtiva eden suçlarla ilgili olarak bu tedbire başvurulabileceğini ifade etmiştir[1077]. ABD'deki Teknik Dinleme Kanunu'nun asıl varlık nedeni de, benzer bir yaklaşımdan kaynaklanmaktadır. Bu neden, organize suçlarla mücadele etmek

---

[1070] ŞEN, (İletişimin Denetlenmesi Tedbiri)s. 109.

[1071] SÖZÜER, s. 109;ÜNVER/ ÖZBEK, s.172; CENTEL/ZAFER, s.362; ERDEM, 98 ; NOYAN, Erdal : Ceza Muhakemesi, Ankara 2005, s.305.

[1072] KUNTER/ YENİSEY/NUHOĞLU , s.708.

[1073] KÜNHE, s. 105.

[1074] Bk. PRADA BUGALLO-İSPANYA.

[1075] KLASS-ALMANYA, Pr. 51.

[1076] DÜLGER, s. 6.

[1077] MALONE-BİRLEŞİK KRALLIK, Pr. 81; Fransa'nın mahkum edildiği Kruslin ve Huvig kararlarının hemen akabinde, AİHM'nin, ancak belirli ağırlıktaki suçlar için bu tedbire başvurulabilmesine müsamaha eden yaklaşımı Fransa'yı gerekli değişiklikleri yapmak noktasında harekete geçirmiştir. Bu bağlamda, Fransız Adalet Bakanlığı yetkililerince başlatılan çalışmada dikkate alınan hususlardan biri de, yalnızca ağır suçlar bakımından bu tedbire başvurulabilmesine izin veren bir yasal düzenleme yapılması olmuştur.(ERRERA, s. 861.)

düşüncesidir[1078]. Bu amaca yönelik olarak, anılan kanunun orijinal metninde teknik dinlemenin bir soruşturma yöntemi olarak kullanılmasına imkan tanıyan 26 suç türü, genellikle organize suç ve ulusal güvenliği ilgilendiren ağır[1079] federal[1080]suçlardı.

Katalog dışı suçlarda sadece "iletişimin tespiti" işlemi yapılabilmektedir. Konuşmanın içeriği dinlenmediği için bazı yazarlar tarafından özel hayata tam bir müdahale olarak nitelendirilmeyen bu tedbire, katalog dışı suçlar bakımından ve sadece hakim kararı ile başvurulması Yargıtay tarafından tasdik edilmektedir[1081]. Yargıtay 5. Ceza Dairesi 03.10.2005 tarih ve 2005/14969-20489 sayılı kararında"…5271 sayılı CMK'nın, 5353 sayılı kanunun 17. maddesiyle değişik 135. maddesi uyarınca, "bir suç dolayısıyla yapılan soruşturma ve kovuşturmada, suçun işlendiğine ilişkin kuvvetli şüphe sebeplerinin varlığı ve başka surette delil elde edilmesinin mümkün olmaması durumunda, hakim veya gecikmesinde sakınca bulunan hallerde Cumhuriyet Savcısının kararıyla şüpheli veya sanığın telekomünikasyon yoluyla iletişimi tespit edilebilir, dinlenebilir, kaydı alınabilir ve sinyal bilgileri değerlendirilebilir" denilmekte, iletişimin tespiti kararının verilebilmesi için tedbir kararına konu olan suçun CMK 135/6. maddesi kapsamında olmasının gerekmediği ifade edilmektedir. 5353 sayılı Kanunun 17. maddesiyle değişik CMK'nın 135/6 fıkrasında bu madde kapsamında "dinleme, kayda alma ve sinyal bilgilerinin değerlendirilmesine" ilişkin hükümlerin fıkrada sayılan katalog suçlarla ilgili olarak uygulanabileceği öngörülmüştür. Soruşturma evresinde şüphelinin kullandığı telefonla yaptığı görüşmelere ilişkin detay bilgilerinin, yani telefonla yapılan bağlantıların kimlerle ve ne zaman yapıldığının belirlenmesi anlamına gelen "tespit" yukarıda belirtilen CMK'nın 135. maddesinin 6. fıkrası kapsamı dışında bırakılmıştır. Bu nedenle, hangi suça ilişkin olursa olsun, şüpheliye ait telefondan kimlerle, ne zaman görüşüldüğüne dair "tespit" CMK'nın135/1. maddesi uyarınca hakim veya gecikmesinde sakınca bulunan hallerde Cumhuriyet Savcısının kararıyla mümkün olacaktır[1082].

Bilindiği üzere, iletişimin denetlenmesi tedbiri üst başlığında yer alan iletişimin dinlenmesi, kayda alınması ve sinyal bilgilerinin değerlendirilmesi tedbirlerinin

---

[1078] ÖZDOĞAN, (2004), s. 30.

[1079] AN OVERVIEW OF ELECTRONIC SURVEILLANCE: History and Current Status, D.1.1; DEMPSEY, "Communications Privacy In The Digital Age: Revitalizing The Federal Wiretap Laws To Enhance Privacy".

[1080] STEVENS/DOYLE, s. 37.

[1081] KUNTER/YENİSEY/NUHOĞLU , s.708.

[1082] NUHOĞLU, Ayşe: Adli Amaçlı Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi, Yargı Dünyası, Sayı.128,Ağustos 2006, s. 10

uygulanmasında katalog suç koşulu aranırken, iletişimin tespiti kararının verilmesi için katalog suç şartı bulunmamaktadır[1083]. Kanundan doğan bu zorunluluğun değiştirilmesi, başka bir anlatımla, iletişimin tespiti bakımından da katalog suçu tasnifinin getirilmesinin uygun olacağı kanaatindeyiz[1084]. AİHM içtihatları kapsamında, bu nitelikteki bilgiler de özel hayat kapsamında korunduğundan[1085] iletişimin tespiti işleminin tüm suçlar için uygulanabilmesinin doğru bir uygulama olmadığını düşünmekteyiz. Bazı yazarlar[1086] tarafından özel hayata tam bir müdahale olarak nitelendirilmeyen bu tedbir kapsamında, iletişim bilgilerinin ayrıntılı dökümünün çıkarılması, normalden farklı bir amaçla kullanıldığında, özel hayatın ihlali anlamına gelecektir. Nitekim, bazen niteliksiz bir bilginin işlenmesi, birtakım kritik bilgilere ulaşılmasını sağladığı için, bu bilgilere uygulanacak rejimin dikkatli seçilmesinde fayda vardır. Bu verileri inceleyen yetkililer, aslında bilmemeleri gereken verilere ulaşabilmektedirler[1087]. Bu itibarla, özel hayatın özüne ilişkin bu işlem bakımından da katalog uygulamasının getirilmesi uygun olacaktır. Katalog suçu şartının getirilmesi ile kastettiğimiz CMK 135'te sayılan suçlar için bu tedbire başvurulmasının sağlanması değildir. Kanaatimizce, bu tedbire ancak belli bir ceza eşiğinin aşılması halinde başvurulmalıdır.

Kanunda sayılan suçlara teşebbüs veya iştirak halinde de, bu tedbire başvurulabilir. Mesela, bir olayda A'nın, bir otomobilin içinden B'ye ateş ederek öldürmeye teşebbüs etmesi ve bu otomobilin de C tarafından kullanıldığı şüphesinin bulunması halinde A ve C'nin telefonları denetim altına alınabilecektir. Aynı olayda kullanılan aracın D tarafından çalınmış olduğu şüphesi varsa, hırsızlık suçu katalog suçlar arasında yer almasa bile, suçta kullanılan otomobilin çalınması, kasten adam öldürme suçunu işlemeye yönelik olabileceğinden D'nin telefonu da dinlenebilir[1088]. Buna göre CMK'nın 135/3. maddesine göre madde kapsamındaki suçlardan biri söz konusu olduğunda, kuvvetli şüphe ve başka türlü delil elde etme imkanının olmaması halinde, bu suçlara

---

[1083] ŞAHİN, s. 379.

[1084] 5271 sayılı CMK'nın 135/6. maddesinde yer alan "bu madde hükümleri" ifadesi, 5353 sayılı kanunun 17. maddesi ile "bu madde kapsamında dinleme, kayda alma ve sinyal bilgilerinin değerlendirilmesine ilişkin hükümler" olarak değiştirilmiştir. Bu değişikliğe gidilmesinin temel sebebi, katalogda sayılan suçlarla ilgili tedbirlerin sadece dinleme, kayda alma ve sinyal bilgilerinin değerlendirilmesi olup "iletişimin tespiti" bakımından suç yönünden bir katalog sınırlaması olmamasıydı(ÖZBEK, s. 424;ÜNVER / HAKERİ, s. 172; NUHOĞLU, s. 11).

[1085] MALONE-BİRLEŞİK KRALLIK, Pr. 84; KUNTER/YENİSEY/NUHOĞLU, s. 704.

[1086] KUNTER/YENİSEY/NUHOĞLU , s.708.

[1087] Hakim PETTITI, MALONE-BİRLEŞİK KRALLIK.

[1088] TURHAN, s.267-268; ÖZTÜRK/ ERDEM, s. 608.

iştirak edenler hakkında da iletişimin denetlenmesi tedbiri uygulanabilir. Buna karşılık, işlendikten sonra faillere yardım veya aracılık ya da yataklık yapan kişilerin iletişimi, bunların fiili suçtan önceki bir iştirak ilişkisi çerçevesinde olmadığı sürece denetlenmesi mümkün değildir. Nitekim, suç delillerini yok etme, gizleme veya değiştirme (TCK md. 281) ile suçluyu kayırma (TCK. Md.283) suçları iletişimin denetlenmesi tedbirinin uygulandığı katalog suçlar arasında yer almamaktadır[1089].

İletişimin denetlenmesi tedbirinin uygulanması sırasında, katalog dışındaki bir suçun öğrenilmesi durumunda bu kaydın kullanılması mümkün olmamaktadır. Ancak dinleme yapan görevlinin kamu görevlisi olması karşısında, bu suçu bildirme yükümlülüğünün bulunup bulunmadığı değerlendirilecek olursa, TCK'nın 279. maddesi karşısında kamu görevlisinin göreviyle bağlantılı olarak haberdar olduğu bir suç söz konusu olduğundan bunu ilgili makamlara bildirmek zorundadır. Her ne kadar CMK'nın 138. maddesinde, tesadüfen elde edilen delillerin ancak bu katalog suçlarla ilgili olması halinde kullanılabileceği belirtilmekte ise de, anılan madde kamu görevlisinin ilgili makamlara bildirimde bulunmasını engellememektedir[1090].

4422 sayılı kanun, sadece örgütlü suçlarda bu koruma tedbirine imkan vermekte ve belirtilen bu suçların 4422 sayılı Kanunun 1. maddesinde belirtilen amaçlarla işlenen suçlardan olması gerekmekteydi. Bu düzenleme hem kanunilik ilkesine aykırı olduğu ve hem de bu şekilde ve anılan kanunun 1. maddesinde belirtilen amaçla işlenen tüm suçları kapsadığı için eleştirilmekte ve bunun yerine katalog esasının getirilmesi önerilmekteydi[1091]. Bu bağlamda, CMK, ilk düzenlemede on altı suç bakımından bu tedbire imkan veriyordu. 5353 sayılı kanun ile fuhuş suçu ve Bankalar Kanununun 22. maddesinin 3.ve 4. fıkralarında tanımlanan zimmet suçu da eklenmek suretiyle toplam on sekiz suç bakımından bu tedbirin uygulanması mümkün hale gelmiştir. Bu suçların çıkar amacıyla ya da örgütlü olarak işlenmesi zorunlu değildir. Katalogda sayılan ve bireysel olarak işlenebilen kasten adam öldürme, işkence ve cinsel saldırı suçları bakımından bu tedbire başvurulması mümkündür[1092].

[1089] ÜNVER / HAKERİ, s. 176.

[1090] ÜNVER / HAKERİ, s. 172-173.

[1091] CENTEL, Nur: Ceza Muhakemesi Usulü Kanunu 2000 Tasarısına eleştirel Yaklaşım, Mahmut Teffik Birsel'e Armağan, İzmir 2001,(armağan), s.508;ERDEM/ÖZBEK, s.283-285.

[1092] ÖZBEK, s.424. CMK'nın 2001 tasarısında ise, katalog tarzı uygulamadan ziyade beş yıl veya daha fazla hürriyeti bağlayıcı ceza gerektiren suçlarda bu tedbirin uygulanabileceği belirtilmekteydi.(ÜNVER / HAKERİ, s. 172.)

Hakkında iletişimin denetlenmesi tedbiri uygulanabilecek suçlar bakımından herhangi bir tasnif yapmayan AİHM'nin[1093] belirlediği ilkeler çerçevesinde yapılacak bir değerlendirme ile; hukukumuzdaki adli amaçlı iletişimin denetlenmesi tedbiriyle ilgili yasal düzenlemelerin birtakım eksikliklere rağmen, Sözleşme ve Mahkeme kriterlerini karşıladığı söylenebilir. Nitekim, bu düzenlemeler incelendiğinde, verilen takdir hakkının ölçülülük ilkesi çerçevesinde kullanıldığı, her suçun bu tedbir kapsamına alınmaması suretiyle birey merkezli ve insan haklarını koruma kaygısı taşıyan düzenlemelere yer verildiği, basit kuşku şöyle dursun, bu tür tedbirlere başvurabilmek için kuvvetli şüphe kriterinin arandığı, bir suçla ilişkisi olduğu düşünülen tüm bireylerle ilgili toplu izinlerin verilmesini imkan sağlayan düzenlemelerden kaçınıldığı ancak şüpheli veya bu kişiyle bağlantısı olduğu tahmin edilen kişiler hakkında bu tedbire başvurulabildiği anlaşılmaktadır.

3.2.3.1.2. Katalogda Yer Alan Suçlar

İletişimin tespiti tedbirinin uygulanması bakımından katalog suç sınırlaması söz konusu değilken iletişimin dinlenmesi, kaydedilmesi ile sinyal bilgilerinin değerlendirilmesi tedbirine, ancak aşağıda belirtilecek katalog suçlar bakımından başvurulabilecektir. Bu suçlar;

3.2.3.1.2.1.Türk Ceza Kanununda Yer Alan Suçlar

1. Göçmen kaçakçılığı ve insan ticareti (Madde 79, 80),

2. Kasten öldürme (Madde 81, 82, 83),

3. İşkence (Madde 94, 95),

4. Cinsel saldırı (birinci fıkra hariç, Madde 102),

5. Çocukların cinsel istismarı (Madde 103),

6. Uyuşturucu veya uyarıcı madde imal ve ticareti (Madde 188),

7. Parada sahtecilik (Madde 197),

8. Suç işlemek amacıyla örgüt kurma (iki, yedi ve sekizinci fıkralar hariç, Madde 220),

9. Fuhuş (Madde 227, fıkra 3), (Ek alt bent: 25/05/2005-5353 S.K./17.madde)

[1093] KLASS-ALMANYA, Pr.51.

10. İhaleye fesat karıştırma (Madde 235),

11. Rüşvet (Madde 252),

12. Suçtan kaynaklanan malvarlığı değerlerini aklama (Madde 282),

13. Silahlı örgüt (Madde 314) veya bu örgütlere silah sağlama (Madde 315),

14. Devlet Sırlarına Karşı Suçlar ve Casusluk (Madde 328, 329, 330, 331, 333, 334, 335, 336, 337) suçları.

3.2.3.1.2.2. Ateşli Silahlar ve Bıçaklar İle Diğer Aletler Hakkında Kanunda Tanımlanan Silah Kaçakçılığı Suçları.

İletişimin denetlenmesi tedbirinin uygulanacağı suçlar arasında 6136 sayılı Ateşli Silahlar Ve Bıçaklar İle Diğer Aletler Hakkında Kanun'unun 12. maddesinde tanımlanan "Silah Kaçakçılığı" suçuna da yer verilmiştir. 6136 sayılı kanundaki silah kaçakçılığı bireysel olarak olabileceği gibi örgüt kapsamında da işlenmeye müsait bir suçtur. Buna göre, bir kimse bu kanunun kapsamına giren ateşli silahlarla bunlara ait mermileri ülkeye sokma veya sokmaya kalkışma veya bunların ülkeye sokulmasına aracılık etme veya bunları Türkiye'de Harp Silah ve Mühimmatı Yapan Hususi Sanayi Müesseselerinin Kontrolü Hakkındaki 3763 sayılı ve Makine ve Kimya Endüstrisi Kurumu Hakkındaki 5591 sayılı Kanunların hükümleri dışında ülkede yapma veya bu surette ülkeye sokulmuş ve ülkede yapılmış olan ateşli silahları veya mermileri bir yerden diğer bir yere taşıma veya yollama veya taşımaya bilerek aracılık etme, satma veya satmaya aracılık etme veya bu amaçla bulundurma şüphesi altında olursa ve bu kapsamda başka türlü delil elde etme imkanı da yoksa bu kişi ya da kişiler veya suç örgütleri hakkında iletişimin denetlenmesi tedbirine başvurulması mümkündür.

3.2.3.1.2.3. Bankalar Kanununun 22. (160) Maddesinin (3) ve (4) Numaralı Fıkralarında Tanımlanan Zimmet Suçu

Bankacılık Kanunun 3 ve 4. fıkralarında düzenlenmiş olan zimmet suçu, 5271 sayılı CMK'nın ilk halinde bulunmuyordu . CMK'da 25.05.2005 tarihinde 5353 sayılı kanunun 17. maddesi ile yapılan değişiklikle bu suç da iletişimin denetlenmesi tedbirinin kapsamına girmiştir.

4389 sayılı Bankalar Kanunu, 01/11/2005 tarih ve 25983 Mükerrer sayılı Resmi Gazete'de yayımlanan 19.10.2005 tarih ve 5411 sayılı "Bankacılık Kanunu"nun 168. maddesinin A fıkrası ile, aynı kanunun geçici maddelerindeki düzenlemeler hariç olmak

üzere, ek ve değişiklikleri ile birlikte yürürlükten kaldırılmıştır. Ayrıca 5411 sayılı Bankacılık Kanunu'nun 169.maddesinde, bu kanunla yürürlükten kaldırılan 4389 sayılı Bankalar Kanununa yapılan atıfların, bu Kanun'un ilgili maddelerine yapılmış sayılacağı belirtilmiştir. Buna göre, mülga Bankalar Kanun'unun 22. maddesinin 3 ve 4. fıkralarında tanımlanan zimmet suçuna paralel düzenleme, 5411 sayılı Bankacılık Kanununun 160. maddesinde düzenlenmiştir. Bu maddedeki düzenlemeye göre, görevi nedeniyle zilyetliği kendisine devredilmiş olan veya koruma ve gözetimiyle yükümlü olduğu para veya para yerine geçen evrak veya senetleri veya diğer malları kendisinin ya da başkasının zimmetine geçirdiği konusunda kuvvetli suç şüphesi bulunan banka yönetim kurulu başkan ve üyeleri ile diğer mensupları ile faaliyet izni kaldırılan veya fona devredilen bir bankanın; hukuken veya fiilen yönetim ve denetimini elinde bulundurmuş olan gerçek kişi ortaklarının, kredi kuruluşunun kaynaklarını, kredi kuruluşunun emin bir şekilde çalışmasını tehlikeye düşürecek şekilde doğrudan veya dolaylı olarak kendilerinin veya başkalarının menfaatlerine kullandırmak suretiyle, kredi kuruluşunu her ne suretle olursa olsun zarara uğrattıkları hususunda kuvvetli şüphe varsa ve başka türlü de delil elde etme imkanı yoksa bu kişiler hakkında da iletişimin denetlenmesi tedbirine başvurulabilir.

3.2.3.1.2.4 Kaçakçılıkla Mücadele Kanununda tanımlanan ve hapis cezasını gerektiren suçlar

4926 sayılı Kaçakçılıkla Mücadele Kanunu, 31/03/2007 tarih ve 26479 sayılı Resmi Gazete'de yayımlanan 21/03/2007 tarih ve 5607 sayılı Kaçakçılıkla Mücadele Kanunu'nun 25. maddesi ile yürürlükten kaldırılmıştır. 5607 sayılı Kanun'un geçici 1. maddesine göre, diğer kanunlarda mülga 7/1/1932 tarihli ve 1918 sayılı Kaçakçılığın Men ve Takibine Dair Kanun ile bu Kanunla yürürlükten kaldırılan Kaçakçılıkla Mücadele Kanununa yapılan atıfların, 5607 sayılı kanuna yapılmış sayılacağı belirtilmiştir. Buna göre iletişimin denetlenmesi tedbirinin kapsamındaki katalog suçlar arasında yer alan kaçakçılık suçlarından hapis cezasını gerektiren eylemler, bu kanunun üçüncü ve dördüncü maddesinde hüküm altına alınmıştır. Bu maddelerde hapis cezasını gerektiren eylemler şunlardır:

1. Eşyanın, gümrük işlemlerine tâbi tutmaksızın Türkiye'ye ithal edilmesi veya eşyanın, belirlenen gümrük kapıları dışından Türkiye'ye ithal edilmesi,

2. Eşyanın , sahte belge kullanmak suretiyle gümrük vergileri kısmen veya tamamen ödenmeksizin, Türkiye'ye ithal edilmesi,

3. Transit rejimi çerçevesinde taşınan ve serbest dolaşımda bulunmayan eşyanın, rejim hükümlerine aykırı olarak gümrük bölgesinde satılması,

4. Belli bir amaç için kullanılmak veya işlenmek üzere ülkeye geçici ithalat ve dahilde işleme rejimi çerçevesinde getirilen eşyanın, sahte belge ile yurt dışına çıkarılmış gibi işlem yapılması,

5. Yukarıda tanımlanan fiillerin işlenmesine iştirak etmeksizin, bunların konusunu oluşturan eşyanın, bu özelliği bilinerek ve ticarî amaçla satın alınması, satışa arz edilmesi, satılması, taşınması veya saklanması,

6. Özel kanunları gereğince gümrük vergilerinden kısmen veya tamamen muaf olarak ithal edilen eşyanın, ithal amacı dışında başka bir kullanıma tahsis edilmesi, satılması veya devredilmesi ya da bu özelliğinin bilinerek satın alınması veya kabul edilmesi,

7. İthali kanun gereği yasak olan eşyanın ithal edilmesi veya ithali yasak eşyanın , bu özelliği bilinerek satın alınması, satışa arz edilmesi, satılması, taşınması veya saklanması,

8. İhracı kanun gereği yasak olan eşyanın Türkiye'den ihraç edilmesi,

9. İhracat gerçekleşmediği halde gerçekleşmiş gibi gösterilmesi ya da gerçekleştirilen ihracata konu malın cins, miktar, evsaf veya fiyatını değişik göstererek ilgili kanun hükümlerine göre teşvik, sübvansiyon veya parasal iadelerden yararlanmak suretiyle haksız çıkar sağlanması,

3.2.3.1.2.5 Kültür ve Tabiat Varlıklarını Koruma Kanununun 68. ve 74. Maddelerinde tanımlanan suçlar

Kültür ve Tabiat Varlıklarını Koruma Kanunun 68. maddesi, aynı kanunun 32. maddesinin 1. fıkrasına aykırı davrananların cezalandırılacağını öngörmektedir. Bu kanunun 32. maddesi ise yurt içinde korunması gerekli taşınır kültür ve tabiat varlıklarının yurt dışına çıkarılamayacağını; ancak, milli çıkarlarımız dikkate alınarak, bunların her türlü hasar, zarar, tehdit veya tecavüz ihtimaline karşı, gideceği ülke makamlarından teminat almak ve sigortalanmak şartı ile, yurt dışında geçici olarak sergilendikten sonra geri getirilmelerine; Kültür ve Turizm Bakanlığınca teşkil edilecek yükseköğretim kurumlarının arkeoloji ve sanat tarihi bilim dallarının başkanlarından oluşan bilim kurulunun kararı ve Kültür ve Turizm Bakanlığının teklifi üzerine Bakanlar Kurulunca karar verileceğini düzenlemiştir. Dolayısıyla, bu hükme aykırı davrandığı

konusunda şüphe duyulan ve haklarında başka türlü delil elde etme imkanı bulunmayan bu kişi veya kişiler hakkında iletişimin denetlenmesi tedbirine karar verilebilir.

Kültür ve Tabiat Varlıklarını Koruma Kanunu'nun "İzinsiz Araştırma, Kazı Ve Sondaj Yapanlar" başlığını taşıyan 74. maddesinde ise, ruhsatsız sondaj ve kazı yapanlar, izinsiz define araştıranlar ve izinsiz araştırma yapanların cezalandırılacağı öngörülmüştür. Ayrıca maddenin devamında, söz konusu fiilleri yurt dışına kültür varlıklarını kaçırma amacıyla yaptıkları anlaşılanlar ve bu fiili işleyenlerin kültür varlıklarının korunmasında görevli kişiler olması halinde cezalarının arttırılacağı öngörülmüştür. Buna göre, bu madde kapsamındaki eylemler hakkında şartların bulunması halinde CMK'nın 135. maddesi uygulanabilecektir.

3.2.3.1.2.6. Terörle Mücadele Kanununda Yapılan Değişiklikle Tedbir Kapsamına Alınan Suçlar

Telekomünikasyon yoluyla iletişimin denetlenmesi tedbirinin uygulanacağı suçları düzenleyen CMK'nın 135/6. maddesi uyarınca suç işlemek amacıyla örgüt kurma suçlarını düzenleyen TCK'nın 220. maddesinin iki, yedi ve sekizinci fıkraları hariç olmak üzere tedbir kapsamında olduğu belirtilmiştir. Dolayısıyla, suç işlemek için kurulan bir örgüte üye olanlar (TCK md.220/2) ile, örgüt içindeki hiyerarşik yapıya dahil olmamakla birlikte, örgüte bilerek ve isteyerek yardım eden (TCK md.220/7) ve örgütün veya amacının propagandasını yapan kişilerin (TCK md.220/8) iletişimi denetim altına alınamayacaktır. Ancak, 3713 sayılı Terörle Mücadele Kanunun 10. maddesinde 29.06.2006 tarihinde 5532 sayılı kanunun 9. maddesi ile yapılan değişiklikle Ceza Muhakemesi Kanununun 135. maddesinin altıncı fıkrasının (a) bendinin (8) numaralı alt bendindeki istisnaların uygulanmayacağına yönelik düzenleme getirilmiştir. Yapılan bu değişiklikle terör örgütü olması koşulu ile bu terör örgütüne üye olanlar (TCK md.220/2), örgüt içindeki hiyerarşik yapıya dahil olmamakla birlikte, örgüte bilerek ve isteyerek yardım edenler (TCK md.220/7) ve örgütün veya amacının propagandasını yapanların(TCK md.220/8) iletişimi denetim altına alınabilecektir.[1094]

3.2.3.1.3. Suç Vasfının Değişmesi

Telekomünikasyon yoluyla yapılan iletişimin denetlenmesi tedbiri, ancak belli suç tipleri için başvurulabilen bir yöntemdir. Bu tedbirin uygulanabileceği suç tipinin dar tutulması,

[1094] ÇOLAK/TAŞKIN, s.635.

tedbire başvurmak isteyip de yasal engeller nedeniyle başvuramayan kolluk için bir handikap oluşturmaktadır. Gerçekten de, bazı suçların katalog dahilinde olmaması özellikle kolluk tarafından eleştirilmektedir. Bu engelin aşılması için kullanılan yöntemlerden biri, suçun vasfının değiştiği şeklinde yorumlara gidilmesi olabilmektedir.

Bu tedbirin uygulanması esnasında, suç vasfının değişmesi halinde nasıl bir yol izleneceğine dair kanunda açık bir düzenleme bulunmamaktadır. Eylemin katalog dışı bir suça dönüştüğü anlaşıldığında, tedbirin gecikmeksizin sonlanacağı konusunda tartışma yoktur. Suç vasfının değişmesi, yeni suçun da katalogda yer alan başka bir suç olduğunun anlaşılması halinde de tedbire son verilmesi gerekir. Bununla birlikte, ortaya çıkan yeni suça göre, tedbirin koşullarının yeniden ele alınması ve buna göre yeniden bir hakim kararı verilmesi gerektiği öğretide savunulmaktadır[1095]. Ancak burada sorun olan husus, suçtaki vasıf değişikliğin kim tarafından ve nasıl değerlendirileceğidir. Bu sebeple, suçun vasıf değişikliğinin söz konusu olduğu hallerde, tedbirin uygulanmasına hemen son verilmeyerek, durumun kararı veren mahkemeye bildirilmesi ve mahkemeden buna ilişkin ek karar alınması sorunu klasik bir şekilde çözmek anlamına gelir.

Kanaatimizce, tedbirin sonlandırılmasını gerektiren bir halin ortaya çıkması halinde, Cumhuriyet Savcısının vereceği bir kararla uygulamanın nihayetlendirilmesi usul ekonomisi bakımından yararlı olacaktır. CMK'nın 103. maddesinde yer alan uygulama benzeri bir usulle konunun hakim önüne taşınması ihtiyacı ortadan kaldırılabilecektir. Bilindiği üzere, soruşturma evresinde Cumhuriyet savcısı adli kontrol veya tutuklamanın artık gereksiz olduğu kanısına varacak olursa, şüpheliyi kendiliğinden serbest bırakabilmektedir. Keza, kovuşturmaya yer olmadığı kararı verildiğinde de şüpheli salıverilmektedir. Bu uygulamaya benzer bir yöntemle, suç vasfının değişmesi nedeniyle tedbire son verilmesi gerektiğinde, bu işlemin Cumhuriyet Savcısının emriyle gerçekleştirilmesinin uygun olacağını düşünmekteyiz.

3.2.3.2.Kuvvetli Suç Şüphesinin Bulunması

3.2.3.2.1. Şüphe Kavramı

Şüphe, zihnin çeşitli alternatifler arasında seçme yapma konusunda tereddüt etmesi, hangi seçeneğin doğru olduğunu kestirememesi durumudur. Basit şüphe, fiilin suç olması ve soruşturulabilir nitelik arz etmesidir. Yeterli şüphe, eldeki delillere göre

[1095] ÜNVER/HAKERİ, s. 238;ÇOLAK/TAŞKIN, s.636.

yapılacak muhakeme sonucunda sanığın mahkum olması ihtimalinin beraat etme ihtimaline göre daha kuvvetli olması halini belirlerken, makul şüphe, hayatın akışına göre somut olaylar karşısında genellikle duyulan şüpheyi tanımlamaktadır[1096]. Kuvvetli şüphe ise, mevcut delillere göre yapılacak muhakeme sonucunda mahkum olma ihtimalinin kuvvetle muhtemel olmasıdır[1097].

Hak ve hürriyetlere müdahale niteliği taşıyan düzenlemelerle ilgili sınırlayıcı koşulların teferruatlı olarak düzenlenmesini yine hakkın korunması için bir koruma olarak algılayan AİHM, bir kimsenin belirli suçları işlemeyi planladığına, işlemekte olduğuna veya işlediğine dair kuşku duymak için maddi belirtilerin bulunması gerektiğini ifade etmektedir[1098]. Bu yaklaşım, ABD hukukunda makul sebep (probable cause) olarak adlandırılmakta ve muhik neden olmadıkça Anayasa ile muhafaza altına alınan alandan devletin el çekmesini öngörmektedir. Somut bir suçu işlediğine ya da işlemekte olduğuna ilişkin makul bir sebep bulunduğu takdirde, kişi hakkındaki anayasal koruma sonlandırılacaktır[1099]. Şüpheyi somut belirtilerin üzerine kuran Mahkemenin bu tavrı, devletlere tanınan takdir yetkisini daraltan, bireylerin haklarını genişleten bir tavırdır.

Türk hukukunda iletişimin denetlenmesi tedbirine başvurulabilmesi için bir suçun işlenmiş veya işleniyor olduğuna dair kuvvetli şüphe bulunması gerektiği CMK'nın 135. maddesinde vurgulanmıştır. Ancak bu şartı anlamlı kılan, bulunması gereken şüphenin derecesidir. Suçun işlenmiş olduğuna dair şüphenin bulunduğundan söz edebilmek için her halükarda somut bir dayanak noktası olmalıdır[1100]. Suçun istatistiksel sıklığı, kişinin daha evvel aynı suçu işlemiş olması gibi olgular herhangi bir somut dayanakla desteklenmediği sürece bu tedbir için yeterli sayılması mümkün değildir[1101]. Bu tedbirin uygulanması için, şüphenin somut olguya dayanması kriterinde, iletişimin denetlenmesi açısından yeterli olacak şüphede bir kısım ek niteliklerin aranması da yaygın bir

---

[1096] Makul şüphe konusunda AİHM'nin 22.10.1997karar tarihli Erdagöz – Türkiye ve 30.08.1990 karar tarihli Fox, Campell ve Hartley - Birleşik Krallık davası kararlarına bakılabilir.

[1097] GÖKCEN, s.66; ÇOLAK/TAŞKIN, s.628.

[1098] KLASS-ALMANYA, Pr. 51.

[1099] 'The purpose of the probable-cause requirement is … to keep the state out of constitutionally protected areas until it has reason to believe that a specific crime has been or is being committed is thereby wholly aborted'.(ELECTRONIC SURVEILLANCE AND THE FOURTH AMENDMENT.)

[1100] ÖZBEK, s. 424;MALKOÇ/YÜKSEKTEPE, s. 372.

[1101] ÖZTÜRK/ERDEM, s.266; KEKLİK, s.230.

uygulamadır. Bu nitelikler genellikle şüphenin kuvvetli olması veya belli suçlara ilişkin olması şeklinde ortaya çıkmaktadır[1102].

3.2.3.2.2. Kuvvetli Suç Şüphesi

İletişimin denetlenmesine ilişkin olarak, CMK 135. maddesinde şüphenin niteliği, "suç işlendiğine ilişkin kuvvetli şüphe sebeplerinin varlığı" şeklinde somutlaştırılmıştır. Burada dikkat edilmesi gereken husus, şüphenin kuvvetli olmasının, hakkında tedbire başvurulacak kişinin suçu işlemesi bakımından değil, soruşturmaya veya kovuşturmaya konu suçun herhangi biri tarafından işlenmesi bakımından aranacağıdır. Hakkında tedbire başvurulacak kişi bakımından ise soruşturmaya veya kovuşturmaya konu suçu işlediğine dair kuvvetli şüphe bulunmasının aranmayacağını belirtmek gerekir. Bu kapsamda, bu tedbire başvurulabilmesi için başka türlü delil elde edilememesi gerektiği kanunda açıkça öngörülmüştür[1103].

Kuvvetli suç şüphesinin aranması ve ayrıca başka surette delil elde etme imkanının bulunmaması şartlarının birlikte aranmasının, bu tedbirin uygulanmasını zorlaştıracağı düşünülebilir[1104]. Bununla birlikte, tedbirin kişilerin özel hayatına, haberleşme özgürlüğüne yönelik ağır ve derin bir müdahale olması nedeniyle, suçları aydınlığa kavuşturmada görevli makamların kolaycılığa kaçarak, hemen iletişimin denetlenmesi yoluyla delil elde etmeleri engellenmek istenmiştir. Çünkü bu tedbirin delil elde etmede son çare olarak uygulanmasının amaçlandığı ve istisnai bir tedbir olduğu kanun koyucunun iradesinden anlaşılmaktadır[1105].

Tedbirin uygulanması bakımından CMK'nın 137/3. maddesinde tedbirin sona ereceği hallerden birinin de, tedbirin uygulanması sırasında şüpheli hakkında kovuşturmaya yer olmadığına dair karar verilmesi olduğu belirtilmiştir. Kovuşturmaya yer olmadığı kararı özellikle suç şüphesinin kamu davası açmaya yeterli olmaması durumunda verileceğinden, tedbirin henüz yeterli suç şüphesinin oluşmadığı bir dönemde verilmiş olması ve tedbire rağmen de bu kuvvetli suç şüphesi seviyesine ulaşılamadığı için tedbire son verilecektir[1106].

[1102] ÇOLAK/ TAŞKIN, s.445; ÖZBEK, Veli Özer/DOĞAN, Koray/BACAKSIZ, Pınar/KANBUR, M. Nihat: Ceza Muhakemesi Hukuku Bilgisi, Ankara 2007, s.568.

[1103] KEKLİK, s. 230;

[1104] ÖZTÜRK/ERDEM, s.602.

[1105] ÜNVER/ HAKERİ, s. 173-174; MALKOÇ/YÜKSEKTEPE, s. 372.

[1106] ÜNVER/ HAKERİ, s. 174.

“Kuvvetli belirti” ifadesi, 4422 sayılı Kanun’da kullanılmakta ve “şüphe” ile “belirti” kavramları kesin olarak birbirinden ayrılmaktaydı. İletişimin denetlenmesi kararı verilebilmesi için haricen algılanabilen kuvvetli belirtilere bağlı somut olgular aranmasına karşılık CMK’nın 135. maddesinde 4422 sayılı Kanundan farklı olarak “belirtiden” değil “kuvvetli şüphe sebeplerinden” söz edilmektedir. CMK’nın 100. maddesinin birinci fıkrasında tutuklama kararı verilebilmesi için “kuvvetli suç şüphesinin varlığını gösteren olgu” aranırken iletişimin denetlenmesine karar verilebilmesi için “kuvvetli şüphe sebebi” aranmaktadır. Bu iki şüphe derecesi arasında mutlaka bir fark bulunması gerekmektedir. Zaten tutuklama kararı verecek kadar kuvvetli suç şüphesi varsa iletişimin denetlenmesi tedbirine başvurulamaz[1107].

Öğretide, “şüphe” ile “belirti “ kavramları arasındaki ayırımın yapılması gerektiği ifade edilmektedir. İletişimin denetlenmesi kararı verilebilmesi için “çok basit” bir suç şüphesinin varlığı yeterli ise de, suç işlendiğine ilişkin “belirtilerin kuvvetli” olmasının zorunlu olduğu dile getirilmektedir. Ayrıca buradaki amacın keyfiliği önlemek , somut olgulara dayanan kuvvetli belirtilerin varlığını saptamak, fakat kişi hakkındaki şüphenin henüz yoğunlaşmamış olması durumunda da, iletişimin denetlenmesi kararının verilmesini sağlamak olduğu ve bu kapsamda 5271 sayılı CMK’nın değiştirilerek 4422 sayılı kanundaki “kuvvetli belirti” kriterinin getirilmesi gerektiği savunulmaktadır[1108].

Ayrıca öğretide, iletişimin denetlenmesi tedbirine karar verilebilmesi için kuvvetli şüphe şartının aranmasını, hak ve hürriyetlerin keyfi olarak çiğnenmesinin önlenmesi adına yapılmış bir yanlışlık olduğu savunulmaktadır. Bu görüşe göre, bu tedbire başvurabilmek için yakalamanın da ön şartı olan kuvvetli şüphe standardına ulaştıracak iz, belirti, emare veya delilin kolluğun elinde olması durumunda, zaten bu tedbirlere başvurmaya gerek olmayacağı, bu nedenlerle iletişimin denetlenmesinde yakalama ve tutuklama standardında kuvvetli şüphe aranmasının yanlış olduğu, makul şüphenin yeterli kabul edilmesi gerektiği ifade edilmektedir[1109]. Bu konuda orta yolu arayanlarda mevcuttur[1110]. Kanun koyucunun 135. maddenin aşırı kullanımını engellemek amacıyla bu kriteri ortaya koyduğu, iletişimin denetlenmesi tedbirine başvurulmasında, şüpheli tarafından suçun işlendiği şüphesini kuvvetli bir şekilde ortaya koyacak delil ve

---

[1107] KUNTER/YENİSEY/NUHOĞLU, s. 702.

[1108] KUNTER/YENİSEY/NUHOĞLU, s.702.

[1109] ERYILMAZ, Mesut Bedri, Suçla Mücadele Politikası Açısından Yeni Ceza Muhakemesi Kanunu, Ceza Hukuku Dergisi, Sayı 1, Eylül 2006,, s. 224.

[1110] TAŞKIN, s.102-104.

emarelerin öncelikle elde edilmesi olarak nitelendirilebilecek derecede bir zorluk öngörülmediği de öğretide ifade edilmektedir[1111].

Kanaatimizce, kanun koyucu tarafından belirlenen 'kuvvetli şüphe' kriteri isabetlidir. Çok katı olarak bina edilen bazı kurumların zaman içinde gevşediği, uygulayıcının, keşfettiği alternatif yollarla çabuk çözüm getiren yollara tevessül ettiği gerçeği karşısında, hürriyetlerin özüne ilişkin tedbirlerde kuralların katı kurulmasının doğru olduğunu düşünmekteyiz. Bu 'kolaycı' yöntemler sadece kolluğun uyguladığı yollar değildir. Bu tür yollar hakim ve savcılar tarafından da tercih edilmektedir. Buna en yakın örnek olarak, yeni CMK ile getirilmiş uzlaşma kurumunun kısa bir sürede by-pass edilmesi gösterilebilir.

Öte yandan, CMK'nın, "kuvvetli şüphe sebepleri"nin varlığını zorunlu kılması ile, AİHM'nin, 'güçlü şüphe düzeyi' kriteri karşılanmış olmaktadır. AİHM, bir kimsenin, bir suça ilişkin fiilleri ciddi olarak işlemeyi planladığını ya da işlemekte olduğunu ya da işlediğini gösteren kuvvetli maddi belirtilerin bulunması halinde ve diğer yöntemlerle bu tür delillerin elde edilmesinin mümkün olmadığı anlaşıldığında, iletişimin denetlenmesi tedbirine başvurulmasını haklı görmektedir. Başka yöntemlerle delil elde etmenin mümkün bulunmamasının yanı sıra, çok güç olması hali de bu tedbire başvurulması için yeterli şartların oluştuğu anlamına gelir[1112].

3.2.3.3.İletişimin Denetlenmesi Tedbirine Son Çare Olarak Başvurulabilmesi

Başka yollarla delil elde edilmesinin mümkün olduğu hallerde başvurulamayacak bir tedbir olan iletişimin denetlenmesi, madde gerekçesinde de belirtildiği üzere "son çare" olarak başvurulacak bir tedbirdir. Başka tedbirlerle olayın aydınlatılması ve delil elde edilmesi mümkün ise, bu tedbire başvurulması mümkün değildir[1113]. Katalog suçlarla ilgili olarak verilen tedbir kararının icraya başlanmasından sonra başka tedbirlerle delil elde edilebilmesi ya da başka bir surette delil elde edilmesi imkanının doğması halinde, tedbire son verilmelidir. Nitekim, tedbir için zorunlu olan koşullar ortadan kalkmıştır[1114]. Ancak burada diğer tedbirlerin uygulanması ve bu şekilde delil elde edilememiş olmasından ziyade bu tedbire başvurulsa dahi sonuç alınamayacağına yönelik bir

---

[1111] ŞEN, (İletişimin Denetlenmesi Tedbiri), s. 105-106.

[1112] Bk. KLASS-ALMANYA.

[1113] KÜNHE, s. 105.; ŞAHİN, s. 379.; ŞAHİN, Ceza Muhakemesi Hukuku, s.268

[1114] ÇOLAK/TAŞKIN, s. 629.

beklentinin varlığı önemlidir[1115]. Bu bağlamda, klasik ceza muhakemesi yöntemleri ile delil elde edilmesi mümkün iken, olağanüstü bir tedbir niteliğinde olan iletişimin denetlenmesi tedbirinin uygulanması sonucu elde edilen delillere dayanılarak hüküm tesis edilmesi mümkün olamayacaktır[1116]. Bu değerlendirmeyi yapacak makam olan Mahkeme, iletişimin denetlenmesi suretiyle elde edilen bilgilerin, buna ilişkin koşullara uygun olarak elde edilip edilmediğini irdelemek zorundadır. Eğer koşullardan bazılarına uyulmaksızın delil elde edilmişse, mahkeme bu delili yargılamada kullanamayacak ve de delil değerlendirme yasakları ile karşı karşıya kalınabilecektir[1117].

İkinci derecede uygulanabilirlik[1118] ya da başka bir surette delil elde etme imkanının bulunmaması[1119] olarak da adlandırılan bu ilke, AİHM ve ABD hukukunda kabul edilmiş bir yaklaşımdır. AİHM yaklaşımına göre, bir kimsenin bir suça ilişkin fiilleri ciddi olarak işlemeyi planladığına, işlemekte olduğuna ya da işlediğine dair kuvvetli maddi belirtilerin bulunması halinde ve diğer yöntemlerle bu tür delillerin elde edilmesinin mümkün olmadığı anlaşıldığında, iletişimin denetlenmesi tedbirine başvurulabilir. Başka yöntemlerle delil elde etmenin mümkün bulunmamasının yanı sıra çok güç olması halleri de bu tedbire başvurulması için yeterli şartların oluştuğu anlamına gelir[1120]. AİHM, iletişimin denetlenmesine başvurulacak dava sayısını azaltmak ve mahremiyete yönelik riskleri en aza indirgemeyi hedefleyen bu ilkeyi[1121], uygulayıcıların keyfi birtakım uygulamalara yeltenmesinin önlenmesi bakımından önemli görmektedir[1122].

Son çare olarak başvurulması gerekli olan iletişimin denetlenmesi tedbiri, uygulamada, olması gerekenden daha erken kapısı çalınan bir koruma tedbiri olarak karşımıza çıkmaktadır. Ülkemizde, diğer normal soruşturma teknikleri tüketilmeden bu 'sıra dışı' yola başvurulmakta, suç konusu olayın vuku bulmasından daha saatler geçmeden bu tedbir devreye konulmaktadır. Kanaatimizce, iletişimin denetlenmesi tedbirinin en son

---

[1115] TURHAN, s. 268; ÇOLAK/TAŞKIN, s. 629; ŞEN, (İletişimin Denetlenmesi Tedbiri), s. 107; ŞAHİN, s. 379; KUNTER/YENİSEY/NUHOĞLU, s. 704.

[1116] ÇOKSEZEN, Atakan: 5271 Sayılı Ceza Muhakemesi Kanunu ve Avrupa İnsan Hakları Sözleşmesi Çerçevesinde Ceza Muhakemesi Tedbiri Olarak İletişimin Dinlenmesi, İstanbul 2006, s. 8.

[1117] TAŞKIN, s.107.

[1118] ERDEM, Gizli Soruşturma, s.320.

[1119] ŞEN, (İletişimin Denetlenmesi Tedbiri), s. 101.

[1120] DOĞRU, s. 243.

[1121] DONOHUE, s.8; AN OVERVIEW OF ELECTRONIC SURVEILLANCE: History And Current Status, D.1.2; EHRLICH, s. 8.

[1122] KÜNHE, s. 105.

çare (ultima ratio) olarak kullanılması, mutlaka sıkı sıkıya uyulması gerekli olan bir şart olarak algılanmalıdır. Nitekim, bu ilke, kaynağını kanunun emredici hükmünden almaktadır.

3.2.3.3.1. Orantılılık İlkesi ve Son Çare Şartı

Orantılılık ilkesi uyarınca, bir hakka müdahalenin hakka en az zarar verecek şekilde yapılmış olması gerekmektedir. Orantılılık ilkesinin somut bir görünümü olarak, iletişimin denetlenmesi tedbirine, haberleşme özgürlüğüne ağır müdahale oluşturması nedeniyle, son çare şartı çerçevesinde ancak başka türlü delil elde etme imkanının bulunmaması halinde başvurulabilecektir. Bu şart, aynı amaca hizmet eden ve gerçeğin ortaya çıkarılmasına yarayacak iki tedbir arasında öncelik-sonralık ilişkisini ifade ettiğinden, aynı suçu aydınlatmak üzere başvurulabilecek birden fazla tedbir arasında bir karşılaştırma yapılmasını ve bunlardan temel hak ve hürriyetlerine en az müdahalede bulunan hangisi ise, onun seçilmesini ifade etmektedir. Bu kapsamda CMK'nın 135/1. maddesinde, bu tedbire başvurmak için "başka surette delil elde edilmesi olanağının bulunmaması" koşuluna yer verilmek suretiyle bu tedbirin diğer tedbirlere göre ikincil nitelikte olduğu ve bir anlamda başka çare olmaması halinde uygulanabileceği vurgulanmak istenmiştir[1123].

İkinci derecede uygulanabilirlik şartının gerçekleşmiş sayılabilmesi için, soruşturmanın başında veya soruşturma sürerken başka bir tedbire başvurulması durumunda olayın aydınlatılmasını imkansız kılan bir engel ile karşılaşılması ya da soruşturma kapsamında başka türlü delil elde etme imkanının olmaması gerekir. Soruşturma veya kovuşturma aşamasında delil elde etme amacıyla başka bir tedbire başvurmanın sonuca ulaşmayı güçleştirecek olması, iletişimin denetlenmesi tedbirine başvurmak için yeterli değildir. İletişimin dinlenmesi tedbirine karar vermeden önce diğer tedbire başvurulmuş ve bundan sonuç alınmamış olması gerekmez; bunlara başvurulduğunda sonuç alınamayacağı konusunda bir beklentinin varlığı yeterlidir. Bu yüzden de, bu şartın, tedbirin uygulama alanını sınırlandırmak bakımından etkisi azdır. Gizli olması yüzünden kötüye kullanılma tehlikesi bulunan telekomünikasyon yoluyla yapılan iletişimin denetlenmesi ile, arama, elkoyma, tutuklama gibi diğer geleneksel koruma tedbirleri arasında öncelik-sonralık ilişkisi olması sebebi ile aynı ölçüde soruşturma ve kovuşturma aşamasında delil elde edilmesini

[1123] KAYA, s. 93 ; TURHAN, s.268;ERDEM, s 100; ÇASÖMK m. 2/3'de, "başka bir tedbir ile failin belirlenmesi, ele geçirilmesi veya suç delillerinin elde edilmesi mümkün ise" bu tedbire başvurulamayacağı öngörülmüştü.

sağlayarak olayı aydınlatma şansı bulunan diğer koruma tedbirleri, telekomünikasyon yoluyla yapılan iletişimin denetlenmesine göre bir önceliğe sahiptir[1124].

ABD hukukunda, son çare prensibinin açıklandığı Madde 2518(3)'e göre iletişimin denetlenmesi imkanının kullanılabilmesi için, iletişimin denetlenmesi dışındaki soruşturma yöntemlerinin kullanıldığı, ancak bu yöntemlerin başarısız olduğu, bu tedbir dışındaki yöntemlerin kullanılması durumunda başarı elde edilemeyeceğine ilişkin bir kanaat olduğu veya bu tedbir dışındaki yöntemlerin kullanılmasının çok tehlikeli olduğu tespit edilmelidir[1125]. Görüldüğü gibi, ABD hukukunda, Strasbourg hukukundan farklı olarak bir üçüncü kriter belirlemiştir. Bu tedbire başvurulması için, diğer yöntemlerin başarısızlığı ve imkansızlığı kriterlerinin yanı sıra, diğer yöntemlerin tehlikeliliği de bu tedbire başvurulmasını mazur gösteren bir haldir.

Diğer yöntemlerin tehlikeli olması kriterinin ülkemiz hukukunda uygulanması sağlanabilir mi? Tedbir kararının bir mahkeme tarafından verilecek olması, başka bir ifadeyle bu tedbire başvurulması talebini havi istemin hukuki bir süzgeçten geçecek olması, tehlikelilik gerekçesiyle iletişimin denetlenmesi tedbirine başvurulması hususunda bir sigorta olarak algılanabilir. Bununla birlikte, ABD uygulamasında, iletişimin denetlenmesi kararı için başvuruda bulunan kolluk görevlisinin, kararı verecek hakime, "diğer yöntemleri kullanmak zor" şeklinde bir beyanda bulunmasının dahi son çare prensibinin şartlarını karşılamak olarak değerlendirildiği ifade edilmektedir[1126]. Örneğin ABD-Garcia, kararında mahkeme, elektronik takip için diğer tüm normal yolların tüketilmiş olmasının gerekli olmadığını, diğer normal yolların tüketilmiş olması prensibinin aslında mahkeme hakimine diğer geleneksel yollarda karşılaşılan güçlüklerin bildirilmesi anlamına geldiğini ifade etmektedir.[1127] Bu ve benzeri örnekler, son çare prensibinin gerektiği gibi hayata geçirilmemesi olarak yorumlanmaktadır. Bu nedenlerden dolayı, ülkemiz uygulamasına 'diğer yöntemlerin tehlikeliliği' kriterinin de eklenmesinin tehlikeli bir inisiyatif almak anlamına geleceğini düşünmekteyiz. Tehlikelilik, istisnalar saklı kalmak kaydıyla, sübjektif bir kavramdır. Kişi hak ve

---

[1124] ÖZTÜRK/ERDEM, s. 603; ERDEM, s. 100; KUNTER/YENİSEY/NUHOĞLU, s. 704.

[1125] 18 U.S.C. § 2518(3); DONOHUE, s. 8; AN OVERVIEW OF ELECTRONIC SURVEILLANCE: History And Current Status, D.1.2; ÖZDOĞAN (2004), s. 33; EHRLICH, s. 8.

[1126] ÖZDOĞAN, (2004), s.100; DEMPSEY, "Communications Privacy In The Digital Age: Revitalizing The Federal Wiretap Laws To Enhance Privacy".

[1127] DEMPSEY, "Communications Privacy In The Digital Age: Revitalizing The Federal Wiretap Laws To Enhance Privacy".

hürriyetlerinin sınırlandırılmasında daraltıcı bir yorum yapmayı tercih eden AİHM içtihatları doğrultusunda denilebilir ki, böyle bir kriter suiistimallere neden olabilecektir.

3.2.3.3.2. İletişimin Denetlenmesi Tedbiri ile Diğer Gizli Soruşturma Tedbirleri Arasındaki Öncelik- Sonralık Sorunu

İletişimin denetlenmesi tedbirinde aranan ikinci derecede uygulanabilirlik şartı ile ilgili olarak üzerinde durulması gereken diğer bir sorun da, bu tedbir ile, CMK'nın 139. maddesinde yer alan gizli görevli kullanma ve CMK'nın 140. maddesinde yer alan teknik izleme tedbirleri arasında da öncelik-sonralık ilişkisinin bulunup bulunmadığıdır. Gerçekten "başka surette delil elde edilmesi olanağının bulunmaması" şartına bu tedbirler bakımından da kanunda açıkça yer verilmektedir. Oranlılık ilkesinin gereği olarak, somut olayda bu tedbirlerden hangisi aynı sonuca ulaşmak bakımından, temel hak ve hürriyetlere daha az müdahale oluşturuyorsa, o tedbirin önceliğe sahip olduğu kabul edilmelidir. Bununla birlikte, olayın aydınlatılması bakımından, gerektiğinde her üç tedbire aynı olayda birlikte başvurulabilmesi de mümkündür. Bu bağlamda, temel hak ve hürriyetlere yönelik müdahalenin ağırlığına göre gizli soruşturma tedbirlerinin uygulanma koşulları ve öngörülen muhakeme güvenceleri açısından bir ayırıma gidilmemiş ise de; yine de, bizzat gizli soruşturma tedbirleri arasında da, müdahalenin yoğunluğuna göre bir öncelik-sonralık sırasının izlenmesi, oranlılık ilkesinin bir gereğidir[1128]. Yapılan soruşturma veya kovuşturmada her üç gizli soruşturma tedbirine birden başvurulmasının zorunlu olması halinde, her bir tedbir açısından kanunda öngörülen şartların oluşması ve her bir tedbire ilişkin kararın ayrı ayrı verilmesi gerekmektedir.

3.2.3.4.İletişimin Denetlenmesinin Belirli Kişiler Hakkında Uygulanabilmesi

İletişimin denetlenmesi tedbiri temelde sanık ve şüpheliye yönelik olarak uygulanacağı mevcut düzenlemeden anlaşılmaktadır. Ancak şüpheli ve sanıkla iletişim kuran üçüncü kişilerin iletişimi, dolaylı olarak kanun kapsamına alınmıştır. Bundan dolayı, hakkında iletişimin denetlenmesi tedbirine karar verilmemiş olan üçüncü kişilerle ilgili tedbir kapsamında elde edilen deliller, kanunda sayılan katalog suçların veya bu suçlarla bağlantılı diğer suçların ispatında kullanılabilecektir. Buna göre, denetim kapsamında delil elde edilmesi halinde, bu delil muhafaza altına alındıktan sonra Cumhuriyet savcısı durumdan derhal haberdar edilir. Bu durumda şüpheli haline gelen üçüncü kişi ile alakalı yeni bir karar

[1128] TURHAN, s.268; ERDEM, s.100; YİĞİT, s. 19.

alınmalıdır[1129]. Aynı şekilde hakkında iletişimin denetlenmesi kararı verildiğinde yalnızca şüpheli veya sanığa ait iletişim araçları değil aynı zamanda şüpheli veya sanığın üzerine kayıtlı olmasa da , onlar tarafından kullanılan üçüncü kişilere ait iletişim araçları da denetim kapsamındadır[1130]. Şüpheli veya sanığın kullandığı iletişim aracı bir şirkete, derneğe ya da siyasi bir partiye ait ise bunlar da dinleme kapsamına alınabilecektir[1131]. Ancak üçüncü kişiye ait olan ve denetlenecek olan iletişim aracının şüpheli veya sanık tarafından kullanıldığına dair kuvvetli şüphe sebeplerinin bulunması zorunludur. Aksi takdirde, tedbirin uygulama alanı çok genişleyeceğinden, bir başkasının kullandığı iletişim aracının denetlenmesi sonucu ortaya çıkar. Bu durumda da tedbirin şüpheli ya da sanığa uygulanmasından ziyade üçüncü kişiye uygulanması söz konusu olacaktır[1132]. Hakkında iletişimin denetlenmesi tedbiri kararı verilen kişi ile iletişim aracının sahibi farklı kişilerse, bu durum talep ve kararda açıkça belirtilmelidir[1133]. Şüpheli veya sanığın, kartlı veya jetonlu telefon gibi kamuya açık telefonları kullanmaları halinde bu iletişim vasıtalarının hukuki durumunun ne olacağı tartışmalıdır. Bu tür vasıtaların denetlenmesinin hukuka uygun olacağı şeklindeki[1134] görüşe biz de katılmaktayız. Bununla birlikte, bu uygulamanın sadece şüpheli ya da sanığın kullandığı cihaz ya da cihazlara hasredilmesine dikkat edilmelidir. Yapılan bir soruşturma kapsamında bir bölgedeki tüm ankesörlü ya da kamuya açık telefonların denetlenmesine izin veren bir kararın çıkarılması AİHM ilkelerinin göz ardı edilmesi anlamına gelecektir.

İletişimin denetlenmesi tedbirine başvurmak için muhakemenin hangi aşamasında bulunulduğu önem taşımamakla birlikte, "kovuşturmaya yer olmadığı kararı" verilmiş ise, kişi artık "şüpheli" sıfatını kaybettiği için, bu karardan sonra aynı kişiye yönelik olarak bu tedbire başvurulamaz. Bundan dolayı CMK'nın 137/3. maddesinde "şüpheli hakkında kovuşturmaya yer olmadığına dair karar verilmesi" durumunda tedbire son verileceği

---

[1129] ÖZBEK, s.426; ABD hukuk tarihinde bu hususa ilişkin olarak verilmiş ilginç bir karar olarak not edilen 1974 tarihli Kahn davasında (United States v. Kahn) Yüksek Mahkeme, bir mahkeme kararı olmaksızın yapılan dinleme sonucunda elde edilen delillerin sanık aleyhine kullanılabileceği gibi ciddi sonuçlar doğuran bir karar vermiştir. Irving Kahn hakkında, mahkeme kararı alınarak yapılan dinleme neticesinde elde edilen delillerle dava açılmıştı. Dinlemeye konu telefon görüşmelerin bir kısmı Kahn ile karısı Minnie arasında cereyan etmekte idi. Minnie hakkında alınmış bir dinleme kararı bulunmamasına rağmen elde edilen bu delillerle Minnie hakkında suçlamalarda bulunuldu. Dinleme kararının kocası hakkında alındığını, bu kararın kendisine teşmil edilemeyeceğini ifade eden Minnie'nin bu iddiası mahkeme tarafından kabul görmedi. Mahkemeye göre ; adı geçmese de, Minnie, Teknik Dinleme Kanunu uyarınca, iletişimin denetlenmesinin uygulanmasını mümkün kılan suçlardan birini işlemiştir. ÖZDOĞAN, (2004), s.18.

[1130] ÇOLAK/TAŞKIN, s.625; TURHAN, s.266-167; ÖZBEK/DOĞAN/BACAKSIZ/KANBUR, s.568; ÖZBEK, s.426.

[1131] DÖNMEZER, s.20.

[1132] CENTEL/ZAFER, s.365.

[1133] ÇOLAK/TAŞKIN, s.625.

[1134] KUNTER/YENİSEY/NUHOĞLU, s.699.

belirtilmek suretiyle bu husus vurgulanmıştır. Aynı durum kesin kararın verilmesi için de geçerlidir. Verilen karar ister beraat, isterse mahkumiyet biçiminde olsun, şüphe ortadan kalktığı için tedbire başvurulması artık mümkün değildir[1135]. Bununla birlikte, aynı kişiye ilişkin yeni kuvvetli şüphe sebeplerinin ortaya çıkması halinde yeniden tedbir talep edilebilir.

CMK'nın 135/2. maddesinde hem şüpheli hem de sanıktan bahsedilmek suretiyle, bu tedbirin dava açıldıktan sonra da uygulanabileceği belirtilmiştir. Bu ifade tarzının doğru olduğunu ifade edenler olduğu gibi[1136], bu denetleme tedbirine yalnızca soruşturma aşamasında başvurulabileceğini savununlar da vardır[1137]. Özellikle iletişimin tespiti bakımından kovuşturma aşamasında aranan sanıkların yakalanması amacıyla bu tedbir uygulama alanı bulabilmektedir[1138]. Bize göre, uygulamada çokça uygulanmasa da kovuşturma aşamasında iletişimin denetlenmesi tedbirine başvurulmasına imkan veren madde hükmü isabetlidir. Kovuşturma aşaması, sanık hakkındaki yargılamanın henüz bitmediği bir evre olduğundan, bu aşamada da kişi hakkında elde edilecek bazı ek bilgilerin olabileceği unutulmamalıdır. Özellikle tutuksuz yargılanan kişilerin iletişimlerinin denetlenmesi suretiyle ek birtakım delillerin elde edilebileceği muhakkaktır.

Hakkında hüküm kesinleşmiş olan bir kişi hakkında, bu kişinin yakalanması amacıyla iletişiminin denetlenmesi kararı hiçbir şekilde verilememektedir[1139]. Doktrinde bazı yazarlar, hükümlülerin yakalanması amacıyla mobil telefonun yerinin tespitine karar verilebilmesinin gerekli olduğunu savunmaktadırlar[1140]. Kanaatimizce bu görüş isabetlidir. Suçluluğu mahkeme kararıyla belirlenmiş kişinin cezasının infazını mümkün kılmak amacıyla bu tedbire başvurulması yararlı olacaktır.

Bütün bu farklı değerlendirmelerden de anlaşılacağı üzere iletişimin denetlenmesini düzenleyen CMK'nın 135/2. maddesi açık bir şekilde kaleme alınmamıştır[1141]. Maddenin sadece şüpheli ve sanığı kapsayacak şekilde yazılmış olması, hakkında iletişimin denetlenmesi tedbiri uygulanabilecek diğer muhtemel kişiler hakkında düzenleme yapılmamış olması bir eksikliktir. Aslında maddenin bu yönü, AİHM tarafından belirlenmiş açıklık ve öngörülebilirlik kriterlerinin ihlali anlamına gelmektedir.

[1135] ÖZTÜRK/ERDEM, s.605; ERDEM, s.101.

[1136] ÖZTÜRK-ERDEM, s. 605.

[1137] CENTEL/ZAFER, s.316; TAŞKIN, s.98-99; KUNTER/YENİSEY/NUHOĞLU, s. 698.

[1138] ÜNVER/ HAKERİ, s.174; KUNTER/YENİSEY/NUHOĞLU, s. 698.

[1139] KUNTER/YENİSEY/NUHOĞLU, s.699.

[1140] TAŞKIN, s.99.

[1141] ÜNVER/ HAKERİ, s.174.

Gerçekten de AİHM, yasal düzenleme şartlarının açık ve net olarak belirtilmesi gereğine işaret etmektedir. Bu husus, keyfi muamelelere başvurulmaması bakımından zorunludur[1142]. Bu itibarla, muhtemel müdahalelerin niteliği, kapsamı, bu tedbirlerin emredilmesi için gerekli sebepler[1143], emri vermeye yetkili merci, uygulayan ve denetleyen birimler, izlenecek usul[1144] gibi hususlar da kanunda ayrıntılı olarak düzenlenmelidir[1145]. Maddenin, bu haliyle, ilgiliye öngörülebilirlik (foreseebility) imkanı tanımaktan da uzak olduğu söylenebilir[1146].

Bu bağlamda, iletişimin denetlenmesi tedbirinin hangi evrelere ilişkin olduğunun açıklanması, kovuşturma aşamasındaki boyutunun izah edilmesi gerekir. Diğer taraftan; hükümlü, müşteki, tanık, kamu görevlileri, milletvekilleri vb. kişilerin durumları hakkında açıklık içeren bir değişiklik yapılması, kanunun belli noktalarda detaycı bir yöntem belirlemesi, hak ve hürriyetlerin keyfi müdahalelere maruz kalmaması bakımından yararlı olacaktır.

3.2.3.5. İletişimin Denetlenebilmesi İçin Hakim Tarafından Karar veya Onay Verilmiş Olması

İletişimin denetlenmesi tedbirine karar verme yetkisi hakime[1147] veya gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısına verilmiştir. Cumhuriyet savcısı tarafından tedbire karar verilmesi halinde bu kararın "derhal" hakim onayına sunulması gerekmektedir. Tedbire savcı tarafından karar verilmesi durumunda, bu kararın yirmi dört saat içinde hakimin onayına sunulması gerekmekte olup, aksi takdirde karar hükümsüz kalacaktır[1148]. Hakim de, en geç yirmi dört saat içinde kararını verecektir. İletişimin denetlenmesi, mahiyeti itibariyle haberleşme özgürlüğüne ağır bir müdahale anlamına gelir ve bu yüzden hakim kararı veya onayı aramak suretiyle özel bir koruma sağlanması isabetlidir. Hakim kararı veya onayı, dengeleme işlevi görmekte ve bundan başka önleyici bir hukuki koruma sağlamaktadır.

[1142] KAYA, s. 92; TEZCAN/ERDEM/SANCAKTAR, s. 238; KILKELLY, s. 25.; RENUCCI, 135.

[1143] RENUCCI, 136.

[1144] ÇOKSEZEN, s. 5.

[1145] ERGEÇ, s. 205; ROTARU-ROMANYA, Pr.57.

[1146] ALCARAZ, s. 229; ŞEN, (İletişimin Denetlenmesi Tedbiri), s. 99.

[1147] Anglo Saxon sisteminde yer alan ABD'den farklı olarak Birleşik Krallık'ta iletişimin denetlenmesine ilişkin kararı İçişleri Bakanı(Home Secretary) verir. Bu kararın verilebilmesi için, RIPA'nın 6. bölümünde sayılan kişiler tarafından yapılmış bir başvuru olması gerektiği gibi, anılan kanunda sayılan birtakım şartların yerine getirilmesi gerekmektedir. RIPA,Bölüm:5 ve 6; bölümlerhttp://www. opsi.gov.uk/ Acts/ acts 2000/ukpga_20000023_en_2#pt1-ch1-pb1-l1g1 , (İET:19.12.2007); FOSTER, s.389.

[1148]ŞEN, (İletişimin Denetlenmesi Tedbiri), s.113; ÖZTÜRK/ERDEM, s.603; ÖZBEK, s.427; CENTEL/ZAFER, s. 364; MALKOÇ/YÜKSEKTEPE, s. 372.; ŞAHİN, s. 379.; ŞAHİN, Ceza Muhakemesi Hukuku, s.269

Hakim tarafından verilen karar, elde edilen bilginin delil hüviyetini kazanması bakımından önemlidir. Yargıtay, kanunla belirlenmiş merciin denetimine tabi olmadan elde edilmiş olan bilgilerin delil olarak sayılamaması şöyle dursun, iletişimin denetlenmesi hakkındaki kararın dosyaya getirtilmemiş, CMK'nın 209. maddesi uyarınca duruşmada okunmamış, ulaşılan kanıtın hukukiliği Yargıtay'ca denetlenebilir açıklıkta olmak üzere hüküm mahkemesi'nce tartışılmamış olmasını, buna karşılık mahkûmiyet hükmüne dayanak teşkil etmesini bozma nedeni saymıştır. Nitekim, Yargıtay Ceza Genel Kurulu'nun 2006 tarihli bir kararında; 'Ancak, mahkûmiyet kararında sübut kanıtı olarak benimsenen telefon görüşmesi de dahil olmak üzere diğer oniki görüşmenin dinlenilmesinin dayanağını oluşturan, iletişimin tespitinin, kim hakkında, hangi iletişim araçları bakımından ve ne süreyle gerçekleştirildiğini gösteren, dolayısıyla telefon görüşmelerine ilişkin kanıtın hukuka uygun biçimde elde edilip edilmediğinin ve kimler hakkında hangi suçla sınırlı olarak kanıt sayılacağının denetlenmesini sağlayacak olan Ankara Devlet Güvenlik Mahkemesi C.Başsavcılığının istem yazısı ile Ankara 1 Nolu Devlet Güvenlik Mahkemesi Yedek Hakimliğinin 07.05.2003 gün ve 563 sayılı dinleme kararı dosyaya getirtilmemiş, CYY'nın 209. maddesi uyarınca duruşmada okunmamış, ulaşılan kanıtın hukukiliği Yargıtayca denetlenebilir açıklıkta olmak üzere Hüküm Mahkemesi'nce tartışılmamış, buna mukabil mahkûmiyet hükmüne dayanak alınmıştır. Bu itibarla, hükmün bu yönüyle de bozulması gerekmektedir ' denilmek suretiyle bu husus önemle vurgulanmıştır[1149].

Genel olarak karşılaştırmalı hukukta da, iletişimin denetlenmesi tedbirine karar verme yetkisi hakime ve hatta hakimler kuruluna tanınmakta, ancak gecikmesinde sakınca bulunan durumlarda Cumhuriyet savcısı da karar verme yetkisine sahip bulunmaktadır[1150]. CMK'nın 135. maddesinde, iletişimin denetlenmesi talebi hakkında karar verecekler arasında mahkemenin belirtilmemiş olması bir unutmadan kaynaklanmaktadır. Bu konudaki belirsizliğin giderilmesi gerekmektedir[1151].

3.2.3.5.1. Görevli ve Yetkili Hakim

Adli amaçlı İiletişimin denetlenmesi tedbiri hakkında, soruşturma aşamasında talepte bulunan savcının bulunduğu yer itibariyle yetkili olan sulh ceza mahkemesi hakimi, kovuşturma aşamasında ise davaya bakan mahkeme karar vermeye yetkilidir[1152]. CMK'nın

---

[1149] CGK, 2006/5.MD-127 E., 2006/180 K., 17.02.2006

[1150] SÖZÜER, s. 110; ERDEM, Mustafa Ruhan, Ceza Muhakemesinde Organize Suçlulukla Mücadelede Gizli Soruşturma, Ankara 2001, (Gizli Soruşturma), s. 334 vd.; CENTEL/ZAFER, s. 363.

[1151] ÜNVER,(CHD), s. 148; ÇOLAK/TAŞKIN, s. 627.

[1152] ŞEN, (İletişimin Denetlenmesi Tedbiri), s. 113.

163. maddesi çerçevesinde, soruşturma işlemlerinin sulh ceza hakimi tarafından yapıldığı durumlarda, sulh ceza hakimi, Cumhuriyet savcısının talebine gerek olmaksızın re'sen iletişimin denetlenmesi tedbirine karar verebilir[1153].

Denetim kapsamındaki suç hangi mahkemenin görev alanına giriyorsa, tedbire o mahkeme karar verebilir[1154]. Özel görevli ağır ceza mahkemelerinin görev alanına giren, yani CMK'nın 250/1. maddesi kapsamındaki suçlar bakımından soruşturma aşamasında farklı bir düzenleme yoluna gidilmemiştir. Kovuşturma aşamasında ise, bu yetki, doğal olarak özel görevli ağır ceza mahkemesine aittir. Kolluğa adli amaçlı iletişimin denetlenmesi tedbirine başvurma imkanı tanınmamıştır[1155]. Birleşik Krallık gibi Anglo Sakson sistemini benimsemiş ülkelerde kolluğa verilen bu yetkinin hukukumuzda kabul edilmemiş olması kanaatimizce doğrudur.

İletişimin denetlenmesi talebini değerlendirecek merci olan hakim, yasal şartların varlığı hususunda yeterli bir araştırma yaptıktan sonra ve somut olayın özellikleri çerçevesinde gerekçeli olarak karar vermelidir. Mahkeme bu anlamda bir tasdik makamı olmaktan çıkarılmalı, şartları oluşmamış tedbir taleplerini reddetmelidir. Bu çerçevede değerlendirilmeden verilmiş bir mahkeme kararının hukuka aykırı olduğu izahtan varestedir[1156]. Bununla birlikte, uygulamada iletişimin denetlenmesi hususunda verilen kararların yeterince değerlendirme yapılmadan verildiği, suçun işlenmesinin hemen sonrasında daha birincil nitelikteki deliller ve soruşturma teknikleri kullanılmadan, başka bir ifadeyle son çare ilkesi dikkate alınmadan bu tedbire başvurulduğu bilinmektedir. Bu şekilde verilen hukuka aykırı kararlara karşı özel bir tazminat yolu öngörülmemiş olmakla birlikte, hakkında tedbir uygulanan kişinin genel hükümlere göre tazminat hakkını kullanması durumunda kararda imzası bulunanların sorumlu olacakları şüphesizdir. Bu tedbirin en çok eleştirilen yönü olan denetim eksikliğinin kanun koyucu tarafından ikmal edilmesi halinde, örneğin ABD hukukunda olduğu gibi; ilgiliye, yasama organına, üst düzey yargı organlarına ve Adalet Bakanlığına denetim yetkisi verilmesi gündeme gelecektir. Bu konudaki kararların daha sağlıklı olmasının sağlanması bakımından, haksız tedbire hükmeden hakim kararı nedeniyle tazminat ödenmesi halinde, karar veren merciye rücu edilmesi gündeme gelebilecektir.

[1153] CENTEL/ZAFER, s. 364.

[1154] KUNTER/YENİSEY/NUHOĞLU, s. 706.

[1155] KUNTER/YENİSEY/NUHOĞLU, s.704; ÜNVER/HAKERİ, s.179;CENTEL/ZAFER, s. 364; ÖZTÜRK/ERDEM, s.603-604; ÇOLAK/TAŞKIN, s.630.

[1156] ŞEN, (İletişimin Denetlenmesi Tedbiri), s.113.

3.2.3.5.2. Cumhuriyet Savcısı Tarafından Verilen Kararın Hakimin Onayına Sunulması

Cumhuriyet savcısınca verilen iletişimin denetlenmesi kararı derhal hakim onayına sunulacak ve hakim yirmi dört saat içinde kararını verecektir. Hakim iletişimin denetlenmesi koşullarının bulunduğu kanaatine varırsa verilen kararı onaylayacaktır. Cumhuriyet savcısı tarafından tedbire karar verilmesi durumunda, hakim, yalnızca tedbirin hukuka uygunluğunu denetlemekle kalmaz. Bunun yanı sıra, tedbir için zorunlu olan şekle ve esasa ilişkin şartların yanında amaca uygunluk hususunu da dikkate alarak kararını verir. Hakim iletişimin denetlenmesi tedbirinin koşullarının oluşmadığına kanaat getirirse, kararı onaylamayacak ve söz konusu denetlemeye derhal son verecektir[1157.] Cumhuriyet savcısı sadece soruşturma aşamasında iletişimin denetlenmesine ilişkin karar verebilir. Cumhuriyet savcısının bu kararı verebilmesi için gerekli tek şart, gecikmesinde sakınca bulunan halin bulunmasıdır. Gecikmesinde sakınca bulunan hal, hakim tarafından verilecek kararı beklemenin telafisi mümkün olmayan zararlara sebebiyet verecek olması durumudur. Derhal işlem yapılmadığı takdirde suçun delil, iz, eser ve emarelerinin ortadan kaybolması ihtimalinin bulunduğu haller de bu çerçevede değerlendirilebilir[1158.] Bu doğrultuda, 10.11.2005 tarihli yönetmelikte gecikmesinde sakınca bulunan hal kavramı, derhal işlem yapılmadığı takdirde suçun iz, eser, emare ve delillerinin kaybolması veya şüphelinin kaçması veya kimliğinin saptanamaması olasılığının ortaya çıkması hali olarak tanımlanmıştır.

Anayasa'nın 22. maddesinde yetkili merci kararının 24 saatlik süre içinde yetkili hâkim onayına sunulması zorunluluğunun öngörülmesi karşısında, derhal ifadesinin 24 saatlik süreyi daha da kısaltmaya matuf olarak kanuna girdiğini kabul etmek gerekir[1159]. Derhal ifadesini, uygulayıcıları bir an önce karar vermeye zorlayan bir ifade olarak yorumlamak dışındaki bir yaklaşım kabul edilebilir değildir. 24 saate göre daha da kısıtlayıcı bir zaman diliminde karar verilmesini gerektiren 'derhal' ifadesinin, Cumhuriyet savcılarının mümkün olan en kısa süre içinde karar verilmesini sağlamak için maddeye eklendiği kuşkusuzdur. Gerçekten de, süre açısından getirilen sınırlamanın uygulamada işlevini yitirmemesi için, hem Cumhuriyet savcısının kararının hakime sunulması ve hem de bu kararın hakim tarafından onaylanması işleminin 24 saatlik süre içinde yapılması zorunluluğuna yer verilmesi daha yerinde olacaktır.

[1157] ERDEM , s. 100; ÖZTÜRK/ERDEM, s. 604.

[1158] ÖZBEK, s.427-428.

[1159] KEKLİK, s. 5.

CMK'nın 135. maddesinin birinci fıkrasında, Anayasa'nın 22. maddesinde yer alan sürelerin kısaltılmış olması neticesinde Cumhuriyet savcısının kararının hakim onayına sunulması için 24 saatlik bir süre dahi verilmemiş olmasının Anayasaya aykırı olduğu görüşü[1160] yukarıda da anlatıldığı üzere isabetli değildir.

3.2.3.5.3.Cumhuriyet Savcısı Tarafından Verilen Kararın Hakim Onayına Sunulmaması Veya Hakim Tarafından Onaylanmaması

İletişimin denetlenmesi için verilen kararın, hakim tarafından değerlendirilmesi için hakime verilen yirmi dört saatlik sürenin dolması veya Cumhuriyet savcısınca verilen kararın hakim tarafından reddedilmesi durumunda CMK'nın 135/1. maddesine göre Cumhuriyet savcısı tedbiri derhal sona erdirmelidir[1161]. Denetim kapsamında elde edilen kayıtların, CMK'nın 137/3. maddesi uyarınca, Cumhuriyet savcısının denetimi altında yok edilerek durumun bir tutanakla tespit edilmesi gerekmektedir. Cumhuriyet savcısı tarafından sonlandırılmasına gerek olmaksızın, tedbirin kendiliğinden sona ermiş sayılmasını gerekli gören kanaat bizce de isabetlidir[1162]. Böyle bir düzenlemenin kabul edilmesi, gereksiz bürokrasinin sonlandırılması anlamına da gelecektir.

3.2.4.Adli Amaçlı İletişimin Denetlenmesi Tedbirinin İstisnaları

Önleme amacıyla yapılan iletişimin denetlenmesi tedbirlerinde herhangi bir sınırlama bulunmamasına rağmen adli amaçlı iletişimin denetlenmesi tedbirinde tanıklıktan çekinme hakkı olan kişiler ve müdafi bakımından sınırlamalar getirilmiştir. Tanıklıktan çekinme hakkı olanlar ile müdafiilere ilişkin sınırlamaların kapsamı ve içeriği birbirinden farklı özellikler taşımaktadır.

3.2.4.1. Şüpheli veya Sanığın Tanıklıktan Çekinme Hakkı Olan Kişilerle Olan İletişiminin Kayda Alınamaması

Şüpheli veya sanığın, tanıklıktan çekinme hakkı olan üçüncü kişi ile kurdukları iletişim denetlenemez. Tanıklıktan çekinme hakkının belirlenememesi sebebiyle denetleme tedbiri uygulanmışsa, bu durumun ortaya çıkması halinde elde edilen bütün kayıtlar derhal yok edilecektir. Her ne kadar Kanun, bu kişiler arasındaki kayıtların kayda alınamayacağını belirtmişse de, tedbirin uygulaması aşamasında tanıklıktan

---

[1160] YİĞİT, s. 24.

[1161] KUNTER/YENİSEY /NUHOĞLU, s.704;TURHAN, s.269.

[1162] YİĞİT, s. 30.

çekinebilecek kişilerin tespitinin zor olacağı göz önüne alınarak, sonradan belirlenmesi halinde kayıtların imha edilmesine ilişkin düzenlemeye yer verilmiştir[1163]. Bu düzenleme hukukumuzun, AİHM içtihatlarına uygunluğunu sağlaması bakımından önemlidir. Gerçekten de, bu hususu düzenleyen hükümlerin yokluğu nedeniyle birçok ülke hakkında ihlal kararları verilmiş bulunmaktadır[1164].

Ceza yargılamasında tanıklıktan çekinebilecek kişilerin yer aldığı 5271 sayılı CMK'nın 45 ve 46. maddelerindeki düzenlemeler dikkate alındığında, şüpheli veya sanık ile akrabalık nedeniyle tanıklıktan çekinebilecek kişiler ile meslekleri nedeniyle tanıklıktan çekinme hakkı olanlar arasındaki iletişim kayıt altına alınamayacaktır[1165]. Ancak, suç işleme şüphesi altındaki tanıklıktan çekinme hakkı olan kişiler hakkında da hakim tarafından veya gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısı tarafından verilecek kararla CMK'nın 135. maddesindeki koşullar çerçevesinde bu kişilerin iletişimi kayıt altına alınabilecektir[1166].

İletişimin denetlenmesi tedbirinin uygulanması sırasında, görevlendirilen kişi, şüpheli veya sanığın tanıklıktan çekinme hakkı olan kişi ile yapmış olduğu konuşmaları kayda almayacaktır. Ancak , dinlemenin canlı değil de, otomatik olarak yapıldığı durumlarda, sonradan bu konuşmaların silinmesi kayıtların bütünlüğü açısından şüphe doğurabileceğinden ve yönlendirme olabileceği ihtimali de göz önüne alınarak, bu kayıtların delil bandı olarak saklanması ve kesintisiz kayıtta muhafaza edilmesi sağlanacaktır. Ancak bu bilgilerin, Cumhuriyet savcılığına verilen kayıt dökümlerinde yer almaması yerinde olacaktır[1167].

İletişimin denetlenmesi tedbirinin uygulanması sırasında getirilen sınırlamalarda, sanık müdafii bakımından, bütün telekomünikasyon araçları tedbir kapsamı dışındayken, tanıklıktan çekinebilecek kişiler bakımından yalnızca "kayda alma" yönünden bir sınırlama mevcuttur[1168]. Burada yalnızca "kayda alma " yönünden sınırlama getirilmesine karşın tespit, dinleme ve sinyal bilgilerinin değerlendirilmesi bakımından bir sınırlama getirilmeyerek ayrıma gidilmesinin sebebi, şüpheli veya sanığın iletişiminin

---

[1163]ÖZBEK,s.426; ÇOLAK/TAŞKIN, s.637;CENTEL/ZAFER, s.365; TURHAN, s.269 ÖZTÜRK/ERDEM,s. 605-606.

[1164] ÜNVER-HAKERI, s. 175.

[1165] KUNTER/YENİSEY/NUHOĞLU, s.700;ÜNVER/HAKERİ, s. 175.

[1166] ÇOLAK/TAŞKIN, s.638.

[1167] KUNTER/YENİSEY/NUHOĞLU, s.700.

[1168] KUNTER/YENİSEY/NUHOĞLU, s.700.

“tespit” edilmesi halinde, otomatik olarak bu kişilerle yapılan iletişimin de tespit edilecek olmasıdır. Ancak bu durum iletişimin dinlenmesi ve sinyal bilgilerinin değerlendirilmesi bakımından açıklayıcı değildir. Bu nedenle şüpheli veya sanığın tanıklıktan çekinme hakkı olan kişilerle yapmakta olduğu iletişimin dinlenmesi ve sinyal bilgilerinin değerlendirilmesi de sınırlama kapsamı içine alınması gerektiği şeklindeki düşünce bizce de isabetlidir[1169].

3.2.4.2. Hakkında İletişimin Denetlenmesi Kararı Verilemeyecek Kişiler

3.2.4.2.1. Akrabalık Nedeniyle Tanıklıktan çekinme hakkı olanlar

a) Şüpheli veya sanığın nişanlısı

b) Evlilik bağı kalmasa bile şüpheli veya sanığın eşi

c) Şüpheli veya sanığın kan hısımlığından veya kayın hısımlığından üstsoy veya altsoyu

d) Şüpheli veya sanığın üçüncü derece dahil kan veya ikinci derece dahil kayın hısımları

e) Şüpheli veya sanıkla aralarında evlâtlık bağı bulunanlar tanıklıktan çekinme hakkına sahiptirler.

3.2.4.2.2. Meslek ve Sürekli Uğraşıları Sebebiyle Tanıklıktan Çekinme Hakkı Olanlar

a) Avukatlar veya stajyerleri veya yardımcılarının, bu sıfatları dolayısıyla veya yüklendikleri yargı görevi sebebiyle öğrendikleri bilgiler,

b) Hekimler, diş hekimleri, eczacılar, ebeler ve bunların yardımcıları ve diğer bütün tıp meslek veya sanatları mensuplarının, bu sıfatları dolayısıyla hastaları ve bunların yakınları hakkında öğrendikleri bilgiler,

c) Malî işlerde görevlendirilmiş müşavirler ve noterlerin bu sıfatları dolayısıyla hizmet verdikleri kişiler hakkında öğrendikleri bilgiler,

Dolayısı ile tanıklıktan çekinme hakkına sahiptirler.

[1169] ÖZBEK, s. 426.

Özellikle meslek ve sürekli uğraşıları nedeniyle tanıklıktan çekinme hakkı olan kişilerin konuşmalarının kayda alınamamasında, tedbirin uygulandığı kişi ile tanıklıktan çekinme hakkı olan kişi arasındaki ilişkinin mesleki güvene dayanması temel sebeptir.

3.2.4.3.Müdafiinin İletişiminin Denetlenememesi

3.2.4.3.1.İstisnanın Kapsamı

Şüpheli veya sanık müdafiinin CMK'nın 154. maddesindeki yasal düzenlemeden kaynaklanan savunma dokunulmazlığı bulunduğu için şüpheli veya sanıkla yapmış olduğu iletişim denetim altına alınamaz[1170]. CMK'nın 136. maddesine göre, şüpheli veya sanığa yüklenen suç dolayısıyla müdafiin bürosu, konutu ve yerleşim yerindeki telekomünikasyon araçları hakkında iletişimin denetlenmesi tedbiri uygulanamaz. Diğer taraftan müdafii, şüpheli veya sanık konumunda ise iletişimin denetlenmesi tedbirine karar verilebilecektir. Bu nedenle mülga 4422 sayılı kanunda bulunmayan bu düzenlemeye CMK'da yer verilmiş olması yerinde bir uygulama olmuştur.[1171] CMK'nun 136. maddesi ile getirilen koruma, müdafilik sıfatının taşındığı sürece münhasırdır. Bilindiği gibi müdafii, şüpheli veya sanığın ceza muhakemesinde savunmasını yapan avukattır. Şüpheli ile avukat arasındaki ilişki müdafilik ilişkisi değilse, örneğin başka bir davada şüpheliyi temsil etmeye dayanan bir vekalet ilişkisi söz konusuysa, 136. maddedeki yasak söz konusu olmayacaktır[1172].

Şüpheli ve sanık müdafiinin CMK'nın 136. maddesi uyarınca denetim tedbiri kapsamında, iletişiminin tespiti, dinlenmesi ve kayda alınması ile sinyal bilgilerinin değerlendirilmesi mümkün değildir[1173].

[1170] KUNTER/YENİSEY/NUHOĞLU, s.700;TURHAN, s.269.

[1171] ÖZBEK, s. 426 ÜNVER / HAKERİ, s. 199.

[1172] TAŞKIN, s.154.

[1173] Fransız hukukunda da avukatların iletişimlerinin denetlenmesi konusunda bir sınırlama yer almaktadır. Fransız CMK'nun 100-7. maddesine göre baro başkanı, iletişimin denetlenmesi tedbiri hakkında soruşturma hakimi tarafından bilgilendirilmedikçe avukatın evi ya da bürosunun bağlı olduğu hat üzerinde bu tedbir gerçekleştirilmesi mümkün değildir"(Aucune interception ne peut avoir lieu sur une ligne dépendant du cabinet d'un avocat ou de son domicile sans que le bâtonnier en soit informé par le juge d'instruction. http://www.lexinter.net/PROCPEN/interception de correspondances.htm İET:23.12.2007). Görüldüğü gibi Fransa'da mutlak bir yasak değil, sadece baro başkanının bilgilendirilmesi zorunluluğu getirilmiştir. Fransız Ceza Usul Kanunu'nun 100-5 maddesine 2005-1549 sayılı Kanunla 12 Aralık 2005 tarihinde 3. fıkra eklenmiştir. Bu hükme, bir avukatın müvekkili ile onun savunma hakkını ilgilendiren konularda yaptığı görüşmelerin kaydedilemeyeceği, kaydedilmişse de geçersiz olduğu belirtilmiştir. (A peine de nullité, ne peuvent être transcrites les correspondances avec un avocat relevant de l'exercice des droits de la défense. http://www.lexinter.net/ PROCPEN/ interception de correspondances.htm İET:23.12.2007). Meslek sırrını muhafaza etmekle yükümlü kişiler arasında gerçekleştirilen konuşmaların, örneğin bir avukatla bir tercümanın kendi aralarında yapmış oldukları görüşmelerin denetlenmesi hususunda daha gevşek bir tavır takınılmaktadır. (CHARRIER, 511)Bk.

3.2.4.3.2.Müdafii Bakımından Getirilen İstisnaya Konu İletişim Araçları

Meslek sırrı ve savunma hakkını garanti altına almak için getirilen CMK'nın 136. maddesinde müdafiinin, bürosu, konutu ve yerleşim yerindeki telekomünikasyon araçlarının denetlenemeyeceği belirtilmiştir. Bu düzenlemeden müdafiin mobil telefonu ile yapacağı iletişimin denetlenemeyeceği gibi bir sonuç çıksa da, düzenlemenin getiriliş amacından söz konusu yasağın müdafiin mobil telefonu da dahil olmak üzere her türlü iletişim aracını kapsadığı kabul edilmelidir. Söz konusu denetim yasağının şüpheli veya sanığa yüklenen suç dolayısıyla getirilmiş olması göz önüne alındığında bu hususun meslek sırrı ve savunma hakkını koruma altına almağa yönelik olduğu açıktır[1174]. Ayrıca CMK'nın 136. maddesinin gerekçesinde bu husus "….avukatın savunmasını üstlendiği şüpheli veya sanık ile haberleşmesi denetlenemez." denilmek suretiyle müdafii ile şüpheli veya sanık arasındaki iletişimin denetlenemeyeceği vurgulanmıştır. Bununla birlikte CMK'nın 135/2. maddesi uyarınca CMK'nın 46. maddesinde sayılan tanıklıktan çekinebilecek kişiler arasında müdafii de bulunduğundan kanundaki bu boşluğun bu hüküm ile de karşılanması mümkündür[1175].

Öğretide, mevcut düzenleme ile getirilen sınırlamaların belirli yerdeki telekomünikasyon araçları açısından olduğu belirtilerek, aracın türü açısından bir sınırlama bulunmadığından, müdafiin konutu, işyeri ve bürosunda olmak şartıyla, mobil telekomünikasyon araçları ile olan iletişiminin denetlenebileceği, bu sebeple mevcut düzenlemenin değiştirilmesi gerektiği dile getirilmektedir[1176]. Kanaatimizce, 136. maddede yer alan düzenlemede kastedilen, her türlü iletişim vasıtasıdır. Bu madde, müdafii ile müvekkili arasındaki ilişkiyi takipten bağışık kılmak amacıyla çıkarıldığından, mobil telefonun bu kapsamdan çıkarılması doğru olmayacaktır. Kanun koyucunun amacının bu kişilere mesleklerinin özelliğinden kaynaklanan bir koruma sağlamak olduğu kabul edildiğinde, bu korumadan mobil telefonu çıkarmak hayatın gerçekleriyle uyuşmayacaktır. Nitekim, günümüz dünyasında müdafii sıfatını da ihraz edebilecek

---

ayrıca Ünal, Avrupa İnsan Hakları Sözleşmesi, s. 221. Almanya'da, avukatların iletişimlerinin denetlenmesi konusunda kanundan kaynaklanan bir sınırlama bulunmamaktadır. Bununla birlikte, Alman Ceza yargılamasında avukatın iletişiminin dinlenebileceğine ilişkin Alman Anayasa Mahkemesinin 1971 yılında verdiği bir karar ile kabul edilmiş ve Anayasa'ya aykırı olmadığı belirtilmiştir. Daha sonra bu görüş yerini dinlemeyi yapan görevlinin telefon görüşmesinin müdafii ile yapıldığını fark ettiği anda dinlemeyi sona erdirmesi gerekeceği görüşüne bırakmıştır. Öte yandan, avukatın kendisi şüpheli konumunda ise, hakkında dinleme tedbiri uygulanması mümkündür (KUNTER/YENİSEY/NUHOĞLU, s. 699; ÇOKSEZEN, s. 11.)

[1174] ÖZBEK, s. 427; TURHAN, s. 269-270.

[1175] ŞAHİN, s.382; ÜNVER/HAKERİ, s.201; ÖZTÜRK/ERDEM, s. 608.

[1176] ÜNVER/HAKERİ, s.201.

durumda olan avukatlar, konuşmalarının çok önemli bir bölümünü mobil telefonları vasıtasıyla yapmaktadırlar.

3.2.5.Adli Amaçlı İletişimin Denetlenmesi Kararının İçeriği ve Unsurları

5271 sayılı CMK, iletişimin denetlenmesi kararında hangi unsurların bulunması gerektiğini 135/3. maddesinde ayrıntılı olarak belirtmiştir. Bu unsurlar şunlardır:

3.2.5.1.İletişimi Denetlenecek Kişinin Kişisel Bilgilerinin Belirtilmesi

İletişimin denetlenmesi tedbiri kararı yazılı olarak verilmelidir. Kararda, kendisine suç isnat edilen sanığın veya şüphelinin adı ve adresi, hakkında tedbir uygulanacak kişinin kimliği, iletişim aracının türü, telefon numarası veya iletişim bağlantısını tespite imkân veren kodunun belirtilmesi, tedbire başvurma nedenine ilişkin yeterli bilgi verilmesi, tedbirin türü, kapsamı ve süresinin de somut olarak belirlenmesi ve olabildiğince sınırlandırılması zorunluluğu aranmaktadır. Bu doğrultuda, CMK m. 135/3. maddesinde "kararda, yüklenen suçun türü, hakkında tedbir uygulanacak kişinin kimliği, iletişim aracının türü, telefon numarası veya iletişim bağlantısını tespite olanak veren kodu, tedbirin türü, kapsamı ve süresi belirtilir" denilmek suretiyle bu husus özellikle belirtilmiştir[1177]. İletişimi denetim altına alınacak şüpheli ya da sanık başkasına ait iletişim araçlarını kullanıyorsa, bu üçüncü kişinin de açık kimlik bilgilerinin kararda belirtilmesi gerekir. Kararın bu şekilde ayrıntılı olması halinde denetim konusu suçla ilgisi olmayan kimselerin iletişiminin denetlenmesinin önüne geçilecektir[1178].

İletişimin denetlenmesi tedbiri kararında, yukarıda belirtilen unsurların hepsinin birlikte bulunması gerekmektedir. Ancak, her zaman bu kadar ayrıntılı bilginin temin edilmesi mümkün olmamaktadır. Tedbirin uygulanması sırasında, yeni bir şüphelinin daha ortaya çıkması durumunda, bu kişinin kimliği hakkında ilk aşamada kesin bilgilere ulaşılması mümkün olmayabilir. Bu sebeple, eldeki mevcut bilgilerle bu kararın verilebilmesi gerektiği [1179]düşüncesi bizce de isabetlidir.

3.2.5.2.Tedbirin Türü, Kapsamı ve Süresinin Belirtilmesi

14/2/2007 tarihli ve 26434 sayılı Resmi Gazetede yayımlanan 'Ceza Muhakemesi Kanununda Öngörülen Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi, Gizli

---

[1177]Bk.ÖZTÜRK/ERDEM, s. 606; TURHAN, s.269; ÜNVER/HAKERİ, s.178;CENTEL/ZAFER, s. 364; KUNTER/YENİSEY/NUHOĞLU, s.711; ÖZBEK, s. 428; ÇOLAK/ TAŞKIN, s. 631.

[1178] ÜNVER/HAKERİ, s.169.

[1179] KUNTER/YENİSEY/NUHOĞLU, s.711.

Soruşturmacı ve Teknik Araçlarla İzleme Tedbirlerinin Uygulanmasına İlişkin Yönetmelik' te, iletişimin denetlenmesi tedbirinin kapsamı anlatılmıştır. Bu bağlamda tedbir kapsamında şu sonuçlara varmak mümkündür:

1. Tedbire, şüpheli veya sanık bakımından karar verilir. Bu husus Yargıtay tarafından da teyit edilmiştir. Gerçekten de Yargıtay 4. Ceza Dairesinin 6.11.2007 tarihli kararında, CMK'nın 135/1. maddesinde yer alan düzenlemeye atıf yapılarak, yalnızca şüpheli veya sanığın iletişiminin tespiti, kayda alınması, dinlenilmesi ve sanal bilgilerin değerlendirilmesinin mümkün olduğu vurgulanmıştır. Kararda; '… somut olayda hakkında soruşturma izni verilen Cumhuriyet Savcısının suç şüphesi altında bulunduğuna ilişkin bir bulgu ya da belgeye rastlanmadığı gibi, aksine soruşturma fezlekesinde "cezai yönden soruşturma açılmasını gerektiren somut bir delilin mevcut olmadığı, ancak eşi ile geçimsizliğini meslektaşlarına deşifre ederek, eşinin de aynı şekilde davranıp, bir bayan avukatın adını bazı hakim ve savcılarla paylaşması neticesinde sübjektif değerlendirmelere neden olacak şekilde davranmaları ve adı geçen Cumhuriyet Savcısının çevresindeki insanlarla olan ilişkilerindeki ölçüyü mesleğinin gerektirdiği şekilde ayarlayamamasının ise disiplin Yönünden kovuşturmayı gerektirdiği" belirtilmektedir. Yasanın buyurucu hükmüne göre suç şüphesi altında bulunmayan, yani şüpheli ve sanık sıfatı taşımayan bir kişi hakkında iletişimin tesbiti karan verilmesi olanaklı değildir' ifadesi yer almaktadır[1180].

2. Tedbirin, hakkında tedbir uygulanacak kişinin üzerine kayıtlı veya kullanmakta olduğu iletişim araçlarının tümü hakkında uygulanabilir. Hakkında karar verilen kişi ile iletişim araç sahibinin farklı kişiler olması hâlinde bu durum talep ve kararda açıkça belirtilir.

3. İletişimin tespiti, dinlenmesi, kayda alınması ve sinyal bilgilerinin değerlendirilmesi kararı kişilerin yurt dışı bağlantılı iletişimini de kapsar.

4. Dinleme ve kayda alma kararının yerine getirilmesi sırasında şüphelinin başka bir iletişim aracını kullandığı belirlendiğinde, buna ilişkin verilecek karar ya da kararların süresi önceki tedbir kararında verilen sürenin bitiş tarihini geçemez.

İletişimin denetlenmesi tedbiri, işlendiği zannedilen suç fiili ile ilgili delil elde etmek veya şüpheli veya sanığın yerini tespit amacıyla uygulanmaktadır[1181]. Şüpheli veya sanık dışındaki

[1180] 4. CD., 2007/8700 E., 2007/8903 K., 6.11.2007

[1181] KUNTER/YENİSEY/NUHOĞLU, s. 711.

kişiler hakkında böyle bir karar verilmesi mümkün olmamakla birlikte, denetime konu iletişim aracının şüpheli veya sanık adına kayıtlı olması gerekli değildir. Başka bir ifadeyle, bu kişilerin fiilen kullandığı tüm iletişim araçlarının denetleme konusu yapılması sözkonusudur. İletişimin denetlenmesi tedbirinin sadece şüpheli veya sanık bakımından uygulanabilmesi kuralının istisnası mobil telefonun yerinin tespitidir. Bu denetleme türünde, izlemeye alınan aracın şüpheli veya sanığa ait olması zorunlu değildir[1182].

İletişimin denetlenmesi kararı verilirken iletişimin bu amaçlardan hangisi için verildiğinin belirtilmesi zorunludur. Bu amaçla verilen kararda; tespit, dinleme, kayda alma, sinyal bilgilerinin değerlendirilmesi ve mobil telefonun yerinin tespiti işlemlerinden hangisinin yapılacağı ve hangi amaçla yapılacağının belirtilmesi gerekir. Bu bağlamda, iletişim denetlenmesi tedbirlerinden birkaçına birlikte de karar verilebilir[1183].

Mülga 4422 sayılı kanuna göre, iletişimin denetlenmesi kararında, tedbirin amacının tespit, dinleme veya kayda alma mı olduğu yoksa hepsinin birlikte mi amaçlandığı hususunun kararda belirtilmesi gerekiyordu. Aynı şekilde kararda şüphelinin kimlik bilgileri ve adresi, iletişim aracına ait tür, numara ve frekans gibi bilgiler, tedbirin hangi suç için istendiği, kuvvetli belirtilerin neler olduğu, dinleme ve tespitin süresi, iletişim aracına ait ve iletişim içeriği dışında kalan kayıtların ve iletişim aracının yerinin tespiti ile başka bir tedbir ile failin belirlenmesi, ele geçirilmesi veya suç delillerinin elde edilmesinin mümkün olmadığına ilişkin açıklamanın da yer alması zorunluydu[1184].

3.2.5.3. Tedbire Konu Kişiye Yüklenen Suçun Türünün Belirtilmesi

Yasal düzenlemeye göre, iletişimi tespit altına alınacak kişinin, katalog suçlardan hangisi ile itham edildiğinin de belirtilmesi zorunludur. Bu kapsamda CMK 135/3. maddesinde belirtilmiş olan ”yüklenen suç”, şüpheli veya sanığın işlediğinden kuşkulanılan fiiller olarak anlaşılmalıdır.

Kanunun ilgili maddesinde belirtilen hususların dışında, şüpheli veya sanığa yüklenen fiilin CMK’nın 135/6. maddesinde sayılan suç tanımlarından birisine uyduğunu ve suçun aydınlatılmasının başka türlü mümkün olmadığını gösteren olgular da açıklanmalıdır. Diğer taraftan, şüpheli veya sanığın söz konusu fiili işlediği veya buna iştirak ettiğine dayanak oluşturan şüphe nedenleri ile tedbire savcı tarafından karar verilmesi durumunda gecikmede

---

[1182] ŞAHİN, Ceza Muhakemesi Hukuku, s.271

[1183] KUNTER/YENİSEY/NUHOĞLU, s. 711.

[1184] ÖZBEK, s. 424; KUNTER/YENİSEY/NUHOĞLU, s. 711.

sakınca bulunduğunu gösteren olgular, tedbire başlama ve sona erme tarihi ve saatinin mutlaka kararda gösterilmesi gerekir[1185].

3.2.6.Adli Amaçlı İletişimin Denetlenmesinde Süre

Türk hukukunda İletişimin denetlenmesi tedbirinin, CMK m. 135/3. maddesi uyarınca en çok üç ay için verilebileceği ve bu sürenin ancak bir defa uzatılabileceğini öngörülmüştür. Buna göre iletişimin denetlenmesi tedbirinde uzatma ile birlikte kararın süresi 6 ayı geçemeyecektir[1186]. Ancak örgütün faaliyeti çerçevesinde işlenen suçlarla ilgili olarak gerekli görülmesi halinde, hakim bir aydan fazla olmamak üzere sürenin müteaddit defalar uzatılmasına karar verebilir[1187]. Öte yandan başvurulan tedbir mobil telefonun yerinin tespitine ilişkin ise tespit kararı en çok üç ay için verilebilecek ve ancak bir defa uzatılabilecektir. Dolayısıyla örgüt faaliyeti çerçevesinde işlenen bir suç da söz konusu olsa, şüpheli veya sanığın yakalanması amacıyla en fazla altı ay süreyle tespit kararı verilebilecektir (CMK md. 135/4)[1188].

Ceza Muhakemesi Kanununda Öngörülen Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi, Gizli Soruşturmacı ve Teknik Araçlarla İzleme Tedbirlerinin Uygulanmasına İlişkin Yönetmeliğin 7. maddesi uyarınca, dinleme ve kayda alma kararının yerine getirilmesi sırasında şüphelinin başka bir iletişim aracını kullandığı belirlendiğinde buna ilişkin verilecek karar ya da kararların süresi önceki tedbir kararında verilen sürenin bitiş tarihini geçemeyecektir.

3.2.6.1.Sürenin Başlama Anı

CMK'da iletişimin denetlenmesine ilişkin sürenin ne zaman başlayacağına ilişkin herhangi bir hükme yer verilmemiştir. Öğretide, iletişimin denetlenmesi tedbirinde sürenin kararın verildiği andan itibaren işlemeye başlayacağını ileri süren görüşler bulunmaktadır[1189]. Sürenin başlamasına ilişkin bir diğer hüküm, 14/01/2007 tarihli Ceza Muhakemesi Kanununda Öngörülen Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi, Gizli Soruşturmacı Ve Teknik Araçlarla İzleme Tedbirlerinin Uygulanmasına İlişkin

---

[1185] ÖZTÜRK/ERDEM, s. 606; TURHAN, s.269; ÜNVER/HAKERİ, s.178;CENTEL/ZAFER, s. 364; KUNTER/YENİSEY/NUHOĞLU, s.700; ÖZBEK, s. 428.

[1186] CENTEL/ZAFER, s. 365;ERDEM, s.104; ÇOLAK /TAŞKIN, s.632.

[1187] KUNTER/YENİSEY/ NUHOĞLU, s.714;ÖZBEK, s. 429;TURHAN, s. 270.

[1188] ÖZBEK, s. 429-430; ÖZTÜRK/ ERDEM, s.606.

[1189] ERDEM, s.104; TURHAN, s. 270.

Yönetmeliğin 12/4. maddesinde yer almaktadır. Bu maddeye göre, süre, kararın başkanlıkta sisteme tanıtıldığı andan itibaren başlayacaktır[1190].

Bununla birlikte, bu düzenleme ile, aynı Yönetmeliğin 5. maddesinin 3. fıkrasında yer alan "Talep veya karar, hâkim veya Başkanlığa ulaştığı anda süreler başlar" hükmü arasında çelişki bulunmaktadır. Birisinde sürenin başlaması kararın TİB'e ulaştığı an olarak belirlenirken, diğerinde kararın sisteme tanıtıldığı an olarak belirtilmiştir.

Sürenin kararın verildiği andan itibaren işlemeye başlaması bazı sakıncalar doğurmuş, kararın sisteme kaydedildiği andan itibaren başlaması uygulaması da Danıştay 10. Dairesi 16.10.2007 tarihinde verdiği kararla, 14.01.2007 tarihli Yönetmeliğin 12. maddesinin 4. fıkrası hükmünün yürütmesinin durdurulmasına karar vermesiyle imkansız hale gelmiştir. Öğretide savunulan üçüncü görüş bizce de isabetlidir. Bu görüşe göre, kararın verildiği an ile kararın TİB tarafından kaydedildiği an arasında yer alan, kararın TİB'e ulaştığı anda, süre işlemeye başlayacaktır[1191].

3.2.6.2.Sürenin Uzatılması

Uygulanan denetim tedbiri kapsamında, koşulların bulunması halinde talep üzerine verilen süre bir defa daha uzatılabilir. Ayrıca bir örgütün faaliyeti çerçevesinde işlenen suçlarla ilgili olarak gerekli görülmesi halinde, hakim bir aydan fazla olmamak üzere sürenin müteaddit defalar uzatılmasına karar verebilir[1192]. Sürenin uzatılması suretiyle denetime devam edilmesinde, bu hususun kötüye kullanılmayacağının tek güvencesi, uzatmanın hakim kararına dayanmasıdır[1193].

İletişimin denetlenmesi tedbirinde sürenin uzatılmasına ilişkin talep ve kararlarda denetleme kararında olması gereken diğer unsurların yanı sıra ilk karara ilişkin bilgiler ile uzatmanın gerekçesi belirtilmelidir. Uzatma kararı verilebilmesi için, başlangıçta tedbir için gerekli şartların mevcut olması ve bu durumun uzatma kararında açıkça gösterilmesi

---

[1190] ÇOLAK /TAŞKIN, s.633; Sürenin başlamasına ilişkin bir diğer görüşe göre, süre kararın verildiği andan itibaren başlar.Sürenin, kararın uygulanmasına başlandığı andan itibaren işlemeye başlayacağının kabul edilmesi halinde, tedbiri uygulama durumunda olan kolluğun, tedbirin süresini istediği andan itibaren başlatabilmesine ve böylece tedbirin uygulamada kötüye kullanılmasına imkan tanınmış olur.(YİĞİT, s. 29; ÖZTÜRK/ERDEM, s. 607; ÖZBEK, s. 429) .

[1191] TAŞKIN, s. 122-123.

[1192] İletişimin denetlenmesi tedbirinde CMK'nın 135/3. maddesine 5353 sayılı Kanunla eklenen hüküm uyarınca, örgütlü suçlar bakımından tedbirin uygulanma süresine bir istisna getirilmiştir. Buna göre, "örgütün faaliyeti çerçevesinde işlenen suçlarla ilgili olarak gerekli görülmesi halinde, hâkim bir aydan fazla olmamak üzere sürenin müteaddit defalar uzatılmasına karar verebilir".

[1193] KUNTER/YENİSEY/NUHOĞLU, s.714;ÇOLAK /TAŞKIN, s.633; KUNTER/YENİSEY/NUHOĞLU, s. 705.

gerekir. Aksi durumda süre açısından getirilen sınırlamanın gereksiz ve keyfi biçimde göz ardı edilmesine açık kapı bırakılmış olur. Hakim tarafından uzatma kararı verilebilmesi için, ilk denetim kararında hedeflenen amacın henüz gerçekleşmemiş bulunması fakat ulaşmanın mümkün olması gerekir[1194]. İletişimin denetlenmesi tedbirinde sürenin uzatılmasına her halükarda hakim karar verecektir. Bu sebeple Cumhuriyet savcısı gecikmesinde sakınca bulunan hali gerekçe göstererek süreyi uzatamaz[1195].

Yapılan soruşturma çerçevesinde birden fazla kişinin iştirak hükümleri çerçevesinde suç işlemeleri halinde, daha uzun süreyle denetleme kararı alabilmek amacıyla eylem örgütlü suç olarak adlandırılmak suretiyle bir takım deliller elde edilebilirse de, yapılan yargılama neticesinde eylemin örgütlü suç olmadığı anlaşıldığında, elde edilen bu deliller değerlendirme yasakları ile karşı karşıya kalabilir. Böyle bir durumda normal bir yolla bile elde edilebilecek deliller dahi hukuka aykırı şekilde tüketilmiş olacak ve yeniden elde edilmeleri mümkün olmayacaktır[1196].

3.2.6.3.Sürenin Sona Ermesi

İletişimin denetlenmesi tedbirine ancak belirli bir süreyle karar verilebileceğine göre, bu sürenin sona ermesi halinde tedbire ilişkin karar bitiş tarihi itibariyle hükümsüz kalacaktır. Bu durumda tedbirin uygulanmasına derhal son verilecektir. Sürenin bittiği tarihten sonra denetleme devam etse de elde edilen bilgilerin delil olarak değerlendirilmesi mümkün değildir. Bu sebeple, iletişimin denetlenmesi kararında öngörülen süre dolduğu anda ve sürenin uzatılmasına ilişkin bir kararın da bulunmaması halinde, tedbire, her hangi bir karara ihtiyaç duyulmadan ilgili kurumca kendiliğinden son verilmelidir[1197].

[1194] ÇOLAK /TAŞKIN, s.633; KUNTER/YENİSEY/NUHOĞLU, s.714; ERDEM/ÖZTÜRK, s. 607; KEKLİK, s. 7.

[1195] KUNTER/YENİSEY/ NUHOĞLU, s.714.

[1196] ÇOLAK /TAŞKIN, s.633; Almanya'da iletişimin denetlenmesine ilişkin karar ancak üç ay süreli olarak verilebilmektedir. Bununla birlikte, tedbirin uygulanmasına ilişkin koşullar devam ettiği sürece, her defasında 3 ayı geçmemek üzere bu süre uzatılabilir ve hatta birden fazla uzatma da mümkündür. Mülga 4422 sayılı kanunun 2/6.maddesine söz konusu tedbirin uygulanmasını üç aylık süre ile sınırlandırmış, bu sürenin her defasında üçer aydan fazla olmamak üzere uzatılması olanağına da yer vermişti. Kanunda sürenin en çok iki defa uzatılabileceği belirtilmiş olduğu için, tedbirin azami süresi dokuz ayı geçemiyordu(KUNTER/YENİSEY/ NUHOĞLU, s.714;ERDEM, s. 103;ÜNVER/ HAKERİ, s.178).

[1197] ÖZTÜRK/ERDEM, s.609.

3.2.7.Adli Amaçlı İletişimin Denetlenmesi Tedbirinin Gizliliği

3.2.7.1.Gizliliğin Korunması

İletişimin denetlenmesine ilişkin işlem ve kararların, hem haberleşme özgürlüğü ve özel hayatın korunması hem de soruşturmanın gizliliği ilkesi gereğince, tedbir süresince gizli tutulacağı CMK'nın 135/5. maddesinde hükme bağlanmıştır. CMK'nın 135/5. maddesine göre hem verilen karar hem de yapılan işlemlerin gizli tutulacağı belirtildiğinden, verilen kararın talep ve karar aşaması gizli olarak verileceği gibi tedbirin uygulanması sırasında da bu gizlilik devam edecektir[1198]. Özellikle Cumhuriyet savcısı tarafından tedbir için görevlendirilen kolluk görevlisi ve soruşturmayı yürüten kolluk yetkilisi dışında kimsenin bilgilendirilmemesi gerekir. Aynı şekilde elde edilen kayıtlar ile alakalı da Cumhuriyet savcısı ve hakim dışında hiç kimsenin bilgilendirilmemesi gerekir. Bunlar dışındaki kişilere kayıt ve işlemlere ilişkin bilgi verilmesi gizliliğin ihlali olacaktır.

Gizlilik hükmü, 14.01.2007 tarihli Yönetmelik'te de yer almıştır. Anılan Yönetmeliğin 5. maddesinin 4. fıkrasında, "Bu maddedeki tüm işlemler sırasında gizliliğe uyulur" şeklindeki hükmün yanı sıra aynı Yönetmeliğin 9. maddesinde "iletişimin dinlenmesi, iletişimin kayda alınması suretiyle yapılır ve gizlilik kurallarına tam uyularak gerçekleştirilir" ifadesi yer almaktadır.

Gizlilik hususunda gerek CMK 135 gerekse ilgili Yönetmelikte hüküm bulunması, AİHM'nin gizlilik konusunda devletlere yüklediği sorumluluk bakımından önemlidir. Nitekim, Craxi-İtalya kararında, Mahkeme, özel hayata giren konuların Sözleşmenin 8. maddesini ihlal edecek şekilde kamuya açılmasının, bunun yanında özel hayatın gizliliği kapsamında bilgiler içeren çözümlemelerin, devletin kaydı altına girdikten sonra güvenli bir şekilde muhafaza edilememiş olmasının 8. maddenin ihlali anlamına geleceğini belirtmiştir.

Mahkemeye göre, devletin sorumluluğu bilgilerin basına sızmasının engellenmesini de kapsamaktadır[1199]. Buna karşılık Ülkemizde ana haber bültenlerinde yayımlanan dinleme kayıtlarında, özel hayata ilişkin olan bilgiler, tanıklıktan çekinme hakkına sahip olanlar arasında geçenler de dahil olmak üzere, hiçbir sınırlamaya tabi olmaksızın açıklanabilmektedir. Oysa ki, iletişimin denetlenmesi tedbiri, yargısal mercilerin ulaşabileceği bilgilerin elde edilmesine matuftur. Bu bilgilerin kamuoyuna açıklanması halinde masumiyet karinesine aykırı davranılmış olacaktır. Mahkeme kararı ile henüz mahkum edilmemiş kişilerin, toplum nezdinde

---

[1198] ÜNVER/HAKERİ, s. 217.

[1199] Bk. CRAXİ-İTALYA, 14.10.1996 tarihli AİHM karar.

mahkum edilmesi ve suçlu olarak sunulmasının önlenmesi amacıyla CMK 157. maddede, soruşturma aşamasındaki tüm işlemlerin gizli olduğu hükme bağlanmış ve bu madde hükme aykırı davranışların TCK'nın 285. maddesine göre cezalandırılacakları belirtilmiştir[1200]. Bu tür tutum ve davranışların cezalandırılması konusunda gerekli adımların atılması, bu tür yayınlar hakkında gerekli soruşturmanın başlatılması caydırıcılık bakımından önemlidir. Bu tür kayıtların kamuoyuna açıklanması suretiyle, isimleri kirletilen insanların uğradıkları zararın büyüklüğü, devletlerin ödeyeceği tazminatların da büyüklüğü anlamına gelecektir. Nitekim, devletlerin omuzlarına yüklenen pozitif sorumluluğun, bu tür eylemlerin önlenmesini de kapsadığı muhakkaktır.

3.2.7.2.Gizliliğin Sağlanması İçin Yapılacak İşlemler

Tedbirin gizliliğine ilişkin olarak Kanundaki düzenlemelere paralel olarak 14 .01.2007 tarihli "Ceza Muhakemesi Kanununda Öngörülen Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi, Gizli Soruşturmacı Ve Teknik Araçlarla İzleme Tedbirlerinin Uygulanmasına İlişkin Yönetmelik"te bazı somut hükümlere yer verilmiştir. Buna göre, Cumhuriyet Başsavcılığı tarafından gönderilen talep yazısı, hâkim tarafından saat belirtilerek havale edilecek ve talep, istemin içeriği gösterilmeksizin, hâkim havalesinde belirtilen saat de işlenmek suretiyle, bu iş için görevlendirilen ilgili zabıt katibi tarafından, mahkemenin değişik iş defterine kaydedilecektir. Tedbir talebi, hangi mahkemenin değişik iş defterine kaydedilmişse, o mahkemenin hâkimi tarafından sonuçlandırılacaktır. Alınan karar, tutanakla Cumhuriyet Başsavcılığına teslim edilecek ve mahkeme kaleminde kalan suretinin gizli tutulması için ilgili hâkim tarafından gerekli tedbirler alınacaktır. Öte yandan, söz konusu kararların gizliliğinin bir gereği olarak tedbir süresince değişik iş kartonuna takılmayacak, ancak tedbirin sona erdiği zaman ilgili kartona ilave edilecektir. Gizliliğin sağlanması için atılan bir diğer adım da, bu işlerde görevlendirilecek katiplerin, ağır ceza merkezindeki komisyon tarafından, diğer yerlerde ise ceza hakimleri ile Cumhuriyet başsavcısı veya kıdemli Cumhuriyet savcısı ile birlikte belirlenmesidir[1201].

3.2.8.Adli Amaçlı İletişimin Denetlenmesi Tedbirinin Yerine Getirilmesi

3.2.8.1. Kararı Yerine Getirecek Kişi ve Kurumlar

3.2.8.1.1. Cumhuriyet Savcısı ve Görevli Adli Kolluk Yetkilisi

---

[1200] TAŞKIN, s. 133.

[1201] ÇOLAK /TAŞKIN, s. 636.

İletişimin denetlenmesi tedbirine ilişkin kararın yerine getirilmesi CMK'nın 137. maddesinde hüküm altına alınmıştır. Diğer koruma tedbirlerinde olduğu gibi, telekomünikasyon yoluyla yapılan iletişimin denetlenmesi tedbiri de, savcılık ve onun yardımcı organı olan kolluk tarafından yerine getirilmektedir. Bununla birlikte bu tedbirin yerine getirilmesi için aynı zamanda haberleşme hizmeti sunan kurumlar için de bazı yükümlülükler getirilebilmektedir. Nitekim CMK'nın 137/1. maddesi uyarınca "Cumhuriyet Savcısı veya görevlendireceği adlî kolluk görevlisi, telekomünikasyon hizmeti veren kurum ve kuruluşların yetkililerinden iletişimin tespiti, dinlenmesi veya kayda alınması işlemlerinin yapılmasını ve bu amaçla cihazların yerleştirilmesini yazılı olarak istediğinde, bu istem derhâl yerine getirilir" denilmektedir[1202]. 4422 sayılı Kanunda bu kuruluşların kovuşturma organları ile işbirliğine gitmemesi durumunda, bu kuruluşları işbirliğine zorlamaya yönelik herhangi bir düzenlemeye yer verilmemiş iken, CMK'nın 137/1. istemin yerine getirilmemesi durumunda zor kullanılabileceğini açıkça öngörmüş bulunmaktadır.

Öğretide, iletişimin denetlenmesi çerçevesinde elde edilecek kayıt ve işlemlerin çözümünde görevlendirilecek kişilerle ilgili olarak, CMK'nın 137/2. maddesinde yer alan "Cumhuriyet savcılığınca görevlendirilen kişiler" tabirininin kullanılması suretiyle, kanun koyucunun kolluğun görevlendirilmesinden kaçındığı ve burada tedbir çerçevesinde tutulan kayıtların kolluk dışında kişiler tarafından metin haline getirilmesinin amaçlandığını dile getiren görüşler mevcuttur. Burada tarafsızlığın sağlanması amacıyla bunun yapıldığı ancak kolluğa bu denli güvensizliğin yerindeliğinin de tartışılması gerektiği dile getirilmektedir[1203]. Ancak, 14.01.2007 tarihli "Ceza Muhakemesi Kanununda Öngörülen Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi, Gizli Soruşturmacı Ve Teknik Araçlarla İzleme Tedbirlerinin Uygulanmasına İlişkin Yönetmeliğin 9. maddesinde "İşlem görevlileri" başlığı altında getirilen düzenleme uyarınca, Cumhuriyet savcısınca belirlenen kolluk birimince; iletişimin dinlenmesi, kayda alınması, sinyal bilgilerinin değerlendirilmesi ve tespitiyle ilgili işlemlerin yerine getirilmesi amacıyla yeterli sayıda personel görevlendirileceği ve bu Yönetmelik kapsamında yapılan işlemlerin ve yapıldığı yerlerin gizliliği, düzeni ve güvenliği ile kolluk görevlilerinin aidiyet numaralarının belirlenmesine ve muhafazasına ilişkin esas ve usuller ilgili kolluğun merkez birimlerince

[1202] ERDEM,s.103.

[1203] ÖZBEK, s.430; Alman hukukunda iletişimin denetlenmesi tedbirini yerine getirme görevi, savcı yardımcısı statüsündeki memurlara tevdi edilmiştir.(KUNTER/YENİSEY/NUHOĞLU, s. 713).

düzenleneceği belirtilmek suretiyle kolluğun görevlendirileceği anlaşılmaktadır. Bu sebeple Kanundaki bu konudaki belirsizlik Yönetmelikle giderilmiştir.

İletişimin denetlenmesi tedbirini içeren karar Cumhuriyet savcısı tarafından ilgili adli kolluk birimine verildikten sonra, kolluk birimi bu karar doğrultusunda işlemleri yapacak kolluk personelinin aidiyet numarasını TİB'e bildirecektir. Bundan sonra bu kuralla ilgili işlemler bildirilen aidiyet numaralı personel tarafından yerine getirilecektir. Aidiyet numarası, iletişimin denetlenmesi tedbirinin uygulanması işlemlerini yapmak üzere görevlendirilen adli kolluk personeline[1204] kimliğinin belirlenmesini sağlamak amacıyla sicil numaralarından farklı olarak kurumlarınca verilen numaradır[1205].

İletişimin denetlenmesine ilişkin veriler, ceza yargılamasında kullanılmak üzere 5237 sayılı Türk Ceza Kanununda belirlenen dava zamanaşımı hükümleri dikkate alınmak suretiyle TİB tarafından arşivlenir. Denetleme işlemi, kararda belirtilen süre dolmadan önce sonlandırıldığında, bu durum Cumhuriyet savcısı tarafından derhal TİB'e bildirilir. TİB'in Kanuna aykırı kararlara karşı itiraz hakkı vardır. İletişimin denetlenmesi tedbirini uygulayacak, başka bir ifadeyle yerine getirilmesini denetleyecek kurum TİB'dir. Bu bağlamda, bu kurum dahil edilmeden yapılan iletişimin tespiti, dinlenmesi, kayda alınması ve sinyal bilgilerinin değerlendirilmesi sonucu Kanuna aykırı olarak elde edilmiş bulgular, hukuken değerlendirilemez ve delil olarak da kabul edilemez[1206].

Kişinin açık rızasının bulunması ve iletişim aracının kendisine ait olması şartıyla şikâyetçinin iletişiminin tespitine ilişkin işlemler de Cumhuriyet savcısının yazılı kararıyla TİB'den talep edilir. Hâkimin 24 saat içerisinde karar vermemesi veya talebi reddetmesi hâlinde tedbir Cumhuriyet savcısınca derhal kaldırılır ve durum TİB'e bildirilir[1207].

3.2.8.1.2. Telekomünikasyon İletişim Başkanlığı

İletişimin denetlenmesi tedbirlerine ilişkin kararların tek elden yürütülmesi amacıyla 5397 sayılı Kanunun 1. maddesi ile TİB kurulmuştur. Bu Kanun çerçevesinde yapılacak işlemler ile CMK'nın 135. maddesi çerçevesinde yapılacak denetlemeler , Telekomünikasyon Kurumu

---

[1204] KUNTER/YENİSEY/NUHOĞLU, s. 710; ÇOLAK/TAŞKIN, s.639.

[1205] ÇOLAK/TAŞKIN, s.636.

[1206] TAŞKIN, s.134.

[1207] TAŞKIN, s.134-135.

bünyesinde, bu kurumun başkanına doğrudan bağlı TİB tarafından ve tek bir merkezden yürütülmektedir[1208].

Telekomünikasyon İletişim Başkanlığı'nın görev ve çalışma usullerini düzenlemek üzere biri 10.11.2005 tarihli "Telekomünikasyon Yoluyla Yapılan İletişimin Tespiti, Dinlenmesi, Sinyal Bilgilerinin Değerlendirilmesi ve Kayda Alınmasına Dair Usul ve Esaslar ile Telekomünikasyon İletişim Başkanlığının Kuruluş, Görev ve Yetkileri Hakkında Yönetmelik" diğeri 14.01.2007 tarihli "Ceza Muhakemesi Kanununda Öngörülen Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi, Gizli Soruşturmacı Ve Teknik Araçlarla İzleme Tedbirlerinin Uygulanmasına İlişkin Yönetmelik" olmak üzere iki yönetmelik çıkarılmıştır.

İletişimin denetlenmesi tedbirini etkin olarak uygulanması ve yapılacak işlemlerin usul ve esasların detaylı olarak düzenlenmesi, AİHM'nin "Malone" kararında da vurguladığı üzere[1209], kamusal güçlere tanınan bu yetkinin hangi hallerde ve şartlarda tanındığının herkese açık bir şekilde bildirecek kadar net düzenlenmesi bağlamında yerinde olmuştur[1210]. TİB hakkındaki değerlendirilme aşağıda yapılacağından, bu başlık altında genel bilgiler verilmesiyle yetinilmiştir.

3.2.8.2. Kararın Yerine Getirilmesi

Ceza Muhakemesi Kanunu'nun 135. maddesi çerçevesinde verilmiş olan iletişimin denetlenmesi kararları, Cumhuriyet savcısı veya görevlendireceği adli kolluk görevlisi tarafından TİB'e iletilecektir. Bu sebeple kararların doğrudan GSM şirketlerine gönderilmesi mümkün değildir. Acele hallerde, savcının, kararın gönderilmesinden önce sözle veya telefonla da emir vererek yazılı kararın sonradan gönderilebileceğini ileri süren görüşler de bulunmasına rağmen[1211] kanaatimizce bu yaklaşım isabetli değildir. Nitekim, böyle bir düşünce, kararın hakim onayından kesinlikle geçeceği varsayımından kaynaklanmaktadır. Bu da, hakim adına önceden karar vermek anlamına gelecektir. Oysa ki, hakim iletişimin denetlenmesine karar verilmesi hususunda savcı gibi düşünmeme hakkına sahiptir. Aksinin kabulü, hakim kararına ipotek konulması olarak algılanacaktır.

[1208] ÜNVER/HAKERİ, s. 180; KUNTER/YENİSEY/NUHOĞLU, s. 713.

[1209] ANAYURT, s.52.

[1210] ÖZBEK, s. 431.

[1211] KUNTER/YENİSEY/NUHOĞLU, s. 713.

Tedbir kararları TİB'e verildikten sonra, bu kararlar ilgili GSM şirketinin bilgisi olmaksızın TİB görevlilerince ve TİB'nın koordinesinde yerine getirilecektir. Buna göre, tedbirin fiilen başladığı ve bitirildiği tarih ve saatler bu kişiler tarafından saptanarak bir tutanağa bağlanacaktır[1212].

İletişimin denetlenmesi tedbiri kapsamında elde edilecek deliller, Cumhuriyet savcılığı veya görevlendirilecek adli kolluk görevlisi tarafından çözümü yapılarak metin haline getirilecektir. Yabancı dildeki kayıtlar bir tercüman vasıtasıyla Türkçe'ye çevrilecektir. Konuşmaların bütünlüğünün bozulmaması için kayıtların tutanağa aktarılması sırasında ekleme ve çıkarma yapılamayacaktır. Bu sebeple sonradan bu tür iddiaların ileri sürülmesini engellemek için, kayıtların tutanağa geçirildikten sonra da muhafaza edilmesi gerekir. Ayrıca CMK'nın 153. maddesi çerçevesinde müdafii dosyayı inceleme hakkı çerçevesinde orijinal kayıtları incelemek istediğinde de bu kayıtlara ihtiyaç olacaktır[1213].

Bazı ülkelerdeki uygulamalarda olduğu gibi, kayıtların tutanağa aktarılması aşamasında metne müdahale edilmesi veya konuşmanın anlaşılmayan yerlerinin kaldırılması bakımından ortaya çıkabilecek anlam sapmalarının önüne geçebilmek için, denetimin bağımsız bir hakimlik kurumuna verilmesi de öğretide dile getirilmektedir[1214.] Benzer bir durumun var olduğu İngiliz hukukunda, İçişleri Bakanlığı (Home Office) tarafından iletişimin denetlenmesi ile ilgili olarak verilen kararlar (warrant), sürecin yasallığını denetlemek için kurulmuş özel bir mahkeme (tribunal) tarafından denetlenmektedir[1215]. RIPA'nın 65 vd. maddeleri uyarınca kurulan, iletişimin denetlenmesi ile ilgili şikayetleri, örneğin istihbarat memurlarının davranışlarını ya da genel olarak iletişimin denetlenmesi ile ilgili davranışları denetleyen, yüksek yargı mensuplarının üyesi olduğu bu mahkeme, RIPA kapsamında vuku bulan iletişimin denetlenmesi ile ilgili şikayetlerin götürüldüğü bir mercidir[1216]. ABD'de de önleme amaçlı denetlemeler için kurulmuş FISA İtiraz Mahkemesi[1217], iletişimin denetlenmesi

---

[1212] ÖZBEK, S.430;ÜNVER/HAKERİ, s. 180;CENTEL/ZAFER, s.365.

[1213]ÖZTÜRK/ERDEM, s.609; ÜNVER/HAKERİ, s. 181; ÖZBEK, s. 430;TURHAN, s. 271; KUNTER/YENİSEY/NUHOĞLU, s. 713.

[1214] ERDEM, s.103.Bu denetim anlayışının bir yansıması olarak, bazı ülkelerde, elde edilen bilgileri inceleme yetkisi olan ancak, kendisi hakkında tedbir uygulanan kişiye bu bilgileri aktarma yasağı ile sınırlandırılmış bir müdafilik sistemi benimsenmiştir. Bu sistem çerçevesinde, ilgilinin hakları korunmaktadır. (ERDEM, s.103).

[1215] MOWBRAY, s. 393.

[1216] FOSTER:, s. 389; RIPA, 65-70., http://www.opsi.gov.uk/Acts/acts2000/ukpga_20000023_en_2#pt1-ch1-pb1-l1g1 ,(İET:19.12.2007).

[1217] 50 U.S.C. § 1803(b).

amacıyla yapılmış taleplerin reddedilmesi halinde inceleme yapan bir mahkemedir[1218]. Bununla birlikte, bu mahkemenin çok fazla çalıştığı söylenemez. Nitekim, hükümet tarafından yapılan başvuruların hemen hepsi kabul edilmektedir. Gerçekten de, 2003 yılına kadar yapılan başvuruların hiçbirisi reddedilmemiş, 2003 tarihinde yapılan 4 başvuru için red kararı verilmiştir[1219].

Ülkemizde, böyle bir mahkeme kurulması yerine, süreci denetleme bağlamında yetkilendirilmiş kurul ya da organların ihdas edilmesinin daha pratik sonuçlar doğuracağını düşünmekteyiz. Gerek yürütme, gerekse yasama çatısı altında kurulabilecek bu kurul ya da organların yapacakları sürekli denetimlerin şeffaf bir süreci doğuracağı, bu şeffaflığın da kamu yararına hizmet edeceği kuşkusuzdur. Bu yarar, kuvvetler ayrılığı prensibinin gücünden kaynaklanan bir yarardır. Öte yandan, yargı içinde de, özellikle Adalet Bakanlığı Teftiş Kurulu'nun daha etkin çalıştırılması suretiyle bu süreç kontrol edilebilir. Bu denetimin, Teftiş Kurulu'nun yaptığı mutat teftiş haricinde, sadece bu amaca matuf bir teftiş olması gerekir. Aksi takdirde, denetim kalemlerinden bir tanesi olarak yapılacak kontrol, eski usulün devamı anlamına gelecek ve arzu edilen denetim yararı elde edilemeyecektir.

3.2.9.Adli Amaçlı İletişimin Denetlenmesi Tedbirinin Sona Ermesi

3.2.9.1. Tedbir Süresinin Sona Ermesi

İletişimin denetlenmesi tedbirine ancak belirli bir süre için karar verilebileceğine göre, bu sürenin sona ermesi halinde tedbire ilişkin karar hükümsüz kalacaktır. Bu durumda tedbirin uygulanmasına derhal son verilecektir. Sürenin bittiği tarihten sonra denetleme devam edilse de elde edilen bilgilerin delil olarak değerlendirilmesi mümkün değildir. Bu sebeple iletişimin denetlenmesi kararında öngörülen süre dolduğu anda ya da sürenin uzatılmasına ilişkin bir kararın da bulunmaması halinde tedbire, her hangi bir karara ihtiyaç duyulmadan ilgili kurumca kendiliğinden son verilmelidir[1220].

3.2.9.2. Hakim Onayının Alınamaması veya Red Kararı Verilmesi

Tedbirin sona ermesine ilişkin olarak CMK'nın 137/3. maddesinde sona erme nedenlerinden birisi olarak da Cumhuriyet savcısı tarafından gecikmesinde sakınca

---

[1218] 50 U.S.C. § 1803(b); BULZOMI,"Foreign Intelligence Surveillance Act", ; DONOHUE, s. 14-15; Ayrıca, Bk. DECKER, s.17; ADLER, s.3.

[1219] WONG, 3.4.4; Bk. The Attorney General's 2003 Report Submitted to the Administrative Office of the US Courts pursuant to FISA, 30 April 2004.

[1220] ÖZTÜRK/ERDEM, s.609.

bulunan durum gerekçesiyle verilmiş olan iletişimin denetlenmesi kararının yasal süre olan 24 saat içinde onaylanmaması veya hakimin bu süre içinde aksine karar vermesi halinde tedbire derhal son verileceği düzenlenmiştir. Bu durumda Cumhuriyet savcısı tarafından tedbir derhal kaldırılacaktır[1221].

3.2.9.3. Şüpheli Hakkında Kovuşturmaya Yer Olmadığına Karar Verilmesi

İletişimin denetlenmesi tedbirinin uygulandığı soruşturma çerçevesinde, elde edilen delillerin ışığında dava açmak için yeterli suç şüphesinin bulunmaması[1222] nedeniyle kamu davasının açılmasının mümkün olmaması halinde Cumhuriyet savcısı kovuşturmaya yer olmadığına karar verecektir. Bu karar sonrasında derhal iletişimin denetlenmesi tedbirine son verecektir[1223].

3.2.9.4. Tedbirin Şartlarının Ortadan Kalkması

İletişimin denetlenmesi tedbirinin sona ermesi sebepleri arasında yalnızca kararın uygulanması sırasında şüpheli hakkında kovuşturmaya yer olmadığına dair karar verilmesi ve Cumhuriyet savcısının CMK'nın 135/1. maddesindeki gerekçelerle vermiş olduğu kararın hakim tarafından onaylanmaması olarak düzenlenmişse de sona erme sebepleri bunlarla sınırlı tutulmamalıdır. Buna göre, tedbir süresi dolmadan ulaşılmak istenen delillere ulaşılması, şüphelinin bulunduğu yerin tespit edilmesi veya tedbirin sonuç vermeyeceğinin anlaşılması halinde tedbire son verilmelidir[1224]. Aynı şekilde şüpheli veya sanık hakkında tedbire başvurulan suçun CMK'nın 135/6. maddesinde sayılan katalog suçlardan olmadığının anlaşılması da sona erme sebebi olarak kabul edilmelidir.[1225] Kanaatimizce, hakkında tedbir uygulanan kişinin ölmesi durumunda da tedbir kendiliğinden sona ermelidir. Kişinin öldüğü anlaşılır anlaşılmaz tedbirin sonlandırılması bir zorunluluk olarak addedilmelidir. Nitekim, iletişim vasıtası açık olduğu takdirde ve tedbire devam edilmesi halinde, cihazı kullanan başka bir kişinin, hakkında herhangi bir tedbir kararı olmadığı halde iletişimine müdahale edilmiş olacaktır.

[1221] ÖZBEK, s. 431; ÖZTÜRK/ERDEM, s. 610; TURHAN, s.272.

[1222] 4422 sayılı ÇASÖMK'nun 2/7.maddesinde sona erme sebepleri , "şüphenin ortadan kalkmasını" bir sona erme nedeni olarak düzenlememişti.(ÖZTÜRK/ERDEM, s. 610).

[1223] ÖZBEK, s. 431;TURHAN, s. 272; ÖZTÜRK/ERDEM, s. 610; KUNTER/YENİSEY/NUHOĞLU, s. 715; ÇOLAK/TAŞKIN, s.637.

[1224] TURHAN, s.272; ÖZBEK, s.431-432; ÖZTÜRK/ERDEM, s. 610; KUNTER/YENİSEY/NUHOĞLU, s. 715; TAŞKIN, s. 140.

[1225] ÖZTÜRK/ERDEM, s. 610; ŞAHİN, s.385.

3.2.10.Tedbir Kapsamında Elde Edilen Bilgilerin Yok Edilmesi

İletişimin denetlenmesi tedbirinin uygulanması neticesinde elde edilen bilgilerin amaç dışı kullanılmasını önlemek için, şüpheli hakkında kovuşturmaya yer olmadığına dair karar verilmesi ve Cumhuriyet savcısının CMK'nın 135/1. maddesindeki gerekçelerle vermiş olduğu kararın hakim tarafından onaylanmaması hallerinde bu bilgilerin yok edileceği CMK'nın 137/3. maddesinde hüküm altına alınmıştır[1226]. İletişimin denetlenmesi sonucu elde edilen kayıt ve bilgilerin yok edilmesi AİHM'nin belirlediği kriterlerin de bir gereğidir[1227]. Mahkemeye göre, kayıtların silinmesi veya bantların imha edilmesi gerekli olan haller belirlenmelidir. Bu, özellikle de sanığın hukuki takibattan kurtulduğu veya beraat ettiği hallerde mutlaka yapılmalıdır[1228].

Buna göre, hukuka aykırı olarak uygulanmış tedbir sonucu elde edilmiş olan bilgilerin yok edilmesi gerekmektedir. CMK'nın 137/3. maddesinde tedbirin uygulanması sonucu elde edilen bilgilerin, savcının denetimi altında yok edileceği düzenlenmiş ve bu yükümlülüğün yerine getirilmesi, "tedbire son verilmesi" şartına bağlanmıştır. Bu kapsamda, tedbire son verilmesi tarihinden itibaren en geç 10 gün içinde[1229] tedbirin uygulanmasından elde edilen tespit ve kayıtlar yok edilecektir[1230].

İletişimin denetlenmesi tedbirinden elde edilen bilgilerin yok edilmesi, "kovuşturmaya yer olmadığı kararı verilmesi" veya "hakim onayının alınamaması" nedeniyle tedbire son verildiği durumlarda söz konusu olacağı CMK'nın 137/3. maddesindeki yasal düzenlemeden anlaşılmaktadır. Buna göre, bu iki hal dışındaki durumlarda, örneğin sanık hakkında açılan kamu davası sonucunda beraat kararı verilmesi halinde yok etme yükümlülüğünün söz konusu olamayacağı sonucuna varılmaktadır[1231]. Ancak öğretide, karşılaştırmalı hukukta olduğu gibi, tedbire gerek kalmadığı her durumda, yok etme yükümlülüğünün söz konusu olacağı yönünde bir düzenlemeye yer verilmesinin daha isabetli olacağı dile

---

[1226] Mülga 4422 sayılı kanunda suçların işlendiğine dair şüphenin ortadan kalkması halinde tedbir kapsamında elde edilen kayıt ve bilgilerin yok edileceği düzenlenmişti.; CMK'da ve 10.11.2005 tarihli Yönetmelikte sadece "yok etme" kavramı kullanılmasına karşın 14.01.2007 tarihli Yönetmelikte hem yok etme hem de imha kavramları birlikte kullanılmıştır.

[1227] ANAYURT, s.53.

[1228] HUVIG-FRANSA, Pr. 34-35.

[1229] Fransız CMK'ya göre, iletişimin denetlenmesi ile elde dilen bilgiler, kamu davasının zamanaşımı süresinin bitiminde başsavcı (procureur de la République) ya da genel savcının (procureur général) gözetiminde yok edilecektir. (Madde 100-6) Loi n°91 -646 du 10 juillet 1991 - art. 2.

[1230] ÖZTÜRK/ERDEM, s.610;TURHAN, s. 272;CENTEL/ZAFER, s. 365; ÜNVER/HAKERİ, s.182; ÖZBEK, s.432.

[1231] TURHAN, s. 272.

getirilmektedir[1232]. Biz de bu yaklaşımı benimsemekteyiz. Nitekim, iletişimin denetlenmesi gibi özel hayat hakkına ciddi bir müdahaleyi barındıran bir tedbirin, kovuşturmaya yer olmadığına ilişkin karara dek bekletilmesi AİHM'nin ihlal gerekçelerinin en önemlilerinden olan keyfilik yasağının gözardı edilmesi anlamına gelecektir. Gerçekten de, kovuşturmaya yer olmadığına ilişkin kararın, iş yoğunluğu nedeniyle gecikmeli olarak verilmesi halinde karar tarihine kadar tedbire devam edilmesi keyfi bir uygulama olacaktır. Bu durumda CMK 103. madde benzeri bir uygulama hayata geçirilebilir. Anılan maddenin ikinci paragrafında yer alan 'Soruşturma evresinde Cumhuriyet savcısı adlî kontrol veya tutuklamanın artık gereksiz olduğu kanısına varacak olursa, şüpheliyi re'sen serbest bırakır. Kovuşturmaya yer olmadığı kararı verildiğinde şüpheli serbest kalır. şeklindeki hüküm tartışma konusu durumla benzerlik göstermektedir. Savcının adli kontrol veya tutuklamanın gereksiz olduğu kanaatine varması halinde şüpheliyi serbest bırakması gibi, iletişimin denetlenmesi tedbirine de kovuşturmaya yer olmadığına ilişkin karar verilmesi beklemeden son verilmelidir.

Verilerin yok edilmesi için Cumhuriyet savcısı tarafından verilen kovuşturmaya yer olmadığına ilişkin kararın kesinleşmesinin beklenilip beklenilmeyeceği de irdelenmesi gerekli olan bir husustur. Bilindiği gibi, Cumhuriyet savcısı tarafından verilen bu karar, CMK'nın 173. maddesine göre itiraza tabi bir karardır ve bu karara karşı tebliğ tarihinden itibaren 15 gün içinde itiraz edilebilir. İtirazın en yakın ağır ceza mahkemesi başkanı tarafından incelenmesi belirli bir zaman alabilmektedir. Buna göre Cumhuriyet savcısı tarafından kovuşturmaya yer olmadığına karar verilmesi nedeniyle iletişimin denetlenmesine son verilmesinden itibaren 10 gün içinde verilerin yok edilmesi gerekeceği gibi, ilgililerin kovuşturmaya yer olmadığına ilişkin karara yaptıkları itirazın haklı bulunması da ihtimal dahilindedir. Bu nedenle, soruşturmanın genişletilmesine karar verilmesi söz konusu olabileceğinden elde edilen verilerin daha önce yok edilmiş olması bir takım sakıncalar doğurabilecekktir. Anılan nedenlerle, kovuşturmaya yer olmadığına dair kararın kesinleşmesinin beklenmesine gerek vardır[1233].

3.2.11. Adli Amaçlı İletişimin Denetlenmesinde İlgililere Bildirim

Diğer soruşturma ve kovuşturma tedbirlerinden farklı olarak, bu tedbire ilişkin karar ve işlemlerin gizli yürütülmesi sebebiyle, ilgili, tedbirin uygulanmasından önce veya uygulandığı sırada hakkında böyle bir tedbirin uygulandığından haberdar olamamakta ve bu durumda

[1232] ÖZTÜRK/ERDEM, s.610.

[1233] TAŞKIN, s.141-142.

ilgili, hukuksal korunma güvencesinden de fiilen yararlanamamaktadır. Bu durum, soruşturmanın gizliliğinden kaynaklanmaktadır.

İletişimin denetlenmesi tedbirine son verildikten sonra, ilgiliye, hakkında tedbir uygulandığı konusunda bilgi verilmesi Anayasa'nın 36. maddesinde düzenlenmiş olan "Hukuksal korunma güvencesi" ilkesinin ve yine Anayasa'nın 38/4 ve AİHS'nin 6. maddesindeki düzenlemelerin getirdiği bir zorunluluktur. Tedbir sonrasında, hakkında tedbir uygulanan kişiye bildirimde bulunulması tedbirin gizli olma niteliğiyle bağdaşmaz değildir. Nitekim, CMK'nın 135/5. maddesinde yer alan gizlilik, tedbir süresince geçerlidir ve tedbir sona erdikten sonra şüpheli veya sanığa muhakemeye aktif olarak etkide bulunma imkanının verilmesi amacıyla bildirim yapılması bir zorunluluktur[1234].

Haber verme yükümlülüğüne ilişkin olarak AİHM değişik kararlarında, iletişimin dinlenmesi ve kayda alınmasının milli güvenlik, suçların önlenmesi ve kamu düzeni gerekçeleriyle mümkün olduğunu ve bu denetleme tedbirine ilişkin faaliyetlerin AİHS'nin 8. maddesine aykırı olmadığını, ancak, ulaşılmak istenen amaç tehlikeye düşmeyecek ise iletişimin denetlenmesi kapsamında dinleme ve kayda alma işleminin sonradan ilgilisine haber verilmesi gerektiği belirtilmiştir[1235]. İletişimin denetlenmesi tedbirinin sonlandırılması sonrasında ilgiliye bildirimde[1236] bulunulması, keyfiliği önleyici yasal güvenceler bakımından büyük önem taşımaktadır[1237]. Keyfilikten kaynaklanabilecek tehlikelerin önlenmesi amacıyla[1238], AİHM, dinleme sona erdiğinde gizli dinlemeye ilişkin olarak ilgiliye sonradan bilgi verilmesi gerekliliğine dikkat çekmiştir. Bununla birlikte, bildirimin yapılması, amacı tehlikeye düşürmemelidir[1239]. Bu yaklaşımın altında yatan temel neden, hakkına müdahale edilen bireyin müdahalenin gizliliği nedeniyle müdahalenin hukukiliğini denetleme imkanından yoksun olmasıdır[1240]. Bu zorunluluk, aynı zamanda, AİHS'nin

---

[1234] SÖZÜER, s. 110;ÖZTÜRK/ERDEM, s.611; ÖZBEK, s. 432;TURHAN, s. 273.

[1235] TEZCAN, Durmuş/ERDEM, M. Ruhan/SANCAKTAR, Oğuz: AİHS Işığında Türkiye'nin İnsan Hakları Sorunu, Ankara 2004, s.406;ÖZBEK, s.406; Örneğin Klass ve Kruslin kararlarında bu hususlar vurgulanmıştır.(ANAYURT, s.51).

[1236] Klass-Federal Almanya kararında, konuyla ilgili terim 'subsequent notification' olarak yer almaktadır. Sözkonusu ifade, kararın Fransızca metninde, 'la notification ultérieure' olarak kullanılmaktadır. Subsequent/ ultérieure sıfatları 'sonraki' anlamına geldiği için 'sonradan bildirim' olarak da çevrilen bu kavramın, bildirim ya da 'tedbir sonrası bildirim' ya da sadece 'bildirim' olarak kullanılmasının daha uygun olacağını düşünmekteyiz.

[1237] KÜNHE, s. 103.

[1238] Bk. KRUSLIN-FRANSA ve HUVIG-FRANSA davaları.

[1239] TEZCAN/ERDEM/SANCAKDAR, s. 238.

[1240] Bk. KLASS-ALMANYA.

13. maddesinde ifadesini bulan, "ulusal bir makama etkili bir başvuru yapabilme hakkı"ndan da kaynaklanmaktadır[1241].

ABD mevzuatında yer alan bu kurum mahkeme kararıyla yapılan eleştirilerle gündeme taşınmıştır. Gerçekten de, Berger kararında yapılan tespit sonrasında Teknik Dinleme Kanunu çıkarılmıştır. Anılan karara göre, şüpheliye, dinleme sonrasında telefonunun dinlendiği bilgisinin verilmemesi, sanığın mahkemede kendi aleyhine delil olarak kullanılacak bilgilerden haberdar olamaması gibi bir sonuç doğurmaktadır ki bu durum iddia ve savunma taraflarının eşit imkanlara sahip olması (equality of arms) prensibini, dolayısıyla adil yargılanma ilkesini ihlal etmektedir[1242].

Mevzuatımızda, kişiye bildirim yapılması hususunu düzenleyen birtakım düzenlemeler bulunmaktadır. Bunların başında Anayasamızın 40. maddesi gelmektedir. Anılan maddede yer alan, "Anayasa ile tanınmış hak ve hürriyetleri ihlal edilen herkes, yetkili makama geciktirilmeden başvurma imkanının sağlanmasını isteme hakkına sahiptir" hükmü hak arama hürriyetinin kullanılabilmesi bakımından, ilgililerin, kendileri hakkında uygulanan hak sınırlayıcı işlemlerden haberdar edilmelerini gerekli kılmaktadır[1243].

Adli amaçlı iletişimin denetlenmesinin düzenlendiği CMK'da da ilgiliye haber verilmesinin şartları düzenlenmiştir. Gerçekten de, iletişimin denetlenmesi kararı çerçevesinde elde edilen tespit ve kayıtlar hakkında ilgiliye haber verilmesinin öncelikli şartı, CMK'nın 137/3. maddesi uyarınca tedbire,

- "kovuşturmaya yer olmadığı kararı verilmesi" veya
- "hakim onayının alınmaması"

nedeniyle son verilmiş olması ve bu sona ermenin ardından da iletişimin tespiti ve kaydına ilişkin elde edilen bilgi ve kayıtların yok edilmiş olmasıdır. Bu bağlamda, bildirim ancak ilgili hakkında "kovuşturmaya yer olmadığı kararı verilmesi" veya "hakim onayının alınmaması" nedeniyle tedbire son verilmesi neticesinde ve dökümanların yok edilmesinden sonra ilgililere haber verilebilecektir[1244]. Hakkında dava açılan veya bu

---

[1241] TAŞKIN, s.147.

[1242] BERGER-NEW YORK, 388, Pr.60.

[1243] TAŞKIN, s.148.

[1244] Almanya, Amerika Birleşik Devletleri ve Avusturya'da iletişimin denetlenmesi kararına son verildiğinde, bu işlem ilgilisine haber verilmektedir. İsviçre'de ilgililere bildirim kanunla düzenlenmiş değildir. Ancak yüksek mahkeme kararı gereğince ilgililere bildirim uygulanmaktadır. Fransa'da ilgililere bildirim kanunla düzenlenmemiştir. Ancak Fransa'da soruşturma ve kovuşturma aşamasında dava dosyası tamamen tarafların denetimine açıktır. Bu nedenle ilgililer iletişimin denetlendiğini öğrenebilmektedirler. İngiltere'de

kapsamda başka tedbirlerle delil elde edilmesi amacıyla soruşturması devam eden kişiye bildirim yapılmayacaktır. Bunun yanısıra, elde edilen bilgi ve belgelerin ilgili hakkında delil olarak kullanılacak olması durumunda bildirim yapılmayacaktır. Çünkü ilgili kişi kovuşturma aşamasında hakkında açılan davanın dosyasından bilgi edinebilecektir. Bunun yanısıra, Bilgi Edinme Kanunu çerçevesinde herkes hakkında böyle bir tedbir uygulanıp uygulanmadığı hususunu her zaman sorabilir[1245].

Bildirim, soruşturma evresinin bitmesinden itibaren 15 gün içinde yapılmalıdır. Belirlenen bu süre, kovuşturmaya yer olmadığına ilişkin kararın kesinleşmesinden itibaren başlayacaktır[1246]. Bildirim yükümlülüğüne ilişkin sürenin başlamasından itibaren 15 gün içinde Cumhuriyet savcılığı, tedbirin nedeni, kapsamı, süresi, ve sonucu hakkında ilgilisine yazılı olarak bilgi verecektir.

Hakkında dava açılan veya bu kapsamda başka tedbirlerle delil elde edilmesi amacıyla soruşturması devam eden ya da elde edilen kayıt ve tespite ilişkin veri ve kayıtlar hakkında delil olarak kullanılacak kişilere de, soruşturmanın amacını tehlikeye düşürmemek koşuluyla, bildirimde bulunulmasının sağlanması gerektiği[1247] görüşü bizce de tutarlıdır. Bildirimin yapılmasının gerektiğine karar verecek merci, bu bildirimin soruşturmanın amacını tehlikeye düşürmeyeceğini en iyi bilecek kişi olduğundan böyle bir uygulamada bir sakınca yoktur.

CMK'nın 137/4. maddesinde bildirim yapılacak kişiler için "şüpheli veya sanık" kavramı kullanılmamış, "ilgili" kavramı tercih edilmiştir. Bu şekildeki bir ifadenin, üçüncü kişileri de kapsadığı görüşü[1248], hayatın gerçekleriyle pek örtüşmemektedir. Gerçekten de, iletişimin denetlendiği süre zarfında, şüpheli veya sanığın görüştüğü herkese bildirim yapılması oldukça kapsamlı bir iş yükü ve maliyeti beraberinde getirecektir. Öte yandan, üçüncü kişilerle ilgili olarak bir suç isnadında da bulunulmamaktadır[1249].

---

ise iletişimin denetlenmesi işlemi ilgilisine bildirilmemektedir. Ancak bu ülkede iletişimin denetlenmesi yoluyla elde edilen bilgi, bulgu ve deliler hiçbir şekilde mahkemede delil olarak kullanılamamaktadır (SÖZÜER, s. 88 vd).

[1245] ÖZBEK, s. 433; TURHAN, s. 173; TAŞKIN, s.147.

[1246] CENTEL/ZAFER, s.366; CMK'nın 137/4. maddesinde 5353 sayılı kanun ile değişiklik yapılmadan önce bildirim yükümlülüğünde süre, kayıtların yok edilmesinden sonra başlamaktaydı.

[1247] TURHAN, s.273; Almanya'da iletişimin denetlenmesi tedbirinin uygulanmasından sonra ilgiliye haber verilmesi zorunluluğu öngörülmüş, ancak bunun için "soruşturmanın amacının tehlikeye düşmeyecek olması" koşulu aranmıştır. Yükümlülüğün kapsamına yalnızca şüpheli veya sanık değil, tedbirden etkilenen üçüncü kişilerin de gireceği öngörülmüştür.(ERDEM, s.106).

[1248] ÖZTÜRK/ERDEM, s.611; ÖZBEK, s. 433; TURHAN, s. 173; KUNTER/YENİSEY/NUHOĞLU, s. 715; Almanya'da yükümlülüğün kapsamına yalnızca şüpheli veya sanık değil, tedbirden etkilenen üçüncü kişilerin de gireceği öngörülmüştür.

[1249] TAŞKIN, s. 150.

3.2.12. Adli Amaçlı İletişimin Denetlenmesi Suretiyle Elde Edilen Delillerin Değerlendirilmesi

Soruşturma veya kovuşturma esnasında elde edilmiş bilgi ve belgelerin delil olarak duruşmada kullanılabilmesi için, soruşturma ve kovuşturma organları tarafından "hukuka uygun" bir şekilde elde edilmiş olmaları gerekir[1250]. Delil serbestisi sistemi ilkesinin gereği olarak, hukuka uygun olarak elde edilmiş ses veya görüntü kayıtları, ancak tahrifata uğradığı veya sahte olduğu hususunda bir tereddüt bulunmadığı takdirde ispat aracı olarak kullanılabilir[1251]. Bu sebeple iletişimin denetlenmesi kapsamında elde edilen kayıt ve işlemlerin delil olarak değerlendirilebilmesi için, öncelikle usulüne uygun olarak verilmiş bir tedbir kararının olması ve bu kararın uygulanması neticesinde, karara konu suç ve kişilere ilişkin olarak elde edilmiş bir delilin olması gerekir[1252]. Bu hususa uyulmadan elde edilen bilgilerin yargılamada delil olarak kullanılması mümkün değildir. Ancak, usulüne uygun olarak, yetkili ve görevli yargılama makamı tarafından verilen iletişimin denetlenmesi kararı, devletin, özel hayatın gizli alanına girmesine izin verir. Arayan kişilerin, şüpheli veya sanıkla yaptıkları konuşmalar da, hakimin kararı içinde kaldığı için, hukuka uygun bir şekilde dinlenebilir ve kayda alınabilir[1253].

İletişimin denetlenmesinde olduğu gibi denetleme sonucu elde edilen verilerin kullanılmasında da denetleme amacına uygun hareket edilmeli, denetleme sonucu elde edilen bilgiler, işlenmiş suçu kanıtlanması dışında başka bir amaçla kullanılmamalıdır[1254]. Elde edilen delillerin, gerekli olan koşullara uygun hareket edilmesi şartıyla, her türlü suçun yargılaması için kullanılabilmesi gerektiği[1255] düşüncesine katılmak mümkün değildir. Katalog suçlarla ilgili olarak başlanan iletişimin denetlenmesi ile elde edilen delillerin her türlü soruşturma ve kovuşturma kapsamında kullanılması, haberleşme özgürlüğünün ve gizliliğinin özünün yok edilmesine yol açacaktır. Bu tedbirle elde edilen bilgiler bir disiplin soruşturmasında doğrudan

---

[1250] KUNTER/YENİSEY/NUHOĞLU, s. 710; YENİSEY /ALTUNÇ, s.19;ÖZTÜRK/ERDEM, s.271; BAYRAM, s.1.

[1251] YILDIZ, Ali Kemal: “Ses ve/veya Görüntü Kayıtlarının İspat Fonksiyonu”, Ceza Hukuku Dergisi, Yıl 1, Sayı 2, Aralık 2006, s. 256.

[1252] YENİSEY /ALTUNÇ, s.19.

[1253] YENİSEY /ALTUNÇ, s.23-24.

[1254] KEKLIK, s. 2.; TAŞKIN, s. 171.

[1255] ÜNVER, Ceza Muhakemesinde…, s. 148.

kullanılamaz ve yine bu bilgilere dayanılarak tazminat davası açılamaz. Çünkü kanun koyucu, bu tedbire sadece katalog suçların aydınlatılması amacıyla izin vermiştir[1256]. Olağanüstü bir nitelik taşıyan, diğer delillerden bir yarar elde edilemediğinde başvurulan, başka bir ifadeyle son çare olarak görülen bu tedbirden ikincil bir mahiyette yararlanılmasına izin verilmesi[1257], kanaatimizce, devletin bireyle yaptığı sözleşmenin ihlali anlamına gelir. Devletin yaptığı sözleşme ifadesinden kasıt şudur ki, devlet, ancak belli suçlarda bu tedbire başvurulabileceğini yaptığı kanunlarla deklare etmiştir. Bu deklarasyon sonucunda elde edilen bilgilerin başka soruşturma ya da işlemlerde kullanılmasına izin vermek ahde vefa ilkesine ve 'öngörülebilirlik' ilkesine aykırı bir tutum olur. Bir nevi 'örtülü af' ya da 'kovuşturma bağışıklığı' olarak ifade edilebilecek olan bu sistem, ABD'de uygulanan dava pazarlığı (plea bargaining) uygulamasıyla benzer bir mantığa sahiptir. Benzer bir diğer örnek de, Suçluların İadesine Dair Avrupa Sözleşmesinde varolan 'Hususilik Kuralı'dır. Anılan Sözleşmenin 14. maddesinin 1. paragrafında 'İade edilen şahıs iadeden evvel işlediği ve iadeye esas olandan başka bir fiilden dolayı takip veya muhakeme edilemeyeceği gibi bir ceza veya emniyet tedbirinin infazı için tevkif edilemez veya herhangi bir surette hürriyeti kısıtlanamaz' ifadesi yer almaktadır. Hususilik kuralı, iade edilen kişiye tanınmış bir nevi ayrıcalıktır. İade edilen kişi böylece sadece iadeye konu olan suçtan dolayı takibat altına girmekte, bu suçtan daha önce işlediği suç ya da suçları açısından bir tür takipsizlik garantisi elde etmektedir[1258].

İletişimin denetlenmesi tedbiri çerçevesinde elde edilen bilgilerden oluşan delillerin "hukuka aykırı" olduğu iddiası, sanık tarafından CMK'nın 206/2-a maddesi uyarınca süresi içinde ileri sürülebilecektir. Ancak sonradan yapılan hukuka aykırılık iddiası dinlenmeyecektir.Yasal koşulları oluşmadığı halde hakim tarafından verilen denetleme

---

[1256] ÖZTÜRK-ERDEM, s. 602.;TAŞKIN, s. 177-178.

[1257] Yargıtay Ceza Genel Kurulu'nun 26.1.2006 tarihli kararına karşıoy yazan Yargıtay üyesi Koçak, ABD'deki Leon davasına atıf yaparak, yargılamayı yapan mahkemenin, uyuşturucunun arama izni verilen yerin dışında bulunması halinde yargılamada delil olarak kullanılabileceğine karar vermesine dikkat çekmektedir. Mahkemeye göre, polis, uyuşturucunun elde edildiği yere ilişkin arama izni istemiş olsaydı, mahkeme bu izni verecekti. O halde uyuşturucunun bulunduğu yer arama izni kapsamındadır. Mahkeme, "İyi niyet" (Good Faith) çerçevesinde yarar dengesini gözetmektedir. Keza Alman hukukunda elde edilen deliller çok gizli ve özel hayat alanına ilişkinse delil olarak kullanılmaz. Ancak normal gizli hayata ilişkin ise devletin cezalandırmaktaki menfaati ile sanığın kişiliğinin korunmasına ilişkin menfaat arasındaki dengeye bakılacaktır. İşlenen suç ağır ise delil olarak kullanılacaktır. Burada da yarar dengesine bakılmaktadır. (CGK, 2006/4.MD-122 E., 2006/162 K., 13.06.2006)

[1258] Bununla birlikte, iade edilen kişinin, iadeye konu suçtan daha önce işlediği başka bir suçtan takibata konu olabilmesi için iki yol vardır. Bunlardan ilki, iade eden devletin bu hususa muvafakat etmesidir. İkinci yol ise, iade edilen şahsın, nihai olarak hürriyetine kavuşmasını takip eden 45 gün zarfında iade edildiği tarafın arazisini elinde imkân olduğu halde terk etmemesi veya terk ettikten sonra buraya geri dönmesidir. (http://www.uhdigm .adalet.gov.tr/ guncelleme/ aksoz/ sidas. Htm (İET:29.1.2008)).

kararıyla elde edilmiş olan bilgiler değerlendirildiğinde, kişi, kendisi lehine sonuçlar elde edebileceği gibi suçsuzluğunu dahi ortaya koyabilir. Kişi, suç işlenirken kendisinin yaptığı katkının tali nitelikte kaldığını ispat edebileceği gibi, suçun işlendiği sırada kusur ehliyetinin önemli surette azalmış olduğu iddiasını da ileri sürebilecektir[1259].

Bu yolla elde edilen delillerin değerlendirilmesinde, esas hakkında hüküm veren hakim, duruşmada kullanılması istenen bir telefon dinleme delilinin "hukuka uygunluğunu", sadece "sanık tarafından zamanlıca iddia edildiği takdirde" inceler. Bununla birlikte, esas hakkında hüküm verecek olan hakimin, soruşturma evresinde yapılmış olan bütün araştırma ve soruşturma işlemlerinin maddi hukuka uygun olarak yapılıp yapılmadığını kendiliğinden denetleme yetkisinin de mevcut bulunduğunun unutulmaması gerekir. Hakim, soruşturma evresinin Kanun hükümlerine uygun olarak yapılmış bulunduğunu, kural olarak kabul etmek durumundadır[1260].

CMK'nın 206/1. maddesi uyarınca, duruşmanın başında deliller ikame edilirken, müdafiin istemi üzerine mahkeme başkanına bu delillin Kanuna aykırı olarak elde edilmiş olması nedeniyle ikame edilmemesine karar vermesinin yolu açılmış bulunmaktadır. Eğer mahkeme başkanı, dinlemenin Kanuna aykırı bir şekilde verilmiş bir hakim kararına dayandığına kanaat getirecek olursa, bunun ayrıntılı gerekçesini CMK m. 230 uyarınca hazırlayarak bu delili kullanmayabilecektir[1261]. Bununla birlikte, Cumhuriyet savcısının CMK'nın 206. maddesi gereğince delil ikamesi talebini, "hukuka uygun bularak" kabul eden hakimin, "gerekçe gösterme mecburiyeti" yoktur. Esas hakkında hüküm veren hakimin, hükmün gerekçesinde "dinlemenin hukuka uygun bulunmasının gerekçelerini de açıklamak zorunda olduğu" görüşüne katılmak mümkün değildir[1262] Nitekim, mevzuatımızda, mahkemenin kabul ettiği delillerin hukuka uygunluğunu gerekçelendirme mecburiyeti öngörülmemiştir. Soruşturma evresinde denetleme kararı veren hakim kararının hukuka uygun olup olmadığının belirlenmesi sorunu, bütün usuli işlemler gibi, serbest ispat kuralları ile denetlenebilen bir konudur. Davanın esas hakkındaki hükmü veren hakim, iletişimin denetlenmesi tedbirinden elde edilen bilgileri delil olarak kullanmışsa, bunların "değerlendirilebilir delil" olduklarının ayrıca açıklanması gerekmeyecektir. Ancak, usul hukukuna aykırılık iddiası ileriye

[1259] YENİSEY /ALTUNÇ, s.19.

[1260] YENİSEY /ALTUNÇ, s.20.

[1261] YENİSEY /ALTUNÇ, s.31.

[1262] YENİSEY /ALTUNÇ, s.30-31.

sürüldüğünde, Yargıtay dinlemeden elde edilen bilgilerin değerlendirme kapsamı içinde bulunup bulunmadığını ve hükmün buna dayanıp dayanmadığını inceleyecektir[1263].

Cumhuriyet savcısı tarafından verilen kararın hakim onayına sunulmamış olması veya sunulmuş olmakla birlikte bu kararın hakim tarafından reddedilmemiş olması durumunda, bu süre içinde elde edilen bilgilerin delil olarak değerlendirilip değerlendirilemeyeceği hususu CMK'da açıkça düzenlenmemiştir. Bu süre zarfında elde edilmiş olan bilgilerin delil olarak kullanılamaması gerektiği şeklindeki[1264] görüş bizce de isabetlidir. Nitekim, bu tür uygulamaların kabul edilmesi, hukuka aykırı olarak yapıldığı için 'yolsuz denetleme' olarak adlandırılabilecek bir sürece müsamaha edilmesi anlamına gelecektir. Böyle bir uygulamaya izin verilmesi ise, "Pandora'nın Kutusu" nun açılması anlamına gelecektir. Bu şekilde elde edilen bilgilerin, diğer yasadışı delil yöntemleriyle elde edilen bilgiler gibi kabul edilmesi gerekmektedir. Nitekim 'zehirli ağacın meyvesi de zehirlidir'dir.

Bu şekilde elde edilen bilgiler yok edilse dahi tedbiri gerçekleştiren memurun tanık olarak dinlenmesi ve bu bilgilerin yargılamada değerlendirilmesinin sağlanması şeklindeki görüşler de kabul edilebilir değildir[1265]. Soruşturmayı önemli derecede aydınlatacak önemli bir delil niteliği taşısa dahi, bu bilgilerin soruşturma dosyasına konulmaması ve yargılama sonunda verilecek kararda bu bilgilere dayanılmaması sağlanmalıdır[1266.]

Bilginin delil sıfatını kazanması için usulüne göre elde edilmiş olması mutlak zorunluluktur. Bu zorunluluğun bütünüyle kaldırılması yasal engellerle karşılaşacağı için, bu direnç, kanunların ve usulün gevşek uygulanması ve esnetilmesi suretiyle aşılmaya çalışılmaktadır. Antidemokratik bir anlayışa vize verilmesi anlamına gelen bu tür uygulamalara tevessül edilmesi, aslında dünyanın birçok yerinde görülmekte ve eleştirilmektedir[1267].

[1263] YENİSEY /ALTUNÇ, s.31.

[1264] ÖZTÜRK/ERDEM, s.604;TURHAN, s.268-269; ÇOLAK/TAŞKIN, s.631.

[1265] KUNTER/YENİSEY/NUHOĞLU, s. 705.

[1266] TAŞKIN, s.111-112.

[1267] Mahkeme kararı olmaksızın numara tespit cihazı kullanımı ile ilgili olarak verilen Smith-Maryland (1979) kararı, mahkeme kararı olmaksızın elektronik sinyal verici kullanımı ile ilgili olarak verilen ABD-Knotts (1983) kararı, mahkeme kararında ismi geçmeyen kişinin haberleşmesinin yine bu mahkeme kararına istinaden dinlenilmesi ile ilgili ABD-Donovan(1977) kararı gibi kararlar ile usule aykırı olarak elde edilen bilgilerin delil olarak kullanılmasına zımni izin verilmiştir. Kamuoyu tarafından çok ciddi olarak eleştirilen bu kararlar, ABD adalet mekanizmasının, şüphelinin itham edilmesi ile ilgili olarak elde edilen bilgileri her ne şekilde elde edilirse edilsin kullanmak istediğini göstermektedir. (18 U.S.C. § 2518(5)).

3.2.13. Tesadüfen Elde Edilen Delillerin Durumu

3.2.13.1. Genel Olarak

Türk hukukunda şüpheli veya sanık konumuna girmiş olan kişilerin, iletişiminin denetlenmesine imkan tanınmakta, hakkında soruşturma evresi başlamadığı için henüz şüpheli konumuna girmiş olmayan bir kişi hakkında iletişimin denetlenmesi hiçbir şekilde kabul edilmemektedir[1268]. Karşılaştırmalı hukukta ise henüz "şüpheli " durumuna girmiş olmayan kişilerin de, en son çare olarak iletişimlerinin denetlenmesi kabul edilmişken, hukumuzda sadece "şüpheli ve sanık " haline gelmiş olan kişilerle ilgili dinleme yetkisi vermiştir[1269]. Bu durum, kanaatimizce, kişi hak ve hürriyetlerine ve AİHM tarafından belirlenen standartlara kanun koyucu tarafından verilen önemin bir göstergesi olarak değerlendirilmelidir. Gerçeken de, AİHM, hürriyetlerin kısıtlanmasında daraltıcı yorum yapılması esasını benimsemiştir.

CMK'nın 138/2. maddesinde iletişimin dinlenmesinden elde edilen tesadüfi delillerin kullanılma şartları düzenlenmiştir. Şüpheli konumuna girdiği için, iletişiminin dinlenmesi kararı verilmiş olan bir kişi ile konuşan, henüz "şüpheli" konumunda olmayan başka bir kişinin, katalog suçu işlediği şüphesi ortaya çıkarsa, bu tesadüfi bilginin ileride "delil" olarak kullanılması mümkündür. Fakat, hakimin denetleme kararını verdiği sırada, hakkında dinleme kararı verilen kişi henüz şüpheli konumuna girmemişse, yani CMK'nın 160. maddesi uyarınca Cumhuriyet savcısı tarafından soruşturma başlatılmadan iletişimin dinlenmesi kararı verilmiş ise, bu karar hukuka aykırı bir karar

---

[1268] ABD hukukuna göre, iletişimin dinlenmesi esnasında mahkeme kararında belirtilen sınırların aşılmaması bakımından elden gelen gayret gösterilmelidir. Mahkeme kararında belirtilen sınırlar ifadesi kullanılırken kastedilen iki şey vardır. Bunlardan ilki, mahkeme kararında ismi geçmeyen kişilerin mümkün olabildiği ölçüde dinleme kapsamına alınmamasına riayet edilmesidir. Kastedilen ikinci unsur, mahkeme kararında isimleri belirtilen kişilerin, sadece karar konusu suçlardan dolayı dinlenmelerinin sağlanmasıdır. Diğer bir ifadeyle, bu kişilerin kararda belirtilmeyen suçları işlemeleri durumunda, kararda değinilmeyen suçlardan dolayı dinlemeye alınmalarının önlenmesidir. (18 U.S.C. § 2518(5)).

[1269] YENİSEY /ALTUNÇ, s.28; Almanya'da tesadüfen elde edilen deliller, dinleme kararına konu katalog suçla ilgili ise, delil olarak değerlendirilmektedir. Dinleme konusu olmamakla birlikte katalog suçla bağlantılı bir başka suç ise delil sayılmaktadır. Ancak katalog suçla bağlantılı değilse, tamamen bunların dışında bir suçla ilgili ise bu bilgiler delil olarak değerlendirilmemektedir. Ayrıca Alman CMK § 100b V uyarınca uzakla haberleşmenin denetlenmesi sonucu elde edilen bilgiler, bir başka ceza muhakemesinde, 100a'da öngörülen suçlardan birisinin aydınlatılması amacıyla delil olarak değerlendirilebilmektedir. Birleşik Krallık'ta usulüne uygun verilmiş karara göre yapılan telefon dinleme sonucu elde edilen bilgiler hiç bir şekilde ceza muhakemesinde delil olarak kullanılamaz. Ancak bu bilgilere dayanarak elde edilen diğer bulgular, delil olarak kullanılmaktadır. Fransa'da usulüne uygun olarak verilmiş karara göre yapılan dinleme sonucunda elde edilen bilgiler, delil değil, sadece belirti sayılmaktadır. Tesadüfen elde edilen bilgiler haliyle değerlendirilmemektedir.(SÖZÜER, s. 88-108 ; ÖZDOĞAN, Ali: "Alman ve Fransız Teknik Dinleme Mevzuatları", (www.egm.gov.tr /polis.dergisi.S.32., s. 1-4;YİĞİT, s. 34).

olacağından “hukuka aykırı” hakim kararından “hukuka uygun delil” çıkması mümkün değildir[1270].

Yargıtay yakın tarihli bir kararında, bu hususa ilişkin olarak şöyle bir karar vermiştir: Somut olayda, şikayetçi kendisine karşı gerçekleştirilen telefonla tehdit ve hakaret suçlarının faillerinin belirlenebilmesi için, ev ve cep telefonlarıyla çeşitli tarihlerde yaptığı görüşme kayıtlarının incelenmesini ve muhtemel aramalara karşı da telefonlarının dinlenmesini istemiştir. Cumhuriyet savcılığı bu talep üzerine, ilgili servis sağlayıcı kuruma başvurmuş, ancak kurum bu başvurunun gereğini yerine getirmekten kaçınmıştır. Cumhuriyet Savcılığı, CMK’nın 135. maddesi uyarınca bir karar verilmesi için sulh ceza mahkemesine başvurduğunda ise, söz konusu suçun katalog suçlardan olmadığı, bu nedenle de iletişimin denetlenemeyeceği cevabıyla karşılaşmıştır. Buna ilişkin olarak da Yargıtay 4. Ceza Dairesi, sulh ceza hakiminin ulaştığı neticeyi benimsemekle beraber, kararın gerekçesini isabetli bulmamıştır. Daireye göre, iletişimin tespiti, CMK’ nın 135. maddesinde belirlenen katalog suçlar bakımından getirilen sınırlamaya bağlı olmaksızın tüm suçlar açısından uygulanabilmektedir. Ancak bu tedbire sadece şüpheli veya sanık için başvurulabilir. Şikayetçinin veya suçtan zarar görenin iletişiminin tespiti CMK 135. maddesi kapsamında değil, Cumhuriyet savcısının CMK’nın 160 ve 161. maddesinde yer alan genel soruşturma ve kanıt toplama yetkisi çerçevesinde değerlendirmenin isabetli olacağına karar vermiştir[1271].

İletişimin denetlenmesi kararının verildiği ilk aşamada, ilgili kişiler henüz şüpheli konumuna girmemiş olup, bu kişilerden birisi müşteki konumundadır. İletişimin denetlenmesi kararının kurucu unsurlarından olan “başka suretle delil elde edilmesi imkanının bulunmaması” unsurları gerçekleşmemiş ve suç işlendiğine ilişkin kuvvetli şüphe sebeplerinin nelerden ibaret bulunduğu da gösterilmemiştir. Bu nedenle, hakim tarafından verilmiş de olsa, iletişimin denetlenmesi kararının “hukuka aykırı bir karar olduğu” söylenebilecektir. Bu saptama doğrultusunda, hukuka aykırı bir denetleme kararından elde edilen tesadüfi delillerin de, katalog suçu kapsamında olsalar dahi, hüküm verilirken kullanılamayacağı söylenebilir[1272].

AİHM’nin, bir anlamda tesadüfen elde edilen delilleri de irdeleyen Kruslin/Fransa kararına konu olan olayda, başvurucu, telefonu dinlenmekte olan bir yakınının evinde,

---

[1270] YENİSEY /ALTUNÇ, s.29.

[1271] YENİSEY /ALTUNÇ, s.29; 4. CD., 2006/4669 E., 2006/17007 K., 29.11.2006.

[1272] YENİSEY /ALTUNÇ, s.31.

onun telefonundan konuşmuş ve bu şekilde elde edilen konuşmalar delil olarak kullanılmıştır. Diğer bir deyişle, alınan iletişimin denetlenmesi kararı hakkında mahkeme kararı bulunan kişiyle ilgili değildir. Bu nedenle, dinlenen konuşmalardan elde edilen deliller, tesadüfen elde edilmiş sayılmaktadır. Mahkeme, her ne kadar ihlal kararı vermişse de, bu kararına gerekçe olarak, yapılan müdahalenin, kanunla öngörülebilir olmamasını göstermiştir. Başka bir anlatımla, Mahkeme, iletişimin denetlenmesi ile ilgili bir kanunun varlığını saptamakla beraber, bu kanunun ne ilgililer açısından bir çerçeve çizebildiğini ne de keyfi uygulamaları önleyebilecek tedbirlere yer verdiğini belirtmiştir. Bir diğer deyişle, kanun mevcuttur, fakat açık değildir, bu nedenle de keyfiliğe sebep olabilecek niteliktedir[1273].

3.2.13.2. Tedbir Kapsamındaki Şüpheli veya Sanık Hakkında Tesadüfen Elde Edilen Delillerin durumu

3.2.13.2.1. Katalog Suçlar Bakımından

İletişimin denetlenmesi tedbirin uygulanması sırasında tesadüfen elde edilen delil kavramından , yapılan soruşturma ile ilgisi bulunmayan ve soruşturma yapılırken bir başka suçun işlendiğini gösteren ve soruşturma yapılırken ele geçirilen delillerin anlaşılması gerekir[1274]. CMK'nın 138. maddesi, tesadüfi delilerin durumu hakkında bir düzenleme getirmiştir. Buna göre, arama ve elkoyma sırasında, arama ve elkoyma kararına konu olan suç dışında bir başka suçun işlendiğini gösteren bir delil elde edilmişse, CMK'nın 138/1. maddesine göre bu delilin değerlendirilmesi mümkündür. Buna karşılık aynı maddenin iletişimin denetlenmesinden elde edilen tesadüfi delilerin durumunu düzenleyen ikinci fıkrasında, bu delillerin yalnızca katalog suçlar bakımından değerlendirileceği düzenlenmiştir. Görüldüğü üzere, arama ve elkoyma neticesinde elde edilen tesadüfi deliller sınırsız olarak kullanılabilirken, iletişimin denetlenmesi tedbiri kapsamında elde edilen tesadüfi deliller ancak CMK'nın 135/6. maddesinde yer alan katalog suçlar bakımından delil olarak kullanılabilecektir[1275]. Başka bir ifadeyle, tedbir esnasında katalog suçlardan herhangi birinin işlendiği şüphesini uyandıracak bir delil elde edildiğinde, bu delil muhafaza altına alınacak ve durum savcılığa bildirilecektir. Katalog suçlar dışında herhangi bir suçun irtikap edilmesi

---

[1273] YENİSEY /ALTUNÇ, s.25; ERGÜL Ozan: "Yargıdan Telefon Dinlemeye Yeni Bir Yorum", www. yasayan Anayasa.ankara.edu.tr/docs/analizler/telefon_dinleme.pdf, (14.03.2007)).

[1274] ERDEM,s.107.

[1275] ÖZTÜRK/ERDEM, s.611-612; ; ÜNVER/HAKERİ, s. 187.

halinde ise, bu suç zimmet, irtikap, hırsızlık gibi bir suç olsa dahi bu delile dayanarak soruşturma başlatmak mümkün olmayacaktır[1276].

İletişimin denetlenmesi tedbirinin uygulanması sırasında, bir başka suçla ilgili olarak elde edilmiş olan bilgilerin değerlendirilip değerlendirilemeyeceği konusunda 4422 sayılı Kanunda açık bir düzenlemeye yer verilmemişti. Buna karşılık, bu hususu düzenleyen CMK'nın 138/2. maddesi, yapılmakta olan soruşturma veya kovuşturmayla ilgisi olmayan ve ancak CMK'nın 135/6. maddesinde sayılan katalog suçlardan birinin işlendiği şüphesini uyandırabilecek bir delilin elde edilmesi durumunda; bu delil muhafaza altına alınacağını ve durumun Cumhuriyet Savcılığına derhal bildirileceğini belirtmektedir. Bu itibarla, tesadüfen elde edilen delillerin soruşturma veya kovuşturma aşamasında kullanılabilir hale gelebilmesi için, öncelikle yapılmakta olan soruşturma veya kovuşturma ile ilgili olmaması gerekmektedir. Bu konudaki diğer şart da, elde edilen bilgilerin CMK'nın 135/6. maddesinde belirtilen katalog suçlardan birinin işlendiği şüphesini uyandırabilecek nitelikte olmasıdır. Aksi takdirde elde edilen delil niteliğindeki kayıtlar derhal yok edilmelidir[1277].

Bu yaklaşım ABD hukukunda da benimsenmiştir. ABD hukukuna göre, iletişimin dinlenmesi esnasında mahkeme kararında belirtilen sınırların aşılmaması bakımından elden gelen gayret gösterilmeli, bu bağlamda mahkeme kararında isimleri belirtilen kişilerin, sadece karar konusu suçlardan dolayı dinlenmeleri sağlanmalıdır. Diğer bir ifadeyle, bu kişilerin kararda belirtilmeyen suçları işlemeleri durumunda, kararda değinilmeyen suçlardan dolayı dinlemeye alınmalarının önlenmesi gerekmektedir[1278].

3.2.13.2.2. Katalog Dışı Suçlar Bakımından

Türk hukukunda, tesadüfen elde edilen deliller, ancak CMK'nın 135/6. maddesinde belirtilen katalog suçlardan birisine ilişkin ise, delil olarak değerlendirilebilir. CMK'nın 138. maddesinde CMK'nın 135/6. maddesinde sayılan suçlar dışında kalan suçlar açısından bir düzenlemeye

---

[1276] ŞAHİN, Cumhur; Ceza Muhakemesi Hukuku, C:I,(Ceza Muhakemesi Hukuku) Seçkin Yayınları, Ankara, 2007, s.270-271

[1277] ÖZBEK, s. 435-436; ERDEM, s.107; TURHAN, s. 273; KUNTER/YENİSEY/NUHOĞLU, s. 710. CENTEL/ZAFER, s. 366, ŞAHİN, s. 387.

[1278] 'Every order and extension … shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter…' (18 U.S.C. § 2518(5)); Bununla birlikte, hakkında iletişimin denetlenmesi kararı verilmiş kişi dışındaki herhangi biri hakkında suçlayıcı ifade ve bilgilerin takip esnasında ortaya çıkması halinde bu bilgilerin yargılamada kullanılabileceğini kabul eden birçok karar bulunmaktadır. Yüksek Mahkeme, bu bağlamda, çıkarılması istenen mahkeme kararı için yapılan başvurudaki şekil şartlarını daha esnek yorumlamaktadır. Hakkında dinleme kararı aldırılacak muhtemel kişilerin kimliği bilinmediği takdirde, 'diğerleri, ya da henüz bilinmiyor' kaydı düşülebilmektedir. Usulune göre alınmış bir mahkeme kararı ile yapılan dinleme sırasında başka bir suçla ilgili olarak elde edilen bilgiler de delil olarak kabul edilmektedir.(AN OVERVIEW OF ELECTRONIC SURVEILLANCE: History and Current Status).

yer verilmemiş ise de; maddenin lafzi yorumundan, tesadüfen elde edilmiş olan delillerden, katalog dışı suçların aydınlatılması amacıyla yararlanılamayacağı sonucu çıkmaktadır. CMK'nın 135. maddesi kapsamında bir suçtan dolayı tedbire başvurulması sonucu başka bir suçla ilgili olarak elde edilen bilgilerin her hangi bir ayırım yapılmaksızın delil olarak değerlendirilmesi tedbirin kötüye kullanılmasına yolunu açacaktır. Bu da, tedbirin ancak katalogda tek tek sayılmak suretiyle gösterilen belirli nitelikteki suçlar bakımından uygulanabileceği yönündeki kanuni güvencenin ortadan kaldırılması anlamına gelecektir[1279].

Uygulama ve öğretide, yer yer, katalog harici suçlarla ilgili olarak elde edilen bilgilerin kullanılması gerektiği ifade edilse de böyle bir uygulama haberleşme özgürlüğünün özüne müdahale anlamına geldiği açıktır[1280].

Aynı görüşte olan, Yargıtay CGK, 13.06.2006 tarih ve 2006/162 K. sayılı kararında, tesadüfen elde edilen bilgilerin CMK m. 135'teki katalog suçlardan biri hakkında değil, fakat katalogda yer almayan "görevde yetkiyi kötüye kullanma" suçuna ilişkin olması gerekçesiyle yasa dışı olduğunu ve bu nedenle "dışlanması" gerektiğini ifade etmiştir[1281]. Biz de Yargıtay'ın bu görüşünün isabetli olduğunu düşünmekteyiz. Aksinin kabulü, ancak özel durumlar için öngörülmüş bu tedbirin genel bir niteliğe bürünmesi anlamına gelecektir. Oysa ki kanun koyucu, karşılaştırmalı hukukta da olduğu gibi, hürriyetin özüne müdahale anlamına gelen bu tedbiri dar bir alana hasretmeyi yeğlemiş ve katalog suçu düzenlemesini getirmiştir.

Nasıl ki, Cumhuriyet savcısı, bir soruşturma kapsamında, şüphelinin sahte belge hazırlayarak diploma aldığını ve avukatlık yaptığını öğrenmesi durumunda sahte belge hazırlamak suçundan ilgilinin iletişimin dinlenmesine karar veremeyecek ise, başka bir suçla ilgili verilen dinleme kararının uygulaması sırasında bu suçla ilgili elde edilen bilgilerin delil olarak kullanılması da rasyonel değildir. Bu itibarla, Kanundaki düzenlemenin yerinde olduğunu düşünmekteyiz[1282].

3.2.13.2.3. Tesadüfen Elde edilen Delillerin Delil Başlangıcı Olarak Değerlendirilmesi

İletişimin denetlenmesi tedbirinin uygulanması kapsamında elde edilen tesadüfi deliller katalog dışı suçlar bakımından kullanılamasa da, bunlara vakıf olan kamu görevlisinin bir

---

[1279] ÖZTÜRK/ERDEM, s.611-612; ÖZBEK, s. 436; TURHAN, s. 273.

[1280] ÖZTÜRK-ERDEM, s. 612.

[1281] YENISEY-ALTUNÇ, s. 26.

[1282] TAŞKIN, s. 178.

suçun varlığını tespit etmesi durumunda ilgili makamlara bildirme yükümlülüğü bulunmaktadır. Gerekli bildirim yapıldıktan sonra gerekli soruşturma ve delil elde etme işlemleri diğer yasal yollar kullanılarak yapılacaktır[1283]. Bu kapsamda, usulüne uygun olarak verilmiş olan iletişimin denetlenmesi kararı çerçevesinde, soruşturma mecburiyeti ilkesinin de doğal sonucu olarak, şüpheli, sanık veya üçüncü bir kişinin denetim kapsamı dışında kalan katalog dışı suçlardan birini işledikleri öğrenildiğinde, bu tür bilgilerin, ortaya çıkan yeni suçtan dolayı soruşturma yapılması ve araştırma yürütülmesinde yol gösterici olarak değerlendirilmesi gerektiğini düşünmekteyiz[1284].

Hakkında iletişimin denetlenmesi kararı verilen kişi veya denetim kapsamındaki suç ile ilgisi olmayan üçüncü bir kişinin hırsızlık, dolandırıcılık, yağma, zimmet, irtikap gibi toplum vicdanını derinden rahatsız eden ve kamu düzenini tehdit eden suçlardan birini işlemiş olduğuna ilişkin bilgiler edinildiğinde, bu suçlar sebebiyle soruşturma başlatılabilmesi, suçla ve suçluyla etkin mücadele bakımından yerinde olacaktır[1285]. Alman hukuku, hukuka aykırı olarak elde edilen "tesadüfi bilgiler"in, duruşmada delil olarak kullanılamasa bile, "şüphe sebebi" olarak hazırlık soruşturması açısından değerlendirilmesini kabul etmektedir. Ancak, Türk Hukukunda Anayasa'nın 38. maddesinde "kanuna aykırı bulgu" tanımı içinde, bu görüşün benimsenmesi mevcut durum itibariyle mümkün değildir[1286].

[1283] ÜNVER/HAKERİ, s.187;ÖZBEK, s.435.

[1284]Yargıtay Ceza Genel Kurulu'nun 13.06.2006 tarih ve 2006/162 K. Sayılı kararına karşıoy yazan Yargıtay Üyesi Ali Suat Ertosun, 'Dava konusu olayda, şüpheli H.S.Ş. için usulüne uygun şekilde dinleme kararı alınmıştır. Adı geçen bu şüphelinin telefonundan başka birisinin konuşması sırasında yapılan tespitler, konuşan ve karşıdaki kişi yönünden yasak delil niteliğinde olmayıp, tesadüfen elde edilen delil niteliğindedir (CMK.nun 138/2. maddesi). İletişimin denetlenmesi sırasında, yapılmakta olan soruşturma ile ilgisi olmayan ve CMK.nun 135/6. maddesinde sayılan (katalog) suçlar dışında kalan bir suçla ilgili kayıt alınmıştır. Elde edilen bilgiler, ihbar kabul edilerek soruşturma yapılabilecek ve delil başlangıcı olarak kullanılabilecektir. Zira hâkim kararı ile kişinin özel alanına girildiğinden, haksız ve keyfî değil, yasaya uygun bir müdahale söz konusudur. Yasanın bu düzenlemesi karşısında, dinlenmesine karar verilen kişilerle sınırlı delil elde edilebileceği ve kullanılabileceği düşüncesi kabul edilemez. Bir hâkim tarafından karar verildiği için dinleme tamamen yasaldır. Resmî olarak kendisi dinlenmeyen bir kişinin söyledikleri, hatta bir suç itirafı kullanılabilir. Önemli olan kanıt araştırmasındaki doğruluktur ve bunların kötüye kullanılmamasıdır.'şeklindeki beyanıyla benzer bir düşünceye tercüman olmaktadır. Ertosun, buna gerekçe olarak da, sosyal ve ekonomik gelişme ve değişimler karşısında, özel bir önem kazanan ve toplum güvenliğini tehdit eden örgütlü(terör ve çıkar amaçlı) suçlar ve suçlularla mücadelede, telekomünikasyon yoluyla yapılan iletişimin denetlenmesinin önemine ve toplum yararına vurgu yapmaktadır. (CGK, 2006/4.MD-122 E., 2006/162 K., 13.06.2006)

[1285] KUNTER/YENİSEY/NUHOĞLU, s. 710; Karşılaştırmalı hukukta, tedbirin uygulanması sırasında bir başka suçla ilgili olarak elde edilmiş olan bilgilerin delil olarak kullanılmasına ancak sınırlı bir çerçevede olanak tanınmaktadır. Bu kapsamda, Alman CMK § 100b V uyarınca iletişimin denetlenmesi sonucu elde edilen bilgiler, bir başka ceza muhakemesinde, § 100a'da öngörülen suçlardan birisinin aydınlatılması amacıyla delil olarak değerlendirilebilmektedir (ERDEM, S.107; ÜNVER/HAKERİ, S.187).

[1286]YENİSEY, Feridun /ALTUNÇ, Sinan:CMK 135 Hakkında, http://www. hukukturk.com /fractal/ hukuk Turk/ pages/fHm.jsp, s. 30.

3.3. Türk Hukukunda Önleme Amaçlı İletişimin Denetlenmesi

İletişim araçlarının ve hatta insanların karşılıklı konuşmalarının istihbarat amacıyla gizlice dinlenmesi ve kaydedilmesi mukayeseli hukukta düzenlenmiştir[1287]. Yapılan son yasal düzenlemeler öncesinde, 4422 sayılı Kanun kapsamında, önleme amaçlı iletişimin denetlenmesi yapılmakla birlikte, anılan Kanun sadece adli amaçlı dinleme ve kayda almaya izin verdiği için, yapılan önleme amaçlı dinleme ve tespitler hukuka aykırı olarak kabul edilmekteydi[1288]. Bu eksikliği gören TBMM, önleme amaçlı iletişimin denetlenmesi hususundaki boşluğu doldurabilmek amacıyla yaptığı hazırlık çalışmalarında, bu konudaki diğer ülke mevzuatlarını incelemiş ve bu tedbirin adli amaçlı iletişimin denetlenmesi tedbirinden ayrı bir yasal düzenlemeye kavuşturulmasının yararlı olacağı sonucuna varmıştır[1289].

5397 sayılı Kanun öncesi dönemde önleme amaçlı iletişimin denetlenmesi tedbiri herhangi bir yasal dayanak olmaksızın gerçekleştirilmekteydi. 4422 sayılı Kanunun, 5320 sayılı Ceza Muhakemesinin Yürürlük ve Uygulama Şekli Hakkında Kanun[1290] ile 1 Haziran 2005 tarihi itibariyle yürürlükten kaldırılması önleme amaçlı iletişimin denetlenmesi alanındaki boşluğun tamamen ortaya çıkmasına hizmet etmiştir.

5397 sayılı Kanunla, 2559 sayılı Polis Vazife ve Salahiyetleri Kanununa (Ek 7. madde), 2803 sayılı Jandarma Teşkilatı, Görev ve Yetkileri Kanunu'na(ek 5. maddesi) ve 2937 sayılı Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanunu'na (6.maddesinin birinci fıkrasında yapılan değişiklik ve sonra gelmek üzere eklenen fıkralar) önleme amaçlı dinleme, tespit ve kayda almaya ilişkin düzenlemeler eklenmiştir[1291]. Kanun, gerek ulusal gerekse uluslararası esas ve standartlara uyulmak şartıyla, istihbarat ihtiyaçlarını karşılamak için meydana getirilmiştir. Kanunda, önleme amaçlı iletişimin denetlenmesi kapsamındaki hukuka uygun işlemlerin ne suretle gerçekleştirileceği, kararların hangi makamlar tarafından ve ne gibi koşullara uyulması suretiyle alınacağı, bu hususstaki denetim kuralları ve usulleri belirlenmiştir. Kanun bir taraftan çok önemli

---

[1287] Adli ve önleme amaçlı iletişimin denetlenmesi ayrımı Fransız hukukunda da vardır. Önleme amaçlı iletişimin denetlenmesi 10 Temmuz 1991 tarihli Posta ve Telekomünikasyon Kanununa göre yapılmaktadır. (TAŞKIN, s. 64).

[1288] ŞEN, (İletişimin Denetlenmesi Tedbiri), s. 101.

[1289] Bk. 'İnsan Haklarını İnceleme Komisyonu'nun 7 haziran 2001 Tarihli 15. Toplantısında Telefon Dinleme ve Bu Yolla Elde Edilen Kayıt ve Bilgilerin Medyada Yer Alması Üzerine Gündeme Getirilen Usulsüz Telefon Dinleme Konusunu Araştırmak Amacıyla 14 Haziran 2001 Tarihinde Kurulan Alt Komisyon Raporu'.

[1290] R.G., 31.3.2005, S: 25772.

[1291] ŞEN, (İletişimin Denetlenmesi Tedbiri), s. 101.

bir yasal boşluğu doldurmuş, öte yandan da AİHS'nin 8. maddesinde koruma altına alınan haberleşme özgürlüğünün sınırlandırılmasına ilişkin şartları belirlemiştir. Böylece, yetkilerin denetimsiz ve kontrolsüz olarak kötüye kullanılmasının önlenmesi amaçlanmıştır[1292].

Bu işlemlerin tek merkezden yürütülmesi amacıyla TİB kurulmuştur. TİB, önleyici denetleme anlamında sadece bir uygulama ve yürütme makamı olarak görev yapmaktadır.

3.3.1. Kavram

Türk hukukunda 5397 sayılı Kanunun kabul edilmesinden önce önleme amaçlı olarak iletişimin denetlenmesine imkan veren açık ve uygulama şartlarını gösteren yasal bir düzenleme bulunmamaktaydı. Her ne kadar, Polis Vazife ve Salahiyet Kanunu'nun Ek 7. maddesinde "Polis, Devletin ülkesi ve milletiyle bölünmez bütünlüğüne, Anayasa düzenine ve genel güvenliğine dair önleyici ve koruyucu tedbirleri almak, emniyet ve asayişi sağlamak üzere, ülke seviyesinde istihbarat faaliyetlerinde bulunur, bu amaçla bilgi toplar, değerlendirir, yetkili mercilere veya kullanma alanına ulaştırır. Devletin diğer istihbarat kuruluşlarıyla işbirliği yapar." hükmüne yer verilmiş olsa da bu düzenleme, "önleme amaçlı iletişimin denetlenmesi" kavramını açıklamaya, amaç ve kapsamını belirlemeye yeterli değildi. Gerçekten de, bu düzenleme, tedbir uygulanması bakımından gerekli olan "açıklık, netlik ve denetim prosedüründen" yoksun bulunmaktaydı.

Türk hukukunda, mülga 4422 sayılı Kanundaki iletişimin denetlenmesi tedbirine ilişkin düzenlemelerin ardından 1 Haziran 2005 tarihinde yürürlüğe giren 5271 sayılı CMK'nın 135. maddesi ile adli amaçlı iletişimin denetlenmesine imkan verilmiştir. Buradaki düzenleme uyarınca, bir suç dolayısıyla yapılan soruşturma ve kovuşturmada, suç işlendiğine ilişkin kuvvetli şüphe sebeplerinin varlığı ve başka suretle delil elde edilmesi imkânının bulunmaması durumunda, hâkim veya gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısının kararıyla iletişimin denetim altına alınabilmesi mümkün hale gelmişti. CMK'nın bu düzenlemesi yalnızca adli amaçlı iletişimin denetlenmesine yönelikti. İletişimin denetlenmesi tedbirine suçun önlenmesi amacıyla da ihtiyaç duyulması nedeniyle, Anayasa'nın haberleşme hürriyetini düzenleyen 22. maddesi hükmü de dikkate alınarak bu kanun hazırlanmıştır. Anayasa'nın bu hükmü ve çağın

[1292] TAŞKIN, s. 62.

zorunlu gerekleri de göz önüne alınarak hazırlanan bu kanun, önleme amaçlı olmak şartıyla ve hakim kararıyla kolluğa iletişimin denetlenmesi imkanı verilmiştir[1293].

3.3.2.Kapsam

Adli amaçlı olarak telekomünikasyon yoluyla iletişimin denetlenmesi tedbiri, işlenmiş olan bir suçla ilgili olarak delil elde etme amacına hasredilmişken, önleme amaçlı iletişimin denetlenmesi ise, suçun henüz işlenmediği ancak işlenebileceğine dair şüphelerin varolduğu hallerde başvurulacak bir tedbirdir. Bu tedbire başvurulabilmesi için, yakın bir tehlike ihtimali ya da suçun önlenmesi amacı olmalıdır. Nitekim, suç veya tehlike gerçekleştikten sonra ancak adli amaçlı iletişimin denetlenmesi yoluna gidilebilecektir[1294].

Önleme amaçlı iletişimin denetlenmesi tedbirinin uygulanmasından önce, ortada işlenmiş bir suç bulunmadığı gibi, bir suçlu veya suç delilinin de bulunması söz konusu değildir. Tedbir gayri muayyen kişilere yönelik olabileceği gibi dikkat çeken zararlı unsurlara veya "hedef" olarak tabir edilen kişilere karşı da olabilir. Burada henüz işlenmiş bir suçtan ziyade, işlenme ihtimali yüksek olan bir suç söz konusudur[1295]. Bu önlemde temel amaç, delil elde etmekten ziyade bu suçların önlenmesidir.

Uluslararası sözleşmeler ve Anayasa'da yer alan düzenlemelerle güvence altına alınan temel bireysel hürriyetlerden olan haberleşme hürriyetine ciddi bir müdahale niteliği taşıyan önleme amaçlı iletişimin denetlenmesi tedbiri, getirilen yasal düzenlemelerle belirli sınırlamalar ve şartlara tabi tutulmuştur. 5397 sayılı Kanunun tedbirin kapsamı ve sınırlarına ilişkin getirdiği düzenleme uyarınca her bir kolluk birimi, kendi görev alanlarıyla sınırlı kalmak şartıyla 5271 sayılı Ceza Muhakemesi Kanununun, casusluk suçları hariç olmak üzere, 250. maddesinin birinci fıkrasında yer alan suçlar bakımından önleme amaçlı iletişimin denetlenmesi yapabilir. Kolluk birimleri; örgüt faaliyeti çerçevesinde işlenen uyuşturucu veya uyarıcı madde imal ve ticareti suçu, haksız ekonomik çıkar sağlamak amacıyla kurulmuş bir örgütün faaliyeti çerçevesinde cebir ve tehdit uygulanarak işlenen suçlar ile 5237 sayılı TCK'nın ikinci kitap dördüncü kısmın dört, beş, altı ve yedinci bölümünde yer alan devlete ve millete karşı işlenmiş suçlarla ilgili olarak önleme amaçlı bu tedbire başvurmayı talep edebilecektir. Milli İstihbarat Teşkilatı ise, 2937 sayılı Devlet İstihbarat Hizmetleri ve Millî İstihbarat

[1293] KAYA, (İletişimin Dinlenmesi), s.12.

[1294] KUNTER/YENİSEY/NUHOĞLU, s. 716.

[1295] ÇOLAK/TAŞKIN, s. 617-618.

Teşkilatı Kanununun 4. maddesinde sayılan görevlerin yerine getirilmesi amacıyla Anayasa'nın 2. maddesinde belirtilen temel niteliklere ve demokratik hukuk devletine yönelik ciddi bir tehlikenin varlığı halinde devlet güvenliğinin sağlanması, casusluk faaliyetlerinin ortaya çıkarılması, devlet sırrının ifşasının tespiti ve terörist faaliyetlerin önlenmesi amacıyla bu tedbire başvurulmasını yetkili ve görevli makamdan talep edebilecektir.

Önleme amaçlı iletişimin denetlenmesi düzenlenirken kanun koyucu olabildiğince geniş sınırlar çizmiş, adli amaçlı iletişimin denetlenmesi tedbirinde var olan birtakım hukuksal sınırlamalara yer vermemiştir. Gerçekten de, adli amaçlı iletişimin denetlenmesi tedbirinde, tanıklıktan çekinme hakkı olan kişiler ve müdafi bakımından birtakım sınırlamalar getirilmesine karşın, önleme amacıyla yapılan iletişimin denetlenmesi tedbirinin uygulanacağı kişilerle ilgili herhangi bir sınırlama bulunmamaktadır.

Önleme amaçlı iletişimin denetlenmesine ilişkin olarak 5397 sayılı Kanunla getirilen düzenlemede, dört tür iletişimin denetlenmesi işlemi sayılmaktadır. Bunlar iletişimin tespiti, iletişimin dinlenilmesi, iletişimin kaydedilmesi ve iletişimin sinyal bilgilerinin değerlendirilmesi işlemleridir. 5397 sayılı Kanunda, önleme amaçlı iletişimin denetlenmesi tedbirleri arasında mobil telefonu yerinin tespiti tedbirine yer verilmemiştir. Aslında yer tespiti sinyal bilgilerinin değerlendirilmesi işlemleri arasındadır. Bu yönüyle istihbarat birimleri de gerektiğinde bu yöntemi hakim kararı almak suretiyle kullanabilmektedirler. Zaten CMK'da mobil telefonun yerinin tespiti tedbiri şüpheli veya sanığın yakalanması amacıyla kullanılabiliyordu. Burada ortada işlenmiş bir suç ve kaçan bir şüpheli veya sanık olmadığından bu tedbir metne alınmamıştır.

Suç işlenmesinin önlenmesi amacıyla iletişimin denetlenmesi tedbirinin dışında diğer bazı bilgilere ihtiyaç duyulabilmektedir. Bu bağlamda değerlendirilen diğer iletişim bilgileri ya da iletişim detay bilgileri olarak adlandırabileceğimiz bilgiler yukarıda adli amaçlı iletişimin denetlenmesi bölümünde belirtildiğinden ayrıca sayılmamıştır.

3.3.3. Önleme Amaçlı İletişimin Denetlenmesinin Koşulları

3.3.3.1. CMK'nın 250/1. Maddesinde Belirtilen Suçlardan Birinin Bulunması

3.3.3.1.1 Genel Olarak

Önleme amaçlı iletişimin denetim altına alınması, CMK'nın 250/1. maddesinde belirtilen suçların işlenmesinin önlenmesi amacıyla başvurulacak bir tedbirdir. Bu madde, CMK'nın

”Bazı Suçlara İlişkin Muhakeme” başlığını taşıyan dördüncü bölümünde özel yargılama usulüne tabi suçları ve bu suçlara bakacak görevli ve yetkili yargı merciini ve yargı çevresini düzenlemektedir. Maddede belirtilen suçlar ağır nitelikteki suçları ve bireysel olmaktan ziyade bir örgüt kapsamında işlenenleri kapsamaktadır. Buradaki örgüt, ekonomik çıkar sağlamak amacıyla kurulmuş olabileceği gibi ülkenin birliğini, bütünlüğünü, Anayasal düzenini ve huzurunu bozmak amaçlı kurulmuş olan suç birliklerini de kapsamaktadır. Temel bireysel hürriyetlerden olan haberleşme hürriyetine ciddi bir müdahale niteliği taşıyan önleme amaçlı iletişimin denetlenmesi tedbirine başvurulabilmesi için, öncelikle bu maddede belirtilen ve ülke bütünlüğü ve toplum düzenine karşı ciddi manada tehlike oluşturan bu suçların mevcut olması zorunludur. CMK’nın 250/1-c maddesinde belirtilen suçların bireysel olarak da işlenebilen suçlar olması sebebi ile bu suçların önlenmesi için örgütün bulunması zorunlu değildir.

Tedbir kapsamındaki bu suçlar tespit edilmek suretiyle önleme amaçlı iletişimin tespiti, dinlenmesi, kaydedilmesi ve sinyal bilgilerinin değerlendirilmesi yollarına başvurulabilmektedir. Bunların dışındaki suçlarla ilgili olarak bu tedbire başvurulması mümkün değildir. Temel hakları sınırlayıcı kıyas mümkün olamadığından, tedbir kapsamındaki suçların bu yolla çoğaltılması mümkün değildir. Bu sebeple, kapsam dışında kalan diğer suçlarda iletişimin denetlenmesi tedbirine başvurulması hukuka aykırı olacaktır.

Önleme amaçlı iletişimin denetlenmesine konu olan suçların tespiti bakımından katalog belirlenmesinin yararlı olup olmayacağı tartışma konusudur. Yukarıda bir kısmı belirtilebilen geniş bir suç listesi bakımından bu tedbire başvurulabilmesi, başka bir deyişle, geniş ve soyut nitelikteki bir suç listesinin öngörülmüş olması temel haklara bu denli müdahaleyi öngören bir tedbiri tartışmalı hale getirmektedir[1296]. Gerçekten de, iletişimin denetlenmesi tedbiri kişinin özel hayatı bakımından ciddi tehlikeler içermekte, diğer bazı koruma tedbirlerinden farklı olarak devamlılık arz etmekte, sadece belli bir alandaki delillerin değil iletişimin her türlü kapsamının tedbir kapsamına girmesi gibi sakıncalar taşımaktadır. Örneğin, arama tedbiri kısa bir zaman diliminde yapılmakta, tedbir sonucunda kişinin özel hayatına olan müdahale sona ermektedir. Oysa ki, iletişimin denetlenmesi tedbiri çok daha uzun bir zaman dilimi boyunca sürebilmekte, denetleme ile gelişigüzel bilgiler elde edilebilmekte, bu bilgileri tedbir konusu suç bakımından da ayıklamak mümkün bulunmamaktadır. Bu bağlamda, özel hayata bu

[1296] ŞEN, (İletişimin Denetlenmesi Tedbiri), s. 101.

denli müdahaleyi kapsayan bu tedbirin adli amaçlı iletişimin denetlenmesinde olduğu gibi bir kataloga tabi tutulmasının gerekli olduğunu kanaatindeyiz.

İletişimin denetlenmesi tedbirine karar verilirken dikkat edilmesi gereken husus, öncelikle örgüt kapsamındaki suçlar bakımından örgütün varlığının saptanması durumudur. Adli amaçlı iletişimin denetlenmesinde ortada işlenmiş bir suça ilişkin kuvvetli şüphe sebeplerinin varlığı ve başka suretle delil elde edilmesi imkânının bulunmaması durumunda başvurulurken, önleme amaçlı iletişimin denetlenmesine katalogda yer alan suçların önlenmesi amacıyla başvurulmaktadır. Bu sebeple, önlenmesi istenen suçlara ilişkin nitelendirmeye yardımcı olacak ve delil başlangıcı niteliğindeki bilgi ve belgeler çok önemlidir. Çünkü bu bilgi ve belgeler suçun vasıflandırılması açısından hayati önem taşımaktadır. Örgüt suçu olduğuna dair yeterli şüphe bulunmamasına rağmen, bu tedbirle kolayca sonuca ulaşabilmek amacıyla bu yönde talepte bulunabileceği ihtimali dikkate alınarak, hakimin, önleme amaçlı iletişimin denetlenmesine karar verirken suçun vasıflandırılmasına dayanak olarak gösterilen bilgi ve belgeleri özenle değerlendirmesi gerekmektedir. Bu suçların işlenebileceğine dair makul ve yeterli bilgi ve belgenin bulunmaması veya suçun vasfının yanlış olarak belirlendiği durumlarda talep reddedilmelidir. Nitekim, bu tedbirin uygulanması neticesinde, tedbirin amacından uzak sonuçların ortaya çıkması halinde orantılılık ilkesinin de ihlali söz konusu olacaktır.

Adli amaçlı iletişimin denetlenmesi tedbirinde son çare ilkesine yer verilmişken, önleme amaçlı iletişimin denetlenmesinde durum farklıdır. Kanunda belirlenen suçların işlenmesi başka yollarla önlenebilecek olsa dahi, bu suçların işlenmesinin önlenmesi amacıyla iletişimin denetlenmesi yoluna gidilebilir. Bir suçun işlenmesinin önlenmesi amacıyla belirli saatlerde polisin devriye gezmesinin yeterli olacağı durumlarda bile iletişimin denetlenmesi tedbiri uygulanabilecektir. Düzenleme bu ilke yönünden de büyük eksiklik içermektedir[1297]. Gerek AİHM gerekse hukukumuzda kabul edilen orantılılık ilkesi gereği, bireysel özgürlüklere daha az müdahale eden tedbirlerin tercih edilmesi zorunluluğu olmasına rağmen, uygulamada bu hususa uyulduğu pek söylenemez. Örneğin, önleme amaçlı iletişimin denetlenmesi taleplerinde, alınabilecek tedbirlerinin tümünün talep edildiği görülmektedir. Başka bir anlatımla; iletişimin dinlenmesi, izlenmesi, tespit edilmesi, sinyal bilgilerinin değerlendirilmesi, kayda alınması, hedef şahsın ses ve görüntülerinin teknik cihazlarla kaydedilmesi birlikte talep edilmektedir. Oysa ki, bunların arasından en elverişlisinin ve özel hayata en az

[1297] TAŞKIN, s.206.

müdahale edenin belirlenmesi ve ona karar verilmesi tercih edilmelidir[1298]. Böylece hürriyetlere gerektiği kadar ve daha uygun olan yöntemle müdahale edilmiş olacaktır.

Son çare şartının aranmaması sadece ülkemize münhasır bir uygulama değildir. ABD'de de, FISA'ya göre yapılan dinlemelerde son çare prensibinin varlığı, mahkeme tarafından araştırılmamaktadır. Diğer tedbirlere başvurulmasının sonuçsuz, yararsız ya da tehlikeli olduğunu ifade eden hükümet yetkilileri, anılan hususları teyit eden bir sertifikayı ibraz ettiklerinde bu şartın gereğinin yerine getirldiği kabul edilmektedir[1299]. Bununla birlikte, FISA çerçevesinde bir mahkeme kararı verilebilmesi için gerekli olan ve en aza indirgeme ilkesi (minimization procedures)[1300] olarak adlandırılan kurala riayet edilmesi gerekmektedir[1301]. En aza indirgeme ilkesinin temelinde, iletişimin denetlenmesi tedbirinin hürriyetin özüne dokunması tehlikesini en aza indirgeme çabası vardır. Nitekim, iletişimin denetlenmesi, fiziksel arama ve elkoymaya kıyasla özel hayatı daha fazla tehdit eden bir nitelik arz etmektedir.Diğer tedbirler daha kısa bir zaman diliminde gerçekleştirilmekte iken, iletişimin denetlenmesi doğası itibariyle belli bir zamana yayılmaktadır. Ortaya çıkması muhtemel diğer bir sakınca ise müdahale esnasında denetlemenin amacıyla ilgisi olmayan konuların da takibe takılabilmesidir[1302] En aza indirgenmesi kuralına uyulmaması, elde edilen bilgilerin delil sıfatını kazanamaması gibi bir handikap doğurabileceğinden dolayı önemlidir[1303]. Bu ilkenin hayata geçirilmesi ile, mahkeme kararında ismi geçmeyen kişilerin mümkün olabildiği ölçüde dinleme kapsamına alınmamasına riayet edilmesi mümkün olmaktadır. Bu ilke ile elde edilmek istenen bir diğer yarar da, mahkeme kararında isimleri belirtilen kişilerin, sadece karar konusu suçlardan dolayı dinlenmelerinin sağlanmasıdır. Diğer bir anlatımla, bu kişilerin kararda belirtilmeyen suçları işlemeleri durumunda, kararda değinilmeyen suçlardan dolayı dinlemeye alınmalarının önlenmesidir.

İletişimin denetlenmesi tedbirinin hassas mahiyeti dikkate alındığında son çare prensibinin uygulanması, kanaatimizce, suçla mücadele ile hakların korunması arasındaki dengenin muhafaza edilmesi bakımından önemlidir. Kanunda yapılacak

---

[1298] TAŞKIN, s. 206.

[1299] ÖZDOĞAN(2004), s. 100; DEMPSEY, "Communications Privacy In The Digital Age: Revitalizing The Federal Wiretap Laws To Enhance Privacy".

[1300] 50 U.S.C. § 1805 (a)(4).

[1301] WONG,3.4.8; DONOHUE, s. 14-15; STEVENS/DOYLE, s. 48-50.

[1302] AN OVERVIEW OF ELECTRONIC SURVEILLANCE: History and Current Status, D.1.2; SCHWARTZ, A.1.

[1303] AN OVERVIEW OF ELECTRONIC SURVEILLANCE: History and Current Status, D.1.2.

revizyon sonucunda, katalog suçu kriterinin yanısıra bu ilkenin de uygulanması şartının getirilmesi yararlı olacaktır.

3.4.3.1.2. Tedbir Kapsamındaki Suçlar

5397 sayıl Kanun uyarınca yargılaması CMK'nın 250. maddesine göre yapılan ve Türk Ceza Kanununda yer alan aşağıdaki suçlar, iletişimin önleme amaçlı denetlenmesi tedbirinin kapsamındadırlar. Buna göre ;

a. Örgüt faaliyeti çerçevesinde işlenen uyuşturucu veya uyarıcı madde imal ve ticareti suçu,
b. Haksız ekonomik çıkar sağlamak amacıyla kurulmuş bir örgütün faaliyeti çerçevesinde cebir ve tehdit uygulanarak işlenen suçlar[1304]
c. Devletin Güvenliğine Karşı Suçlar

1.Devletin birliğini ve ülke bütünlüğünü bozmak (TCK md.302)

2. Düşmanla işbirliği yapmak (TCK md.303)

3. Devlete karşı savaşa tahrik(TCK md.304)

4. Yabancı devlet aleyhine asker toplama (TCK md.306)

5. Askeri tesisleri tahrip ve düşman askerî hareketleri yararına anlaşma(TCK md.307)

6. Düşman devlete maddî ve malî yardım(TCK md.308)

d. Anayasal Düzene ve Bu Düzenin İşleyişine Karşı Suçlar

1. Anayasa'yı ihlâl (TCK md.309)

2. Cumhurbaşkanına suikast ve fiilî saldırı (TCK md.310)

3. Yasama organına karşı suç (TCK md.311)

4. Hükümete karşı suç (TCK md.312)

5. Türkiye Cumhuriyeti Hükümetine karşı silâhlı isyan (TCK md.313)

[1304] Göçmen kaçakçılığı, kasten yaralama, insan ticareti, çocuk düşürtme, kısırlaştırma, tehdit, kasten öldürme, organ ve doku ticareti, şantaj, cebir, kişiyi hürriyetinden yoksun kılma, mala zarar vermenin nitelikli hâlleri, fuhuş, bilişim alanında suçlar, ihaleye fesat karıştırma gibi haksız ekonomik çıkar sağlama suçları arasında sayılabilir.

6. Silâhlı örgüt (TCK md.314)

7. Silâh sağlama (TCK md.315)

8. Suç için anlaşma (TCK md.316)

e. Millî Savunmaya Karşı Suçlar

1. Askerî komutanlıkların gaspı (TCK md.317)

2. Yabancı hizmetine asker yazma, yazılma (TCK md.320)

3. Savaş zamanında emirlere uymama (TCK md.321)

4. Savaş zamanında yükümlülükler (TCK md.322)

f. Devlet Sırlarına Karşı Suçlar ve Casusluk

1. Devletin güvenliğine ilişkin belgelerin kısmen veya tamamen yok edilmesi, tahrip edilmesi veya bunlar üzerinde sahtecilik yapılması veya geçici de olsa, bunları tahsis olundukları yerden başka bir yerde kullanılması, hileyle alınması veya çalınması suçu (TCK md.326)

2. Devletin güvenliğine ilişkin bilgileri temin etme (TCK md.327)

3. Siyasal veya askerî casusluk (TCK md.328)

4. Devletin güvenliğine ve siyasal yararlarına ilişkin bilgileri açıklama (TCK md.329)

5. Gizli kalması gereken bilgileri açıklama(TCK md.330)

6. Uluslararası casusluk(TCK md.331)

7.Devlet sırlarından yararlanma, Devlet hizmetlerinde sadakatsizlik(TCK md.333)

8. Yasaklanan bilgileri temin(TCK md.334)

9. Yasaklanan bilgilerin casusluk maksadıyla temini (TCK md.335)

10. Yasaklanan bilgileri açıklama (TCK md.336)

11. Yasaklanan bilgileri siyasal veya askerî casusluk maksadıyla açıklama (TCK md.337)

12. Taksir sonucu casusluk fiillerinin işlenmesi (TCK md.338)

13. Devlet güvenliği ile ilgili belgeleri elinde bulundurma (TCK md.339)

3.3.3.2. Suçların Önlenmesi Amacı

İletişimin denetlenmesi tedbirine, işlenmiş bir suçun soruşturulması dışında, suçun önlenmesi amacıyla da ihtiyaç duyulabilir[1305]. Suçun işleneceğine dair şüphelerin ve hazırlık hareketlerinin yer aldığı suç öncesi dönemin etkin bir şekilde kontrol edilebilmesi, suç işlenmesinin önlenmesi bakımından çok önemlidir.

Devletin iç ve dış güvenliğinin korunması, istihbarat hizmetlerinin düzenlenmesini zorunlu kılmaktadır. Gelişen zaman diliminde, topluma ve devlete gelebilecek tehlikelerin önceden sezilmesi ve bunların önlenmesi için tedbirler alınması demokratik hukuk devletinin korunması açısından kaçınılmaz bir zorunluluk haline gelmiştir. 5397 sayılı Kanunun gerekçesinde ifade edildiği üzere, Anayasa'yla koruma altına alınan özel hayat ve haberleşme hürriyetine, suç işlenmeden önce devlet tarafından yapılacak müdahalelerin, çağdaş hukukun standartlarına uygun olarak kanunla yapılması ve denetleme tedbirinin sebeplerinin bir kanunda gösterilmesi gerekmektedir. Hukukumuzda, önleme amaçlı iletişimin denetlenmesi imkanını veren 5397 sayılı kanunun temel amacı budur.

Milli güvenlik ve kamu düzenine yönelik terör odaklarının zamanlıca tespiti, bu örgütlerin taktik ve stratejilerinin önceden tespit edilmesi ve eyleme geçmelerinden önce engel olunması hayati önemi haizdir. İletişimin önleme amacıyla denetlenmesi, suç işlenmesinin ve yakın bir tehlikenin engellenmesi amacıyla başvurulacak bir tedbirdir. Buradaki, suç işlenmesinin ve yakın bir tehlikenin engellenmesinden amaç, ülkenin bütünlüğüne, Anayasal düzene, genel güvenliğe yönelik olan ve engellenmediği takdirde ülke ve toplum bütünlüğünün ciddi manada zarar görebileceği suç ve tehlikelerin engellenmesidir. Bu bağlamda, Anayasa'nın 22. maddesinde ifadesini bulan "Milli güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlakın korunması veya başkalarının hak ve hürriyetlerinin korunması sebeplerinden biri veya birkaçına bağlı olarak" iletişimin denetlenebileceği hükmü, bu tedbirin amacını belirlemektedir.

[1305] KARAYAZGAN, s.53.; ŞAHİN, Ceza Muhakemesi Hukuku, s.264

3.3.3.3. Makul Suç Şüphesinin Varlığının Aranması

Adli amaçlı iletişimin denetlenmesi tedbirinde açıklandığı gibi basit şüphe, fiilin suç olması ve soruşturalabilir nitelik arz etmesidir. Yeterli şüphe, eldeki delillere göre yapılacak muhakeme sonucunda sanığın mahkum olması ihtimalinin beraat etme ihtimaline göre daha kuvvetli olması halidir. Makul şüphe, hayatın akışına göre somut olaylar karşısında genellikle duyulan şüphedir. Kuvvetli şüphe ise, mevcut delillere göre yapılacak muhakeme sonucunda mahkum olma ihtimalinin kuvvetle muhtemel olmasıdır[1306].

Önleme amaçlı iletişimin denetlenmesi tedbiri bakımından hukukumuzda makul şüphe kriteri benimsenmiştir. Bu tür girift yapılı ve dış kaynaklı örgütler tarafından organize edilen suçlara ilişkin yeterli bilgi ve belgenin ele geçirilmesi kolay olmadığından, kuvvetli şüpheye yetecek kadar şüphenin varlığının aranması halinde bu tedbirin uygulanması oldukça zorlaşacağı için makul şüphe kriterinin arandığı anlaşılmaktadır.

Bununla birlikte, hem 4422 sayılı Kanunda hem de CMK'da yer verilen, kuvvetli şüphe kriterinin, önleme amaçlı iletişimin denetlenmesinde de kullanılabileceği bazı yazarlar tarafından savunulmakta, 5397 sayılı Kanunda bu konuda bir hüküm bulunmaması, anılan kanunun önemli eksikliklerinden birisi olarak sayılmaktadır[1307]. Gerçekten de, Kanun metninde; "Devletin ülkesi ve milletiyle bölünmez bütünlüğüne, Anayasa düzenine ve genel güvenliğine dair önleyici ve koruyucu tedbirleri almak, emniyet ve asayişi sağlamak üzere…" yazılı suçların işlenmesinin önlenmesi amacıyla dinleme kararı verilir denilmektedir. Bu suçların işleneceğine dair nasıl bir ağırlık, yakınlık veya yoğunluk aranacağının belirtilmemiş olması karşısında istihbarat kuruluşlarının getireceği taleplerin yeterli bir denetlemeye tabi tutulamayacağı açıktır[1308].

3.3.3.4. Önleme Amaçlı İletişimin Denetlenmesine Hakim Tarafından Karar veya Onay Verilmiş Olması

Haberleşme hürriyetinin Anayasal şartlarını düzenleyen Anayasa'nın 22/2. maddesine göre, bu hürriyetin sınırllandırılması için mutlaka usulüne uygun olarak verilmiş bir hakim kararı veya gecikmesinde sakınca bulunan hallerde yetkili merciin yazılı emrinin bulunması gerekmektedir. Buna göre önleme amaçlı iletişimin denetlenmesi tedbirine hakim kararı veya

---

[1306] GÖKCEN, s.66; ÇOLAK/TAŞKIN, s.628.

[1307] ALTIPARMAK, s. 48.; TAŞKIN, s. 273.

[1308] TAŞKIN, s. 273-274.

gecikmesinde sakınca bulunan hallerde bu konuda 5397 sayılı Kanununun yetkili kıldığı merciin yazılı emriyle başvurulabilir. Yetkili merciin yazılı emriyle tedbire karar verilmesi halinde bu karar, yirmi dört saat içinde görevli ve yetkili hakimin onayına sunulmalıdır. Hakimin, yirmi dört saat içinde kararını vermesi gereklidir. Hakim kararı veya onayı aranması, tedbirin haberleşme özgürlüğüne ağır müdahale oluşturması sebebiyle, haberleşme özgürlüğüne hukuki bir koruma sağlamaktadır[1309]. Bununla birlikte, daha suç işlenmemişken bu tedbire başvurulabilmesi hürriyetler bakımından bir tehlike teşkil ettiğinden, hakim tarafından karar verilirken hangi ölçütlere ve şartlara göre değerlendirme yapılarak karar verileceği hususlarının düzenlenmemiş olmasının keyfiliğe yol açması mümkündür[1310]. Gerçekten de, hürriyetin kısıtalanması sonucunu doğuran bu işlem hakkında verilecek karara ilişkin sürecin ölçü ve şartlarının belirli ve öngörülebilir olması gerekmektedir.

3.3.3.4.1. Yetkili Ve Görevli Hakim

Anayasa'nın 22/2. maddesinde haberleşme özgürlüğüne müdahale edebilmek için, mutlaka usulüne uygun olarak verilmiş bir hakim kararına gerek olduğu hükme bağlanmış olup, gecikmesinde sakınca bulunan hallerde kanunla yetkili kılınmış merciin yazılı emri ile de haberleşme özgürlüğüne müdahale edilebileceği öngörülmüştür. Bununla birlikte, Kanunla yetkili kılınmış merciinin yazılı emri nihai karar olmayıp 24 saat içinde hakim onayına sunulmalıdır. 5397 sayılı Kanun da, Anayasamızdaki bu hükme uygun olarak, önleme amaçlı olarak iletişimin denetlenmesi kararının mutlaka hakim tarafından verilmesi gerektiğini hükme bağlamıştır.

5397 sayılı Kanun uyarınca, bu tedbire karar vermeye yetkili olan hakim, tedbir talebinde bulunan kolluk biriminin bulunduğu yer itibariyle yetkili olan ve 5271 sayılı CMK'nın 250/1. maddesine göre kurulan özel yetkili ağır ceza mahkemesi üyesidir[1311].

Önleme amaçlı iletişimin denetlenmesine hakim kararı ile başvurulabilmesi uygulaması, ABD hukukunda da vardır. FISA Kanunu çerçevesinde verilecek önleme amaçlı iletişimn denetlenmesi kararını verecek makam FISA Mahkemesi (FISC-Foreign Intelligence Surveillence Court) olarak adlandırılan özel görevli[1312] ve gizli[1313] bir mahkemedir.

[1309] ÇOLAK/TAŞKIN, s. 619; ŞEN, (İletişimin Denetlenmesi Tedbiri), s. 102.

[1310] ÜNVER/HAKERİ, s. 192;ŞAHİN, s. 379.

[1311] CENTEL/ZAFER, s. 367;ÜNVER/HAKERİ, s. 192; ÇOLAK/ TAŞKIN, s. 619; Fransız hukukunda istihbarat amaçlı denetlemelerde kural olarak başbakan ya da onun yetkilendirdiği içişleri bakanı ile milli savunma veya gümrüklerden sorumlu bakan izin verebilmektedir. İzinler yazılı ve gerekçeli olmak zorundadır. (HANUCH, Sebastien, İnterception, http://www.supinfo-projects.com/fr/2004 /interception s. 3).

[1312] Bu mahkemenin FISA sürecini kontrol etmek dışında herhangi bir fonksiyonu yoktur. STEVENS/ DOYLE, s. 46.

Hakim, FISA uyarınca yapılmış başvuruyu reddettiğinde, FISA İtiraz Mahkemesine[1314] başvurulabilir. ABD Yüksek Mahkemesi Başkanı tarafından atanan 3 hakimden oluşan bu mahkeme başvuruların reddine ilişkin olarak verilen kararı incelemekle yükümlüdür. FISA İtiraz Mahkemesinin verdiği gerekçeli karara karşı temyiz mercii olan Yüksek Mahkemeye başvurulması mümkündür[1315].

3.3.3.4.2. Gecikmesinde Sakınca Bulunan Hal Kavramı ve Yazılı Emir

Önleme amaçlı iletişimin denetlenmesine kural olarak hakim karar verecektir. Ancak gecikmesinde sakınca bulunan hallerde, 5397 sayılı Kanun ile belirlenen yetkili makamlar da yazılı emirle bu tedbire karar verebilirler. İletişimin denetlenmesi tedbirinin haberleşme özgürlüğüne müdahaledeki niteliği göz önüne alındığında "gecikmesinde sakınca bulunan hal" kavramının ne anlama geldiğinin iyi belirlenmesi gerekir. Çünkü, haberleşme özgürlüğüne müdahaleye hukuki koruma niteliğinde bulunan hakim kararı alınmadan, bu alana müdahale söz konusudur. Bu kapsamda gecikmesinde sakınca bulunan hal, derhal işlem yapılmadığı takdirde, milli güvenlik ve kamu düzeninin, genel sağlık ve genel ahlakın veya başkalarının hak ve hürriyetlerinin korunmasının tehlikeye girmesi veya zarar görmesi, suç işlenmesinin önlenememesi, taşınması veya bulundurulması yasak olan her türlü silah, patlayıcı madde veya eşyanın tespit edilememesi ihtimalinin ortaya çıkması ve gerektiğinde hakimden karar almak için vakit bulunmaması durumlarını ifade etmektedir[1316]. Bu doğrultuda 10.11.2005 tarihli Yönetmeliğin 3. maddesinde "gecikmesinde sakınca bulunan hal" kavramının "Derhal işlem yapılmadığı takdirde suçun iz, eser, emare ve delillerinin kaybolması veya şüphelinin kaçması veya kimliğinin saptanamaması olasılığının ortaya çıkması halini," ifade ettiği belirtilmiştir. Dolayısıyla bu haller dışındaki durumlar da, "gecikmesinde sakınca bulunan hal" olarak değerlendirilerek görevli ve yetkili kolluk makamı tarafından iletişimin denetlenmesi için yazılı emir verilemeyecektir[1317].

[1313] DONOHUE, s. 14; EFF ANALYSIS OF PATRIOT ACT.

[1314] 50 U.S.C. § 1803(b).

[1315] 50 U.S.C. § 1803(b); BULZOMI,"Foreign Intelligence Surveillance Act", ; DONOHUE, s. 15-18; Ayrıca, Bk. DECKER, s.17; ADLER, s.3.

[1316] ÇOLAK/ TAŞKIN, s. 619.

[1317] Bu düzenlemeye daha uygun bir gecikmesinde sakınca bulunan hal tanımı Adlî ve Önleme Aramaları Yönetmeliğinin 4. maddesinde adli ve önleme ayrımı yapılmak suretiyle tanımlanmıştır. Buna göre "Önleme aramaları bakımından, derhâl işlem yapılmadığı takdirde, millî güvenlik ve kamu düzeninin, genel sağlık ve genel ahlâkın veya başkalarının hak ve hürriyetlerinin korunmasının tehlikeye girmesi veya zarar görmesi, suç işlenmesinin önlenememesi, taşınması veya bulundurulması yasak olan her türlü silâh, patlayıcı madde veya eşyanın tespit edilememesi ihtimâlinin ortaya çıkması ve gerektiğinde hâkimden karar almak için vakit bulunmaması hâlini" ifade edeceği belirtilmiştir. Her ne kadar burada önleme aramasından söz edilmekteyse de bize göre bu tanım önleme amaçlı iletişimin denetlenmesi müessesesine daha uygundur. TAŞKIN, s. 209.

Gecikmesinde sakınca bulunan hâllerde, Millî İstihbarat Teşkilatı Müsteşarı veya yardımcısı, Emniyet Genel Müdürü veya İstihbarat Dairesi Başkanı ve Jandarma Genel Komutanı veya İstihbarat Başkanı tarafından telekomünikasyon yoluyla iletişimin denetlenmesi için yazılı emir ile karar verebilirler[1318]. Bu makamlar tarafından verilen yazılı emir, yirmi dört saat içinde görevli ve yetkili hakimin onayına sunulması gerekmektedir. Onay talebine ilişkin olarak hâkim, kararını en geç yirmi dört saat içinde verecektir. Hakim yazılı emri onaylamadığı takdirde ya da verilen yirmi dört saatlik sürede herhangi bir karar vermez ise tedbire derhal son verilecektir[1319].

Ülkemizde kamu yönetimi sistemi İl İdaresi Kanunu temelinde yürütüldüğünden dolayı mülki idare sisteminin iletişimin denetlenmesi boyutunda yer alması gerektiği düşünülmektedir. Özellikle illerde suç işlenmesinin önlenmesi, kamu düzeni, genel ahlak ve genel sağlılığın korunması için görevli ve yetkili kılınan valiler, önleyici istihbarat yapılmasında sistemin dışında bırakılmışlardır. Bu durum kolluk birimlerinin doğrudan hakimlerle çalışması gibi bir duruma yol açmakta, idarenin işleyişinin dışında olan hakimlerin, önleyici istihbarat gibi idari niteliği ağır basan bir konuda doğrudan kollukla muhatap olmaları çeşitli sakıncalara neden olmaktadır. Sivil ve demokratik yönetim sistemi açısından valilerin kollukla hakimler arasındaki karar alma sürecinde mutlaka bulunmaları gerektiği anlaşılmaktadır. Böylece, valilerde yazılı emir yetki ve göreviyle donatılmalıdırlar.

3.3.4. Önleme Amaçlı İletişimin Denetlenmesi Kararlarında Bulunması Gereken Unsurlar

3.3.4.1. Temel Unsurların Kararda Belirtilmesi

İletişimin önleme amaçlı denetlenmesi için verilecek kararda ve yazılı emirde, hakkında tedbir uygulanacak kişinin kimliği, iletişim aracının türü, kullandığı telefon numaraları veya iletişim bağlantısını tespite imkân veren kodlardan belirlenebilenler ile tedbirin türü, kapsamı ve süresi ile tedbire başvurulmasını gerektiren nedenlerin hepsinin belirtilmesi zorunludur[1320].

Yukarıda belirtilen hususların belirtilmesi 5397 sayılı Kanunla değişik 2559 sayılı Polis Vazife ve Salahiyet Kanununun ek 7. maddesi, 2803 sayılı Jandarma Teşkilat, Görev

[1318] Bu görevleri asaleten yürütenlerin belirtilen yetkileri kullanabilecekleri gibi söz konusu görevleri vekaleten yürütenler de aynı yetkiye sahip olacaklardır.

[1319] CENTEL/ZAFER, s. 367;ÇOLAK/ TAŞKIN, s. 619; ÖZBEK, s. 421.

[1320] ÜNVER/HAKERİ, s.192; ŞEN, (İletişimin Denetlenmesi Tedbiri), s. 101.

ve Yetkileri Kanununa aşağıdaki ek 5. maddesi ve 2937 sayılı Devlet İstihbarat Hizmetleri ve Millî İstihbarat Teşkilatı Kanununun (MİT) 6. maddelerinde yapılan düzenlemelerle zorunlu kılınmıştır. Her ne kadar getirilen yasal düzenlemede bu konuya açıklık getirilmemiş olsa da, iletişimi denetim altına alınacak kişiler başkasına ait iletişim araçlarını kullanıyorsa, bu hususla birlikte bu üçüncü kişinin de açık kimlik bilgilerinin kararda belirtilmesi gerekir. Denetim kararının bu şekilde ayrıntılı olması halinde ilgisiz kimselerin iletişiminin denetlenmesinin önüne geçilecek[1321], genel nitelikli ve daha çok kişinin hürriyetini tahdit eden bir uygulama yapılması engellenmiş olacaktır[1322].

İletişimin denetlenmesi tedbiri kararında, belirtilen unsurların hepsinin birlikte bulunması gerekmektedir. Ancak, her zaman bu kadar ayrıntılı bilginin bilinebilmesi mümkün olmamaktadır. Örneğin kimliği tespit edilememiş bir örgüt üyesinin eylem yapacağına ilişkin gelen istihbarat kapsamında bu örgüt üyesinin eylemini engelleme ve kendisini yakalamak amacıyla bu tedbire başvurulmak istenmesi halinde yukarıda belirtilen temel bilgilerin hepsinin elde edilmesi güç olabilir. Bu sebeple karar aşamasında eldeki mevcut bilgilerle de, bu kararın verilebilmesi gerekir. 5397 sayılı Kanunun içeriğinden de kararda bulunması gereken hususlarda zorunlu bilgiler ve ihtiyari bilgiler olmak üzere ikili bir ayrıma gidildiği anlaşılmaktadır[1323].

Buna göre, tedbir kararında bulunması gereken zorunlu unsurlar;

1. Tedbirin Türü,

2. Tedbirin Kapsamı,

3. Tedbirin Süresi,

4. Tedbire başvurulmasını gerektiren nedenler.

İhtiyari unsurlar ise;

1. Hakkında tedbir uygulanacak kişinin kimliği,

2. İletişim aracının türü,

3. Kullandığı telefon numaraları,

[1321] ÜNVER/HAKERİ, s.169.

[1322] ŞEN, (İletişimin Denetlenmesi Tedbiri), s. 101.

[1323] ÇOLAK/ TAŞKIN, s. 619.

4. İletişim bağlantısını tespite imkân veren kodu.

İletişimin denetlenmesi kararında bulunması gereken zorunlu bilgilerin bulunmaması halinde Telekomünikasyon İletişim Başkanlığı bu kararı veya emri yerine getirmeyerek ve eksikliklerin giderilmesi amacıyla ilgili makamlara iade edecektir. İhtiyari bilgilerin kararda veya yazılı emirde bulunmaması halinde dahi tedbir infaz edilecektir[1324].

10.11.2005 tarihli Yönetmeliğinin 9. maddesinde yapılan değişiklikle[1325] yazılı emirler bakımından yeni bir bilginin daha bulunması zorunlu hale getirilmiştir. Buna göre iletişimin önleme amaçlı denetlenmesine ilişkin verilen yazılı emir metninde "yazılı emrin verildiği tarih ve saat"in de yer alması zorunlu hale getirilmiştir. Ancak burada, "yazılı emrin verildiği tarih ve saat"in yer alma zorunluluğu sadece yazılı emirlerle ilgilidir. Hakimin vereceği kararlarda bu bilginin yer alması zorunluluğu bulunmamaktadır.

Öte yandan 10.11.2005 tarihli Yönetmeliğin 9. maddesinde yapılan bir diğer değişiklikle, "2803 sayılı Kanunun ek 5. maddesi uyarınca iletilen talepler ile verilen kararlar ve yazılı emirlerde sorumluluk alanına ilişkin bilgi ve/veya belgelere de yer verilir" hükmü getirilmiştir. Bu hüküm sadece jandarma teşkilatını ilgilendirmektedir. Polis veya MİT bakımından böyle bir yükümlülük söz konusu değildir[1326].

Amerikan hukukunda hakim FISA kapsamında iletişimin denetlenmesine ilişkin karar verirken bazı şartların varlığını denetler. Bu kapsamda,[1327] Adalet Bakanı tarafından yapılan bir başvuru bulunmalı[1328], hakkında denetleme yapılacak olan hedef, ya bir yabancı güç ya da yabancı ülke ajanı olmalı[1329], hakkında karar çıkarılacak olan yer ve cihazların her birinin yabancı bir güç veya yabancı bir gücün ajanı tarafından bir suçun işlenmesinde kullanılıyor veya kullanılmak üzere olması gerekmektedir[1330]. En aza

---

[1324] ÇOLAK/ TAŞKIN, s. 619.

[1325] Telekomünikasyon Yoluyla Yapılan İletişimin Tespiti, Dinlenmesi, Sinyal Bilgilerinin Değerlendirilmesi Ve Kayda Alınmasına Dair Usul Ve Esaslar İle Telekomünikasyon İletişim Başkanlığının Kuruluş, Görev Ve Yetkileri Hakkında Yönetmelikte Değişiklik Yapılmasına Dair Yönetmelik, 04/07/2007-26572 sayılı R.G.

[1326] Bu düzenlemenin getirilme zorunluluğu 2803 sayılı Kanunun 10. maddesinden kaynaklanmaktadır. Söz konusu maddeye göre "Jandarmanın genel olarak görev ve sorumluluk alanı; Polis görev sahası dışı olup, bu alanlar il ve ilçe belediye hudutları haricinde kalan veya polis teşkilatı bulunmayan yerlerdir". TAŞKIN, s. 212.

[1327] WONG,3.4.8; DONOHUE, s. 14-15; STEVENS/DOYLE, s. 48-50.

[1328] 50 U.S.C. § 1805 (a)(2).

[1329] 50 U.S.C. § 1805 (a)(3)(A).

[1330] 50 U.S.C. § 1805 (a)(3)(B).

indirgeme (minimization procedures)[1331] denilen kavrama riayet edilmiş olması aranmakla birlikte, hakim, bu tedbire başvurulması için gerekli nedenlerin varolup olmadığı hususunu, başka bir ifadeyle makul sebebin (probable cause) olup olmadığını araştırmakla yükümlü kılınmamıştır[1332]. Milli güvenlik ya da milli savunma yetkilisinin bu hususta mahkemeye vereceği teyit mahkeme açısından yeterlidir[1333]. Görüldüğü üzere, burada çok önemli bir hususun irdelenmesi mahkemeye bırakılmamıştır. Mahkeme, makul sebebin var olup olmadığı hususunda bir araştırma yapmakla yükümlü kılınmamış, bu sorumluluk ve yetki talepte bulunan hükümetin omuzlarına yüklenmiştir. Bu bağlamda, önceden belirlenmiş ve milli güvenlik ya da milli savunma yetkilisinin bu hususta mahkemeye vereceği teyit mahkeme açısından yeterli görülmüştür. Elde edilmek istenen bilginin milli güvenliğe ilişkin olduğu ve bilginin normal yollarla temin edilemeyeceği hususunun kanunda belirlenen görevliler tarafından mahkemeye teyit edilmesi başvuru koşulu olarak belirlenmiştir[1334].

3.3.4.2. Suç Türünün ve Tedbir Nedenlerinin Kararda Belirtilmesi

Adli amaçlı iletişimin denetlenmesi tedbirine başvurulmasına karar verilirken CMK'nın 135. maddesinde, iletişimi tespit altına alınacak kişinin kanunda hakkında tedbir kararı verilebilen katalog suçlardan hangisi ile itham edildiğinin de belirtilmesi zorunlu olmasına karşın önleme amaçlı iletişimin denetlenmesini düzenleyen 5397 sayılı Kanun bu konuda açık bir düzenlemeye yer vermemiş yalnızca tedbire başvurulmasını gerektiren nedenlerin belirtilmesi gerektiği belirtilmiştir. CMK'nın 135. maddesinde kararda belirtilmesi gereken hususlar arasında sayılan "tedbire başvurma nedenine ilişkin yeterli bilgi verilmesi" unsuru da hesaba katıldığında 5397 sayılı Kanunun tedbir kapsamına giren suçların belirtilmesi hususunda yeterli olmadığı görülmektedir. Ancak 5397 sayılı Kanunda yer alan "tedbire başvurulmasını gerektiren nedenlerin belirtilmesi" hususunu geniş değerlendirerek, bunun hem tedbire dayanak olan suçun türünü hem de tedbire başvurma nedenleri ve buna ilişkin bilgileri kapsadığını kabul etmek gerekmektedir.

[1331] 50 U.S.C. § 1805 (a)(5).

[1332] 50 U.S.C. § 1805 (a)(3); EFF ANALYSIS OF PATRIOT ACT.

[1333] DONOHUE, s. 14-15; EFF ANALYSIS OF PATRIOT ACT; AN OVERVIEW OF ELECTRONIC SURVEILLANCE, History and Current Status, D.1.3.

[1334] DONOHUE, s. 14-15; EFF ANALYSIS OF PATRIOT ACT.

3.3.5. Önleme Amaçlı İletişimin Denetlenmesinde Süre ve Sürenin Uzatılması

Önleme amaçlı iletişimin denetlenmesi tedbirine ilişkin kararlar, kural olarak üç ay süreyle verilir. Süre, kararın TİB tarafından sisteme tanıtıldığı andan itibaren başlayacaktır[1335]. Ancak verilen bu üç aylık süre bu tedbirin amacı olan suçların önlenmesi ve gerekli istihbaratın sağlanması için yeterli olmayabileceğinden gerekli durumlarda tedbirin devamına ihtiyaç duyulabilir[1336]. Bu sebeple tedbir kararının alındığı zamanki şartlar mevcut olmak koşuluyla hakim üç aylık bir uzatma süresi verebilir. Hakim aynı konuyla alakalı olarak en fazla üç defa uzatma kararı verebilir. Ancak terör örgütünün faaliyeti çerçevesinde devam eden tehlikelere ilişkin olarak gerekli görülmesi halinde hakim üç aydan fazla olmamak üzere bu sürenin müteaddit defalar uzatılmasına karar verebilir. Adli amaçlı iletişimin denetlenmesinde herhangi bir örgütün faaliyeti çerçevesinde işlenen suçlarla ilgili olarak gerekli görülmesi halinde, hakimin, bir aydan fazla olmamak üzere sürenin müteaddit defalar uzatılmasına karar verebileceği belirtilmesine karşın; önleme amaçlı iletişimin denetlenmesinde sürenin müteaddit defalar uzatılabilmesi yalnızca terör suçları bakımından öngörülmüştür. 5397 sayılı kanunda 23/05/2007 tarih ve 5651 sayılı Kanun ile yapılan değişiklikle casusluk suçları bakımından tedbir süresinin uzatılmasına dair yeni düzenlemeler eklenmiştir. Yeni düzenleme uyarınca, casusluk faaliyetlerinin tespiti çerçevesinde devam eden tehlikelere ilişkin olarak gerekli görülmesi halinde, hâkim üç aydan fazla olmamak üzere sürenin müteaddit defalar uzatılmasına karar verebilir[1337].

İletişimin denetlenmesi tedbirinde sürenin uzatılmasına ilişkin talep ve kararlarda denetleme kararında olması gereken diğer unsurların yanı sıra ilk karara ilişkin bilgiler ile uzatmanın gerekçesi belirtilmelidir. Uzatma kararı verilebilmesi için, tedbire başvurulabilmesi için gerekli koşulların halen mevcut olması ve bunun mevcut olduğunun da uzatma kararında açıkça gösterilmesi gerekir. Aksi durumda süre açısından getirilen sınırlamanın gereksiz ve keyfi biçimde göz ardı edilmesine açık kapı bırakılmış olur. Hakim tarafından uzatma kararı verilebilmesi için, ilk denetim kararında hedeflenen amacın henüz gerçekleşmemiş bulunması fakat ulaşmanın mümkün olması gerekir[1338].

Sürenin uzatılmasına ilişkin kararlar ancak hakim tarafından verilebilir. İlgili mercilerin yazılı emirle bu süreyi uzatmaları mümkün değildir. Nitekim, verilen ve uygulanmasına

---

[1335] ÇOLAK /TAŞKIN, s.633.

[1336] ŞEN, (İletişimin Denetlenmesi Tedbiri), s. 102.

[1337] TAŞKIN, s. 217.

[1338] ÇOLAK /TAŞKIN, s.633; KUNTER/YENİSEY/ NUHOĞLU, s.714; ERDEM/ÖZTÜRK, s. 607.

devam edilen bir kararda, gecikmesinde sakınca bulunan bir durumun bulunması mümkün değildir. Sürenin uzatılmasını gerektiren sebeplerin bulunması halinde ilgili kolluk yetkilileri sürenin bitiminden önce bu taleplerini gerekçeleriyle birlikte hakime sunarak sürenin uzatılmasını talep edebilirler[1339].

3.3.6. Önleme Amaçlı İletişimin Denetlenmesi Tedbirinin Gizliliği ve Tedbirin Yerine Getirilmesi

3.3.6.1. Tedbirin Gizliliği

Önleme amaçlı iletişimin denetlenmesi tedbirinin uygulanması çerçevesinde elde edilen bilgi ve kayıtların saklanmasında ve korunmasında gizlilik ilkesi geçerlidir. Buna göre gizlilik ilkesine aykırı hareket ederek bu bilgi ve kayıtları ifşa edenler ve amacı dışında kullananlar hakkında, görev sırasında veya görevden dolayı işlenmiş olsa bile gerekli disiplin[1340] ve ceza soruşturması yapılacaktır[1341].

İletişimin denetlenmesine ilişkin işlem ve kararlar, hem haberleşme özgürlüğü ve özel hayatın korunması hem de soruşturmanın gizliliği ilkesi gereğince, tedbir süresince ve tedbir süresinin bitiminden sonra elde edilen kayıt ve bilgilerin gizli tutulacağı 5397 sayılı Kanunun getirdiği yasal düzenlemelerdir. Adli amaçlı iletişimin denetlenmesi tedbirinde tedbir süresince tedbirin gizliliğine riayet edileceği belirtilmesine karşın; önleme amaçlı iletişimin denetlenmesi tedbirini düzenleyen 5397 sayılı Kanun'da "Elde edilen bilgi ve kayıtların saklanmasında ve korunmasında gizlilik ilkesi geçerlidir" şeklinde bir düzenlemeye yer verilmek suretiyle buradaki gizlilik için bir süre belirtilmemiş olduğu anlaşılmaktadır.

Gizlilik ilkesinin ihlal edilmesi halinde gerekli soruşturmanın yapılması amacıyla ve de 5397 sayılı Kanundaki yasal düzenlemelere paralel olarak çıkarılan 10.11 2005 tarihli[1342] Yönetmeliğin 27. maddesinde Yönetmelik hükümlerine göre, yürütülen faaliyetler çerçevesinde elde edilen bilgilerin, Yönetmeliğin dayanağını oluşturan kanunlarda belirtilen amaç ve usul dışında kullanılamayacağı belirtilmiştir. Bu kapsamda elde edilen bilgi, belge ve kayıtların saklanmasında ve korunmasında gizlilik

---

[1339] ÇOLAK/TAŞKIN, s. 620.

[1340] ŞEN, (İletişimin Denetlenmesi Tedbiri), s. 102.

[1341] ÜNVER/HAKERİ, s. 192; CENTEL/ZAFER, s. 368; ŞEN, (İletişimin Denetlenmesi Tedbiri), s. 102.

[1342] Telekomünikasyon Yoluyla Yapılan İletişimin Tespiti, Dinlenmesi, Sinyal Bilgilerinin Değerlendirilmesi ve Kayda Alınmasına Dair Usul ve Esaslar ile Telekomünikasyon İletişim Başkanlığının Kuruluş, Görev ve Yetkileri Hakkında Yönetmelik.

ilkesine riayet edileceği aksi takdirde bu husustaki hükümlere aykırı hareket edenler hakkında görev sırasında veya görevden dolayı işlenmiş olsa bile Cumhuriyet savcılarınca doğrudan soruşturma yapılacağı düzenlenmiştir.

3.3.6.2. Tedbirinin Yerine Getirilmesi

Önleme amaçlı iletişimin denetlenmesine ilişkin hakim kararları ve yazılı emirler, talepte bulunan kolluk veya istihbarat biriminin görevlileri tarafından yerine getirilecektir. Buna göre tedbir kararının amacı doğrultusunda suçları önlenmesi ve gerekli istihbaratın sağlanmasına ihtiyaç duyan ve talepte bulunan merci olarak Emniyet Genel Müdürlüğü İstihbarat Dairesi Başkanlığı, Jandarma Genel Komutanlığı İstihbarat Başkanlığı ve MİT Müsteşarlığı görevlilerince yerine getirilecektir[1343].

İlgili kurum yetkilileri bu yerine getirme işlemlerini TİB aracılığı ile yapacaklarıdır. Bu sebeple ilgili karar ve yazılı emirler doğrudan işletmecilere gönderilmeyecektir. Usulüne uygun olduğu tespit edilen kararlar ve yazılı emirler, ilgili kurum görevlileri ve Başkanlık çalışanları aracılığıyla başkanlığın koordine ve nezaretinde yerine getirilecektir. Adli amaçlı iletişimin denetlenmesi tedbirinin yerine getirilmesinde Cumhuriyet savcılığına görev verilmesine karşın önleme amaçlı iletişimin denetlenmesi tedbirinin yerine getirilmesinde Cumhuriyet savcısına yer verilmemiştir.

Adli amaçlı iletişimin denetlenmesi tedbirinin uygulanması ile ilgili 14.01.2007 tarihli "Ceza Muhakemesi Kanununda Öngörülen Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi, Gizli Soruşturmacı ve Teknik Araçlarla İzleme Tedbirlerinin Uygulanmasına İlişkin Yönetmeliğin 9. maddesinde; "İşlem görevlileri" başlığı ile bu konuya ilişkin düzenleme yapılmıştır. Bu yönetmelikte, Cumhuriyet savcısınca belirlenen kolluk birimince; iletişimin dinlenmesi, kayda alınması, sinyal bilgilerinin değerlendirilmesi ve tespitiyle ilgili işlemlerin yerine getirilmesi amacıyla yeterli sayıda personel görevlendirileceği ve bu kapsamda yapılan işlemlerin ve yapıldığı yerlerin gizliliği, düzeni ve güvenliği ile kolluk görevlilerinin aidiyet numaralarının belirlenmesine ve muhafazasına ilişkin esas ve usuller ilgili kolluğun merkez birimlerince düzenleneceği öngörülmüştür.

10.11.2005 tarihli Telekomünikasyon Yoluyla Yapılan İletişimin Tespiti, Dinlenmesi, Sinyal Bilgilerinin Değerlendirilmesi ve Kayda Alınmasına Dair Usul ve Esaslar ile Telekomünikasyon İletişim Başkanlığının Kuruluş, Görev ve Yetkileri Hakkında

[1343] CENTEL/ZAFER, s. 368; ÜNVER/HAKERİ, s. 194.

Yönetmelik'te ise, önleme amaçlı iletişimin denetlenmesi tedbirinin yerine getirilmesine ilişkin detaylı bir düzenleme bulunmamaktadır. Bu yönüyle Başbakanlık ve İçişleri Bakanlığınca bir yönetmelik çalışması yapılması zorunluluğu bulunmaktadır.

3.3.7. Önleme Amaçlı İletişimin Denetlenmesi Tedbirine Son Verilmesi

3.3.7.1.Sona Erme Sebepleri

3.3.7.1.1.Tedbir Süresinin Sona Ermesi

Önleme amaçlı İletişimin denetlenmesi tedbirine ancak belirli bir süreyle karar verilebileceğine göre, bu sürenin sona ermesi halinde tedbire ilişkin karar, sürenin bittiği andan itibaren hükümsüz kalacağından Telekomünikasyon İletişim Başkanlığınca tedbirin uygulanmasına derhal son verilecektir. Sürenin bitiği tarihten sonra denetleme devam etse de elde edilen bilgilerin delil olarak değerlendirilmesi mümkün değildir. Dolayısıyla 10.11.2005 tarihli Yönetmeliğin 11. maddesinde de belirtildiği üzere iletişimin denetlenmesi kararında öngörülen süre dolduğu anda ve sürenin uzatılmasına ilişkin bir kararın da bulunmaması halinde tedbire, her hangi bir karara ihtiyaç duyulmadan ilgili kurumca kendiliğinden son verilmelidir[1344].

3.3.7.1.2. Hakimin Onayının Alınmaması

İletişimin denetlenmesi tedbirinin sona ermesine ilişkin olarak 5397 sayılı Kanunun getirdiği düzenlemelere paralel olarak 10.11.2005 tarihli Yönetmelik hazırlanmıştır. Bu düzenleme ile; yetkili merci tarafından gecikmesinde sakınca bulunan bir durum gerekçesiyle verilmiş olan iletişimin denetlenmesi kararının 24 saat içinde hakime sunulmaması veya hakimin bu süre içinde yazılı emri iptal etmesi halinde, tedbire derhal son verileceği belirtilmiştir[1345]. Bu kapsamda yazılı emir üzerine yapılan denetimden elde edilen kayıt ve bilgiler delil olarak değerlendirilmeyecektir.

3.3.7.2. Sona Erdirme Kararının Verilmesi

Önleme amaçlı İletişimin denetlenmesi kararına hakim tarafından karar verilmesine karşın, tedbire son verilmesi için hakim tarafından karar verilmesine gerek yoktur. Yukarıda belirtilen sona erme sebeplerinin oluşması halinde TİB tarafından doğrudan tedbirin uygulanmasına son verilecektir. Ancak kanunda açıkça düzenlenmemesine

---

[1344] ÇOLAK/TAŞKIN, s.620;ÜNVER/HAKERİ, s. 194.

[1345] ÇOLAK/TAŞKIN, s.620.

karşın Emniyet Genel Müdürlüğü, Jandarma Genel Komutanlığı veya Milli İstihbarat Teşkilatı yetkilisinin tedbiri sonlandırma yetkisi bulunduğu kabul edilmelidir. Kanunun belirlediği ve önlenmesi amaçlanan katalog suçun işlenmesi veya başka nedenlerle, tedbir ile elde edilecek bir sonucun kalmaması halinde, tedbirin uygulanması bir fayda sağlamayacaktır. Tedbirin sonlandırılması, kişi hak ve hürriyetleri bakımından yararlıdır ve bu nedenle bu yetkinin anılan kurumlara verilmesi yerinde olacaktır[1346].

3.3.8. Önleme Amaçlı İletişimin Denetlenmesi Sonucu Elde Edilen Bilgilerin Yok Edilmesi ve İlgiliye Haber Verme

3.3.8.1. Yok Edilme Usulü

Kanunda belirtilen suçların işlenmesinin önlenmesi amacıyla verilen İletişimin denetlenmesi tedbirinin uygulanması neticesinde elde edilen bilgilerin amaç dışı kullanılmasını önlemek için, tedbirin uygulanma süresinin dolması halinde veya yetkili merci tarafından verilen yazılı emrin hakim tarafından onaylanmaması ya da yazılı emrin onaylanmamasına ilişkin karar verilmesi halinde elde edilen kayıt ve bilgiler, Telekomünikasyon İletişim Başkanının ve tedbir talebinde bulunan ilgili kurumların en üst amirinin denetimi altında en geç on gün içinde yok edilecektir. Kayıt ve bilgilerin yok edilmesi hususu bir tutanakla tespit olunduktan sonra tutanak denetimlerde ibraz edilmek üzere muhafaza edilecektir[1347]. Buradaki yok etme kavramından, elde edilen ancak yok edilen içerikleri itibariyle kullanılmasına gerek görülmeyen bilgiler anlaşılmalıdır. Çünkü 5397 sayılı Kanunun 1/7. maddesinde bu madde hükümlerine göre yürütülen faaliyetler çerçevesinde elde edilen kayıtların, Kanunun amacı dışında kullanılamayacağı, elde edilen bilgi ve kayıtların saklanmasında, korunmasında gizliliğin esas olduğu belirtilmiştir. Bu ifadelerden elde edilen bilgilerin saklanabileceği anlaşılmaktadır[1348].

3.3.8.2. İlgiliye Haber Verilmesi

İletişimin denetlenmesi tedbirine son verildikten sonra, hakkında tedbir uygulanan ilgiliye, tedbir uygulaması konusunda bilgi verilmesi Anayasa'nın 36. maddesinde düzenlenmiş olan "Hukuksal korunma güvencesi" ilkesinin etkili olarak hayata geçirilmesinin bir gereğidir. Bu uygulama aynı zamanda, hak arama özgürlüğünü düzenleyen Anayasa'nın 38/4 ve AİHS'nin 6. maddesindeki düzenlemelerin de zorunlu bir sonucudur.

[1346] ÜNVER/HAKERİ, s. 194; ÇOLAK/TAŞKIN, s.620.

[1347] ÇOLAK/TAŞKIN, s.620;CENTEL/ZAFER, s. 368; ÜNVER/HAKERİ, s. 194.

[1348] KAYA, (İletişimin Dinlenmesi), s.13.

Adli amaçlı iletişimin denetlenmesi tedbirinin uygulanmasına son verildikten ve soruşturma evresinin bitmesinden itibaren 15 gün içinde yapılması ve ilgiliye haber verilmesi CMK'nın 137/4. maddesinde hüküm altına alınmasına karşın; önleme amaçlı yapılan iletişimin denetlenmesi tedbirinde kayıt ve bilgiler yok edildikten sonra ilgililere haber verilmesine ilişkin her hangi bir düzenlemeye yer verilmemiştir.

Devletin yapmış olduğu önleme amaçlı iletişimin denetlenmesi tedbirine son verildikten sonra ilgililere bildirmesi yükümlülüğü iki gerekçeye dayandırılabilir. Bunlardan birincisi , gündeme gelen olaylarda mevcut kanunlar gereği gibi uygulanmadığı için tedbir öncesi güvenceler anlamsız kılınmış ve bu nedenle de alınan tedbirin sona ermesinden sonra ayrı bir önem kazanmıştır. Bu imkanı sağlamak için kişilerin denetim faaliyetinden haberdar edilmesi gerekmektedir. İkinci gerekçe ise, Anayasa'nın 40. maddesine göre devlet, işlemlerinde, ilgili kişilerin hangi kanun yolları ve mercilere başvuracağını ve sürelerini belirtmek zorundadır. Bu hüküm uyarınca tedbir sona erdiğinde ve tedbire sebep olan tehlike de ortadan kalktığında hakkında tedbir kararı verilen kişinin bilgilendirilmesi devletin görevidir. Ancak bu yolun etkili olabilmesi için, devletin kişiye olası ihlalin sonuçlarını ortadan kaldıracak hukuk yollarını göstermesi gerekir. Nitekim, bilgi edinme veya edindirme önemli olsa da yargısal denetimin yerini alması mümkün değildir[1349].

Bununla birlikte AİHM 19 Mart 2002 tarihli (Greuter/Hollanda) kabul edilmezlik kararında, devletin hakkında kovuşturma açılmayan kişiye telefonunun dinlendiğini bildirmemesinin diğer güvencelerin bulunması durumunda Avrupa İnsan Hakları Sözleşmesi'ni ihlal etmeyeceği sonucuna ulaşmıştır. Mahkemenin aynı zamanda eleştirilebilecek bu kararından çıkan sonuç, eğer kanun, dinleme öncesi etkili bir yargısal denetim mekanizması öngörüyorsa ve sistem uygulanabiliyorsa dinleme sonrası ilgiliye bilgi verilmemesi sorun teşkil etmemektedir[1350.]

Ülkemiz bakımından, önleme amaçlı iletişimin denetlenmesinden sonra ilgiliye bilgi verilmesi arzu edilse de bunun düzenlenmemiş olması tek başına önemli bir eksiklik sayılmamalıdır.

[1349] ALTIPARMAK, s.52.

[1350] ALTIPARMAK, s.51-52.

3.3.9.Önleme Amaçlı İletişimin Denetlenmesinden Elde Edilen Kayıt ve Bilgilerin Yargılamada Delil Olarak Kullanılması Sorunu

Önleme amaçlı iletişimin denetlenmesi tedbirinin uygulanması sonucu elde edilen kayıt ve bilgiler ancak Kanunda belirtilen amaçlarla kullanılabilecektir. Kanunda belirtilen amaç ise belirtilen suçların işlenmesinin önlenmesidir.

Bu açık hükme göre, önleme amaçlı iletişimin denetlenmesi sonucu elde edilen bilgiler, soruşturma veya kovuşturmada delil olarak kullanılamaz. Cumhuriyet savcısı bu bilgilere dayanarak kamu davası açamaz. Burada açık bir delil yasağı hükmü bulunması sebebiyle mahkemenin de bu bilgilere dayanarak mahkumiyet hükmü kurması mümkün değildir. Bu tedbirlerin uygulanması suretiyle elde edilen bilgiler, bir disiplin soruşturmasında da doğrudan kullanılamaz. Yine önleme amaçlı iletişimin denetlenmesi sonucu elde edilen bilgiler, bir hukuk davasında kullanılamaz. Örneğin, iletişimin denetlenmesi sırasında kullanılan ifadelerin hakaret oluşturması halinde, bu bilgilere dayanılarak tazminat davası açılması veya bir boşanma davasında ispat aracı olarak kullanılması mümkün görünmemektedir[1351].

Suçun önlenmesi amacıyla verilen ve yasal unsurları taşıyan tedbir kapsamında çerçevesi belirlenen suçlardan birisinin işlenmesi halinde, bu bilgilerin soruşturma ve kovuşturmada delil olarak değerlendirilmesi her ne kadar suçla mücadelede önemli faydalar sağlayacak ise de, yukarıdaki açıklamalar uyarınca bu mümkün değildir. Çünkü, önleme amaçlı iletişimin denetlenmesinin koşulları çok daha esnek bir niteliğe sahiptir. Karşılaştırmalı hukukta da, bu yolla elde edilen bilgilerin delil olarak kullanılması söz konusu değildir.

3.3.9.1. Elde Edilen Bilgilerin Suç Duyurusunda Kullanılması

Önleme amaçlı iletişimin denetlenmesi tedbirini düzenleyen 5397 sayılı Kanundaki yasal düzenleme uyarınca, önleme amaçlı iletişimin denetlenmesi sırasında elde edilen bilgiler delil olarak kullanılamayacaktır. Nitekim, CMK kapsamında başvurulan adli amaçlı iletişimin denetlenmesi sıkı şartlara bağlı olduğu halde, başvuru şartlarının önleme amaçlı iletişimin denetlenmesinde daha gevşek uygulandığı muhakkaktır. Önleme amaçlı tedbir ile elde edilen bilgilerin ceza muhakemesinde delil olarak kullanılmasına izin verilmesi halinde, daha sıkı şartların varlığını şart koşan CMK

[1351] TAŞKIN, s. 226.

hükümlerinin by-pass edileceği şüphesizdir [1352]. Ancak bu bilgiler arasında, işlenmesi önlenemediği için işlenmiş olan suçun aydınlatılmasında kullanılabilecek nitelikte önemli bilgiler bulunmaktadır. Bu bilgiler analiz edildiğinde faillerin tespit edilmesi, suç delillerinin neler olduğu ve nerede bulunabileceğine ilişkin önemli ipuçları elde edilebilecektir. Ayrıca bu bilgilerden yararlanılmaması, suçun failinin belirlenememesi veya bazı önemli delillerin elde edilememesi ve suçun aydınlatılamaması sonucunu doğurabilecektir. Halbuki kolluğun bir başka biriminde bu konuda işe yarayacak önemli bilgiler bulunmaktadır. Bu bilgiler kullanılarak delillere ulaşılabilecektir[1353].

Bu bağlamda Kanunda yer alan "başka amaçla kullanılamama" ilkesi, öncelikle ceza yargılamasında delil olarak kullanılmamayı içermektedir. Bundan başka bir hukuk davasının veya idari bir işlemin dayanağını oluşturmamayı kapsamaktadır. Buna karşılık, önleme amaçlı denetleme sırasında elde edilen bazı bilgilerin, denetlemeyi yapan görevlilerce, gizlilik içerisinde, soruşturma veya kovuşturma birimlerine ihbar edilmek veya suç duyurusunda bulunmak suretiyle değerlendirilmesinin ve bazı delillere ulaşmak amacıyla kullanılmasının mümkün olmasını[1354]savunan görüş bizce de isabetlidir.

3.3.9.2 Tesadüfen Elde Edilen Bilgilerin Değerlendirilmesi

Tesadüfen elde edilen bilgi, önlenmesi amaçlanan suç sınıfı dışında kalan diğer bir suçun işleneceğine ilişkin bilgilerdir. Suçla mücadelede önleme hizmetlerinin etkinliği adına, işlenmesi düşünülen her türlü suçla ilgili bir bilgi elde eden güvenlik görevlileri, bu bilgileri değişik yollarla ilgili adli kolluk birimine ihbar etmeli ve suçların işlenmesinin önlenmesi sağlanmalıdır. Tesadüfen elde edilen bilgilerin, 5397 sayılı Kanunda sayılan suçlarla ilgili olması hali ile diğer suçlarla ilgili olması arasında bir fark olmaması gerekmektedir. Aynı şekilde önleme amaçlı iletişimin denetlenmesi tedbiri A hakkında ve uyuşturucu kaçakçılığı yapılacağı gerekçesiyle uygulanırken A ile telefonla görüşen arkadaşı B'nin yaptığı açıklamalarda bir suç işleyeceğine ilişkin bilgilerin elde edilmesi halinde; bu bilgiler ihbar olarak değerlendirilerek B'nin suç işlemesi önlenmelidir. Aksi takdirde kolluk görevlilerinin suçların işleneceğini bilmesine rağmen önlem almaması ve önlememesi sonucu ortaya çıkacaktır. Bu cümleden olarak, bu şekilde elde edilen

---

[1352] ŞAHİN, Ceza Muhakemesi Hukuku, s.264. ABD hukukunda da bu endişe hakimdir. 11 Eylül olayları sonrasında yapılan mevzuat değişiklikleri ile istihbaratçılar ile ceza muhakemesi soruşturmacıları arasındaki delil paylaşımı kolaylaşmıştır.

[1353] TAŞKIN, s. 227.

[1354] TAŞKIN, s. 228.

bilgilerin bilgilerin doğrudan delil olarak kullanılması mümkün olmasa da "delile götüren bilgi" mahiyetinde bir ihbar kabul edilmesi mümkün olmalıdır. Ayrıca B'nin işleyeceği suçun CMK'nın 250. maddesinin birinci fıkrasında sayılan suçlardan birisi olması ile bunlar dışında kalan diğer suçlardan –örneğin hırsızlık- olması arasında bir ayrım olmamalıdır[1355].

3.4. İletişimin Denetlenmesi Tedbirinde Denetim

3.4.1. Genel Olarak

İletişimin denetlenmesi tedbirine son verilmesinden sonra ilgiliye haber verme yükümlülüğünün hukuki mantığı, kişiye hukuksal korunma güvencesi sağlamaktır. Hukuksal korunma güvencesi, kişiye telekomünikasyon yoluyla yapılan iletişimin denetlenmesi tedbiri bakımından yalnızca üst kanun yollarının işletilmesini değil, aynı zamanda tedbirin gizli olma niteliğinden ileri gelen hukuka aykırı sonuçların ortadan kaldırılmasını sağlamak bakımından yeni üst kanun yollarının da öngörülmesini zorunlu kılmaktadır. Hukukumuzda, iletişimin denetlenmesi tedbirine karşı gidilebilecek özel bir üst denetim muhakemesi yolu öngörülmemektedir. Ancak, genel olarak ceza muhakemesinde koruma tedbirlerine karşı gidilebilecek üst kanun yolları olan itiraz ve temyize bu tedbir için de gidilebileceği kabul edilmektedir. Yalnız burada ilgili, kararın yerine getirilmesinden ve genellikle de elde edilen bilgilerin yok edilmesinden sonra hakkında tedbir uygulandığından haberdar olmaktadır. Bu nedenle de, diğer koruma tedbirlerinden farklı olarak iletişimin denetlenmesi tedbirinin uygulandığı sırada, öngörülen hukuksal korunma olanaklarından fiilen yararlanılması mümkün değildir. Bu yüzden sonradan başvurulan üst kanun yolları, yalnızca tedbirin hukuka aykırılığının tespiti sonucuna yol açabilmektedir[1356].

Tedbirin mahiyeti itibariyle gizli olması, tedbirin uygulanması aşamasında ilgilinin itiraz edememesi ve yargısal denetimi talep edememesi hususlarının yanı sıra ilgiliye bildirim yapıldıktan sonra da itirazın hem mümkün olamayacağı ve de faydasının olamayacağı hususu kişi hakları bağlamında sıkça dile getirilen bir argümandır. Hukuki süreci denetleyen yargının bu tedbirin uygulanması sırasında ve akabinde devreye girmesi de aslında esasa ilişkin bir telafi olarak nitelenemez. Bu nedenle, mevcut mevzuatın AİHM'nin denetim hususundaki içtihatlarına uygunluk arz ettiği söylenemez. Giz içeren bu tedbirin, AİHM'nin birinci ve ikinci aşama olarak ifade ettiği, başlangıç ve yerine getirilme aşamalarında hukuka uygunluğunun denetlenmesi hususunda devletin

[1355] TAŞKIN, s. 231.

[1356] CENTEL/ZAFER, s.364;ERDEM, s.106.

inisiyatif alması, yargının kendi içindeki denetimi de dahil olmak üzere birtakım denetim mekanizmalarının hayata geçirilmesi önem arz etmektedir.

3.4.2. Tedbir Kararına Karşı İtiraz Yoluna Başvurulması

14.01.2007 tarihli Yönetmeliğin "İşlemlerin niteliği" başlığını taşıyan 10. maddesinde Ceza Muhakemesi Kanununun 135. maddesindeki hükümlere aykırı olarak verilen kararlar ile bu Yönetmelikte sayılan ve tanımlanan 'iletişimin tespiti, dinlenmesi, kayda alınması ve sinyal bilgilerinin değerlendirilmesi' işlemleri dışındaki talepleri içerdiği açıkça anlaşılan kararlara karşı Cumhuriyet savcısı, şüpheli, sanık, katılan, suçtan zarar gören, müdafi, vekil, şüpheli veya sanığın yasal temsilcisi ve eşi ile Başkanlık tarafından itiraz edebileceği belirtilmiştir. Bu düzenlemeden de anlaşılacağı üzere, iletişimin denetlenmesi tedbirinden ziyade bu tedbir kararında başka taleplerin bulunması halinde bu kararlara itiraz edilebileceği düzenlenmiştir.

Tedbirle ilgili olarak itiraz hakkının kullanılması da bir güvence olarak karşımıza çıkmaktadır. İşlemlerin tarafı olmamasına rağmen TİB'e hukuka uygunluğu sağlamak bakımından itiraz etme hakkı tanınmıştır. İtiraz hakkını kullanabilecekler arasında yer alan Cumhuriyet savcısının bu hakkı, iletişimin denetlenmesine karar verilmesine ilişkin talebinin reddedilmesi halinde doğar. Gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısının verdiği tedbir kararının hakim onayına sunulması durumunda, hakimin bu kararın iptaline ilişkin kararına itiraz edemez ve tedbire derhal son verilir. Bu kararlar kesindir[1357]. İletişimin denetlenmesine ilişkin olarak hakim tarafından verilen kararlara karşı itiraz yoluna gidilebilir. İtiraz hakkı, aleyhine karar verilen şüpheli ve sanık ile şüpheli veya yasal temsilcisi, eşine veya sanığın müdafiine verilmiştir (CMK, 260-262). Buna karşılık hakimin iletişimin denetlenmesi talebinin ret edilmesine ilişkin kararlarına karşı da katılan ve suçtan zarar gören ile bunların vekilleri itiraz edebilir[1358].

Hakim tarafından verilen denetleme kararlarına karşı itiraz edilmesi halinde ilgililer, kararı öğrendikleri tarihten itibaren 7 gün içinde itiraz edebilirler. İtiraz kararı veren mercie verilecek bir dilekçe veya tutanağa geçirilmek koşulu zabıt kâtibine beyanda bulunmak suretiyle yapılır. Kararına itiraz edilen hâkim, itirazı yerinde görürse kararını düzeltir; yerinde görmezse en çok üç gün içinde, itirazı incelemeye yetkili olan mercie gönderir.

[1357] YİĞİT, s. 23.

[1358] Fransız CMK'nun 100. maddesinde iletişimin denetlenmesi kararının yazılı olacağı ve bu karar adli (yargısal) bir karar olmadığından itiraz edilemeyeceği belirtilmiştir. TAŞKIN, s. 45.

Burada tedbirin gizli olma niteliğinden ileri gelen bu sakıncanın ortadan kaldırılabilmesi bakımından, koruma tedbirlerinden zarar gören kişiler için devletin tazminat yükümlülüğü kabul edilmelidir. Çünkü, iletişimin denetlenmesi tedbirinde, ilgilinin üst kanun yollarına başvurması fiilii olarak imkansızdır. Ancak tedbirden haberdar olduktan sonra, usulüne uygun olmayan bir tedbir kararı varlığı anlaşılmakla buna karşı temel hak ve hürriyetlerine yapılan müdahale kapsamında tazminat talebinde bulunabilecektir. Ancak, Türk hukukunda tazminat ödenmesini gerektiren koruma tedbirleri arasında hukuka aykırı olarak telekomünikasyon yoluyla yapılan iletişimin denetlenmesine yer verilmemiştir. Bu durumda idarenin sorumluluğuna ilişkin genel kurallar çerçevesinde devletin tazminat sorumluluğuna gidilebilecektir[1359].

3.4.3. Hukuka Aykırı Olarak İletişimin Denetlenmesinin Sorumluluğu

3.4.3.1. Tazminat Sorumluluğu

Türk hukukunda iletişimin denetlenmesine imkan veren CMK'nın 135 ila 138. maddeleri ile 5397 sayılı Kanunun getirdiği düzenlemelerdeki usul ve esaslar dışında hiç kimse bir başkasının haberleşme hürriyetini denetim altına alamaz. Her ne kadar CMK'nın 135/7. maddesinde bu husus "hiç kimse, bir başkasının telekomünikasyon yoluyla iletişimini dinleyemez ve kayda alamaz" şeklinde hüküm altına alınmışsa da bu düzenleme yeterli olmayıp bu hususun genel olarak "iletişimin denetlenememesi" olarak düzenlenmesi yerinde olurdu. Ancak yasal düzenleme bu olmasına karşın buradan anlaşılması gereken, kişinin, kanunlarda öngörülen usul ve esaslar dışında iletişiminin tespiti, dinlenmesi, kayda alınması ve sinyal bilgilerinin değerlendirilmesinin mümkün olmamasıdır. İletişimin denetlenmesi tedbirine karşı kişinin önceden haberdar olup hukuka aykırı olan tedbirin durdurulması için üst kanun yollarına başvurmasındaki fiili imkansızlık sebebiyle ilgiliye yapılacak bildirimden veya kişinin tedbirden başka bir şekilde haberdar olması halinde temel hak ve hürriyetlerine yapılan müdahale sebebiyle tazminat hakkı doğacaktır[1360].

Türk hukukunda koruma tedbirlerinin uygulanması esnasında sanık, şüpheli veya ilgililerin maruz kalabileceği zararlara ilişkin olarak getirdiği tazminat yükümlülüğü CMK'nın 141 ila 144. maddeleri arasında düzenlenmiştir. Ancak telekomünikasyon yoluyla iletişimin denetlenmesi bir koruma tedbiri olmasına rağmen bu tedbir için

---

[1359] ERDEM, s.106.

[1360] ÖZBEK, s. 433;ÜNVER/HAKERİ, s.197; TAŞKIN/ÇOLAK, s.638.

tazminat istenmesi bu kapsama dahil edilmemiştir. Muhtemeldir ki, kanun koyucu burada maddi bir zararın söz konusu olmadığını düşünmektedir. Ancak, 141. madde hem maddi hem de manevi zararların karşılanacağını öngördüğüne göre, hükmün her türlü koruma tedbirini içerecek şekilde genişletilmesi gerekmektedir[1361]. İletişimin denetlenmesi tedbirinin temel hak ve hürriyetlere müdahalesinin ağırlığı dikkate alındığında bu tedbirin de kapsama dahil edilmesinde bir zorunluluk bulunmaktadır. Haberleşme hürriyeti, özel hayatın gizliliği gibi çok önemli Anayasal hakları ihlal edilen bir kişinin, bu duruma karşılık yapabileceği hiçbir şeyin olmaması öncelikle 'Hukuk Devleti' ilkesine de önemli bir aykırılıktır. Açık yasal düzenleme bulunmaması sebebiyle bu tedbirin uygulanması sebebiyle oluşacak zararlar ancak tazminat hukukunun genel hükümleri çerçevesinde tazmin edilebilecektir. Tedbire ilişkin kararın kanuna aykırı veya hatalı olarak verilmesi durumunda genel hükümler çerçevesinde devletin sorumluluğu olacaktır[1362].

3.4.3.2.Ceza Sorumluluğu

5397 sayılı Kanunda belirtilen koşulların dışında gerek kamu görevlileri gerekse üçüncü kişiler tarafından bir kimsenin iletişiminin denetlenmesi halinde failler hakkında ceza sorumluluğu da doğacaktır. Bu işlemler TCK'nın birden fazla hükmü ile çelişmekte ve buralarda düzenlenen suçları oluşturabilmektedir.

En başta 5397 sayılı Kanunda ve CMK'da belirtilen koşullara aykırı olarak iletişimin denetlenmesi halinde TCK'nın 133. maddesinde düzenlenen "Kişiler Arasındaki Konuşmaların Dinlenmesi ve Kayda Alınması Suçu"nu oluşturacaktır.

Yine TCK'nın 132. maddesinin 1. fıkrasında düzenlenen "Haberleşmenin Gizliliğini İhlal" suçu oluşabilecektir. TCK'nın 132. maddesinin 2. fıkrasında düzenlenen "Kişiler Arasındaki Haberleşme İçeriklerinin Açıklanması" suçunun da meydana gelmesi söz konusu olabilcektir. Koşullarının varlığı halinde TCK'nın 132. maddesinin 3. fıkrasında düzenlenen "Kişinin Kendi İletişimini Kayda Alması ve Açıklaması" suçu da olaşabilecektir.

Yine CMK'nın 258. maddesinde düzenlenen "Göreve İlişkin Sırrın Açıklanması" suçu da işlenebilecektir. Bu suçlardan başka Adli amaçlı iletişimin denetlenmesi tedbirinin uygulanması sırasında soruşturma gizliliğinin ihlali suçunun işlenmiş olması da muhtemeldir.

[1361] ALTIPARMAK, s. 59.

[1362] ÜNVER/HAKERİ, s. 196;ÖZBEK, s. 433.

Görüldüğü gibi hukuka ve kanuna aykırı olarak iletişimin denetlenmesi halinde TCK'nın birden fazla hükmünün ihlal edilmesi ve bu maddelerde belirtilen yaptırımların uygulanması söz konusu olabilcekitr.

3.5.Telekomünikasyon İletişim Başkanlığı (TİB)

3.5.1.TİB'in Kuruluşu

Türkiye Cumhuriyeti Anayasası'nın 03.10.2001-4709/7 maddesi ile değişik ve Haberleşme Hürriyeti Başlıklı 22. maddesi[1363] ile "Herkes, haberleşme hürriyetine sahiptir. Haberleşmenin gizliliği esastır" hükmü getirilmiştir. Anılan maddenin söz konusu hakka birtakım sınırlandırmalar getiren ikinci maddesinde;

- Millî güvenlik,
- Kamu düzeni,
- Suç işlenmesinin önlenmesi,
- Genel sağlık ve genel ahlâkın korunması
- Başkalarının hak ve hürriyetlerinin korunması,

sebeplerinden biri veya birkaçına bağlı olarak usulüne göre verilmiş hâkim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; haberleşmenin engellenemeyeceği ve gizliliğine dokunulamayacağı hükmü getirilmiştir. Yetkili merciin kararı yirmi dört saat içinde görevli hâkimin onayına sunulur" hükmünü amirdir. Bu hüküm doğrultusunda, 23.07.2005 tarihli Resmi Gazete'de yayımlanarak yürürlüğe giren ve 2559, 2803 ve 2937 sayılı Kanunlarda değişiklik yapan 5397 sayılı Kanun ile (2559 sayılı Polis Vazife ve Salahiyet Kanununun Ek 7'nci maddesi) Telekomünikasyon İletişim Başkanlığı kurulmuştur[1364].

Türk hukukunda telekomünikasyon yoluyla iletişimin denetlenmesi tedbirinin niteliği ve kötüye kullanılmasını önlemek ve aynı zamanda uluslararası standartlara uygun olarak tedbirin yerine getirilebilmesini sağlamak amacıyla tüm iletişimin denetlenmesi tedbirlerinin tek merkezden yürütülmesi benimsenmiştir. Bu amaç doğrultusunda 5397

[1363] http://www.tbmm.gov.tr/Anayasa.htm.

[1364] Sıkça sorulan sorular, http://www.tib.gov.tr/detay.aspx?cid=24.

sayılı Kanunun 1. maddesi ile 2559 sayılı Polis Vazife ve Salahiyet Kanununun ek 7. maddesine eklenen hükümlerle Telekomünikasyon İletişim Başkanlığı[1365] kurulmuştur.

Adli amaçlı olarak[1366], 5271 sayılı Ceza Muhakemesi Kanunu kapsamında yetkili Cumhuriyet savcılıkları veya mahkemeler, suçun önlenmesine yönelik ise, ilgili kurumların kendi kanunlarında belirtilen yetkilendirilmiş merciler TİB'den talepte bulunabilmektedirler. Bu itibarla sayılan merciler ve kurumlar dışında doğrudan vatandaşların veya herhangi bir kurum ya da kuruluşun başvuru hakkı bulunmamaktadır[1367].

Telekomünikasyon yoluyla iletişimin denetlenmesi tedbiri kapsamında hem adli hem de önleme amaçlı iletişimin denetlenmesi, Telekomünikasyon İletişim Başkanlığı aracılığı ile mümkündür. Başkanlığın çalışma usul ve esasları 10.11.2005 tarihli Telekomünikasyon Yoluyla Yapılan İletişimin Tespiti, Dinlenmesi, Sinyal Bilgilerinin Değerlendirilmesi ve Kayda Alınmasına Dair Usul ve Esaslar ile Telekomünikasyon İletişim Başkanlığının Kuruluş, Görev ve Yetkileri Hakkında Yönetmelikle belirlenmiştir. Ancak söz konusu Yönetmelikte 4.7.2007 tarihli ve 26572 sayılı Resmi Gazetede yayımlanan Yönetmelik değişikliği[1368] ile Başkanlığın yapısı ve işleyişine yönelik yeni düzenlemeler getirilmiştir.

3.5.2.TİB'in Yapısı

Telekomünikasyon Kurumu bünyesinde doğrudan kurum Başkanlığına bağlı olarak faaliyet gösterecek olan TİB, Başkan ile Teknik, Hukuk, İnternet ve İdari Daire Başkanlıklarından oluşmaktadır.[1369].

TİB Başkanı, Telekomünikasyon Kurumu Başkanının teklifi üzerine Başbakan tarafından atanmaktadır. Bu hüküm, Anayasa Mahkemesine itiraz yoluyla götürülmüş ancak henüz dava neticelendirilememiştir. İtiraza esas teşkil eden husus, Başkan'ın ortak kararname ile atanmamasıdır. TİB Başkanı'nın ortak kararname veya Bakanlar

---

[1365] Telekomünikasyon İletişim Başkanlığı, http://www.tib.gov.tr/.

[1366] TİB'e yapılan başvuruların bir ceza soruşturması veya kovuşturması ile ilgili olması gerekmektedir. Bu bağlamda, bir hukuk davası ile ilgili olarak yapılan iletişimin denetlenmesi talebi TİB tarafınan reddedilmektedir.

[1367] http://www.tib.gov.tr/detay.aspx?cid=25.

[1368] 4/7/2007 tarihli ve 26572 sayılı Resmi Gazetede yayımlanan Telekomünikasyon Yoluyla Yapılan İletişimin Tespiti, Dinlenmesi, Sinyal Bilgilerinin Değerlendirilmesi ve Kayda Alınmasına Dair Usul ve Esaslar İle Telekomünikasyon İletişim Başkanlığının Kuruluş, Görev ve Yetkileri Hakkında Yönetmelikte Değişiklik Yapılmasına Dair Yönetmelik, http://www.tib.gov.tr/detay.aspx?cid=53.

[1369]4/7/2007 tarihli ve 26572 sayılı Yönetmelik değişikliği, http://www.tib.gov.tr/detay.aspx?cid=53.

Kurulu kararıyla atanması kanaatimizce daha isabetli olacaktır. Başkan, Telekomünikasyon Kurulu üyelerinin sahip olduğu özlük haklarına sahiptir. Başkanlığın faaliyetlerini yürütmede yardımcı olmak üzere, TİB Başkanının görüşü doğrultusunda Telekomünikasyon Kurumu Başkanı tarafından kurum içinden veya kurum dışından yeteri kadar teknik, hukukçu ve idarî personel görevlendirilmiş ve 23 Temmuz 2006 tarihi itibariyle kurum göreve başlamış bulunmaktadır. Ayrıca, TİB'de, Millî İstihbarat Teşkilatı, Emniyet Genel Müdürlüğü ve Jandarma Genel Komutanlığının ilgili birimlerinden birer temsilci bulundurulmaktadır. Başkanın, daire başkanlarının ve ilgili kurum personelinin görev ve yetkileri ilgili Yönetmelikte ayrıntılı olarak düzenlenmiştir.

5397 sayılı Kanun ile kurulan TİB, Telekomünikasyon Kurumu bünyesinde doğrudan Kurum Başkanına bağlı olarak görevlerini tek merkezden yürütmektedir. TİB'in üstlendiği bu çok önemli misyon dikkate alındığında kurumun Telekomunikasyon Kurumu bünyesinden çıkarılarak özerk bir yapıya kavuşturulmasının daha yerinde olacağını düşünmekteyiz.

TİB'e bağlı herhangi bir taşra teşkilatı bulunmamaktadır. Telekomünikasyon Kurumuna bağlı toplam 7 adet (Ankara, İstanbul, İzmir, Samsun, Mersin, Diyarbakır ve Erzurum) Bölge Müdürlüğü'nün TİB'in görev kapsamına giren hususlara ilişkin herhangi bir yetkilendirilmesi söz konusu değildir. TİB'in görev alanına giren konularda bölge müdürlükleri ile yapılan yazışmalar, gereksiz ve mükerrer yazışmalara ve evrakın ciddi olarak gecikmesine sebep olmaktadır. Bu nedenle adli mercilerin iletişim ile ilgili işlem taleplerini doğrudan TİB'e iletmeleri usul ekonomisi bakımından yararlı olacaktır.

3.5.3.TİB'in Görevleri

Telekomünikasyon yoluyla yapılan iletişimin tespiti, dinlenmesi, kayda alınması ve sinyal bilgilerinin değerlendirilmesi ile ilgili faaliyetler TİB üzerinden yürütülmektedir. Gerek önleme amaçlı gerekse adli amaçlı iletişiminin denetlenmesine ilişkin olarak yetkili ve görevli hakimlerden alınan kararlar ile gecikmesinde sakınca bulunan hallerde hakim onayına sunulmak üzere verilen yazılı emirler ve Cumhuriyet savcılığı kararları, yerine getirilmek üzere ilgili kurumlarca TİB'e gönderilmektedir. TİB, ilgili kararların usulüne uygun olduğunun anlaşılması halinde kararların infazına ilişkin işlemlere başlayacaktır.

10/11/2005 tarihli ve 25989 sayılı Yönetmeliğin 17 maddesinde TİB'in görevleri olarak aşağıdaki hususlar sayılmıştır:

a) 2559 sayılı Kanunun ek 7. maddesi, 2803 sayılı Kanunun ek 5. maddesi ve 2937 sayılı Kanunun 6. maddesi uyarınca, telekomünikasyon yoluyla yapılan iletişimin tespiti, dinlenmesi, sinyal bilgilerinin değerlendirilmesi ve kayda alınmasına yönelik iş ve işlemleri tek bir merkezden yürütmek,

b) 5271 sayılı Kanunun 135. maddesi kapsamında yapılacak iletişimin tespiti, dinlenmesi, kayda alınması ve sinyal bilgilerinin değerlendirilmesine yönelik iş ve işlemleri tek bir merkezden yürütmek,

c) (a) ve (b) bentleri kapsamındaki taleplerin ilgili mevzuata uygun olup olmadığını incelemek ve gerektiğinde yetkili mercilere başvuruda bulunmak,

d) (a) ve (b) bentleri uyarınca gerçekleştirilen işlemler sonucunda elde edilen verileri ve bilgileri ilgisine göre Millî İstihbarat Teşkilatı Müsteşarlığına, Emniyet Genel Müdürlüğüne ve Jandarma Genel Komutanlığına, talep etmeleri halinde mahkemeye ve Cumhuriyet başsavcılıklarına iletmek,

e) Bu Yönetmelik çerçevesinde yapılacak tespit, dinleme, sinyal bilgilerinin değerlendirilmesi ve kayda alınması faaliyetlerini mümkün kılacak her türlü teknik alt yapının, kamu kurum ve kuruluşları ile kamu hizmeti veren kuruluşlar ve işletmeciler tarafından kurulmasını sağlamak, sağlatmak, gerekli alt yapıyı kurmayan işletmecilerin cezalandırılması yönünde girişimde bulunmak,

f) 12. maddenin ikinci fıkrası ile 15. maddenin üçüncü fıkrası saklı kalmak kaydıyla, Başkanlık faaliyetleriyle ilgili olarak kamu kurum ve kuruluşları, kamu hizmeti veren kuruluşlar ile işletmecilerden gelen her türlü bilgi, belge ve kayıtların bilgi güvenliği kriterlerine uygun olarak arşivlenmesini sağlamak,

g) Görev alanına giren konularla ilgili mevzuatta ulusal ve uluslararası alanda meydana gelen gelişmeleri takip etmek,

h) Başkanlık faaliyetleri için yurt içinden ve yurt dışından teminine ihtiyaç duyulan her türlü malzeme, sistem, yazılım ve donanımı belirleyerek Kurum Başkanına bildirmek,

i) Başkanlık faaliyetleriyle ilgili olarak talep ettiğinde derhal Başbakana bilgi vermek,

j) Kanunlarla verilen diğer görevleri yerine getirmek.

Başkanlığın henüz yeni ihdas edilmiş olması nedeniyle görevine ilişkin hususlar adli ve idari merciler tarafından zaman zaman tam olarak anlaşılamamaktadır. Bu bağlamda

aslında Başkanlığın görev alanına girmeyen bazı talepler görülmektedir. Bunun dışında gözlenen sorunlar genellikle iki başlık altında toplanabilir: Bunlardan ilki iletişimin tespiti, dinlenmesi, kayda alınması ve sinyal bilgilerinin değerlendirilmesine dair işlemlere taalluk etmeyen, bir suç dolayısıyla yapılan soruşturma ve kovuşturma ile herhangi bir yargılama kapsamında Cumhuriyet Başsavcılıkları veya mahkemeler tarafından talep edilen ve aslında doğrudan işletmeciler tarafından istenilmesi gerekli olan bilgi ve belgelere ilişkindir. Örneğin, icra müdürlüklerinin borçlunun telefon numarasından adres tespitine yönelik talepleri, yukarıda hususlar kapsamında doğrudan ilgili işletmecilere gönderilmelidir.

Bu bilgiler şunlardır[1370]:

- Abone ismi, abone adresi, kimlik bilgisi (Abone sözleşmesi ve buna dair bilgiler),

- Telefon numarası, IP numarası, E-mail bilgisi, sim kart bilgisi ve eşleştirmesi, pin-puk numarası,

- İmei/numara sorgusu ve eşleştirmesi (IMEI-telefon numarasından kullanıcıların numarası-, kullanım tarihi, kimlik ve adres bilgisi araştırması),

- İmsi bilgisi, kontör kartları bilgisi ve eşleştirilmesi, roaming bilgisi, telefonun açık olup olmadığı bilgisi, fatura bilgisi, ithal vb olup olmadığı bilgisi.

Diğer bir sorun ise şekle ilişkindir. TİB'in görev alanına giren diğer tüm tespit taleplerinde, mevzuatta öngörülen şartlara uygun olmayan ve örneğin soruşturma numarasının, kovuşturma aşamasında ise mahkeme esas numarasının belirtilmemesi, yetkili imzaların (kaşe-mühür vb) eksik olması, tespit taleplerinin tarih aralıklarının ve diğer unsurlarının açıkça belirtilmemesi gibi konular sayılabilmektedir[1371].

Adli soruşturma kapsamında Cumhuriyet savcıları tarafından değerlendirilen "sabit telefonların tespit trankına bağlanma işlemleri," ilgili işletmeci olan Türk Telekomünikasyon A. Ş. Genel Müdürlüğünün il müdürlükleri tarafından yapılmaktadır.

İletişimin denetlenmesine ilişkin işlemlerin tek merkezden yürütülmesi konusunun AİHM kriterlerine uygunluk arz edip arz etmediği tartışması TİB'le birlikte gündeme gelmiştir. Denetlemenin bu şekilde yapılmasıyla, haberleşme özgürlüğünün daraltıldığı ve özel

[1370] http://www.tib.gov.tr/detay.aspx?cid=40.

[1371] http://www.tib.gov.tr/detay.aspx?cid=40.

hayata müdahalenin artırıldığı iddia edilmektedir[1372]. İstihbarat faaliyeti yürüten kurumların her birinin kendi bünyesinde iletişimin denetlenmesi tedbirini uyguladığı dönemde, yanii 5397 sayılı Kanunun yürürlüğe girmesinden önce; yeknesaklığın bulunmaması, tedbir düzenleyen kurumlar arasındaki irtibatsızlık, bu kurumların herhangi bir merci tarafından ortak bir politika benimsenmesi bakımından yönlendirilmemesi, denetimsizlikten kaynaklanan keyfi ve hukuka aykırı uygulamalar gibi birtakım sıkıntılar mevcuttu. Bugünkü durum itibariyle, en azından yeknesaklığın sağlanması amacıyla atılmış bir adım olduğu unutulmamalıdır. Aslında mevcut durum itibariyle sorun, TİB'in varlığı değildir. Sorun, bu kurumu destekleyecek birtakım denetleme mekanizmalarının olmamasıdır.

5397 sayılı Kanunun yürürlüğe girmesiyle iletişimin denetlenmesine ilişkin tüm faaliyetlerin merkezi bir makam tarafından yürütülmesi hükme bağlanmıştır. TİB, bu bağlamda tüm istihbarat birimlerinin iletişimin denetlenmesine ilişkin uygulamalarını organize edecek ve denetleyecektir. Tek merkezlilik, toplanan bilgilerin kolayca tek merkezden öğrenilebilmesi ve kötüye kullanılması gibi birtakım riskler ihtiva ettiği iddia edilmekle birlikte, iletişimin denetlenmesine ilişkin işlemlerin tek elden yürütülmesi özellikle de keyfiliği önleme bakımından son derece önemli bir güvence olarak kabul edilmektedir[1373]. TİB'in varlığı dinleme ve tespit işlemlerinin sivil bir kurum tarafından yapılması gibi sivil ve demokratik sistem açısından çok yararlı olabilecek bir gelişme sayılmalıdır. Anılan kanunda önleme amaçlı bilgi elde etme işleminin sadece belirli nitelikteki örgütlü suçlar için öngörülmüş olması, gelecekte ortaya çıkma olasılığı olan bir tehlikenin aranması, etkin ve adil sivil bir denetim mekanizmasının getirilmesi, kayıt tutulması ve bu kayıtların muhafaza edilmesi ve gerektiğinde yok edilmesi gibi hususlarda ayrıntılı ve yeterli düzenlemeler getirilmesi keyfiliği önleyici mekanizmalar bakımından önemli verilerdir. Bu sistemin bir diğer yararı da, denetlemenin bir merkezden yapılması ile bir kişinin iletişiminin birden fazla istihbarat biriminin müdahalesine maruz kalması gibi birtakım tehlikeleri bertaraf edilmesidir[1374].

5397 sayılı Kanun ile 2559, 2803 ve 2937 sayılı Kanunlarda yapılan değişikliklerle telekomünikasyon yoluyla yapılan iletişime ilişkin tespit, dinleme, kayda alma ve sinyal bilgisi değerlendirilmesi şeklindeki işlemlerin tek merkez olarak İletişim Başkanlığı tarafından yürütüleceği açıkça vurgulanmıştır. Bu hükümler uyarınca hazırlanan

[1372] ERYILMAZ, s. 148.

[1373] KUNTER-YENİSEY-NUHOĞLU, s. 735.

[1374] ERYILMAZ, s. 148.

Yönetmeliğin Başkanlığın görevlerini düzenleyen 17. maddesinde Başkanlığın görevlerinden biri olarak da, Başkanlık faaliyetleriyle ilgili olarak kamu kurum ve kuruluşları, kamu hizmeti veren kuruluşlar ile işletmecilerden gelen her türlü bilgi, belge ve kayıtların bilgi güvenliği kriterlerine uygun olarak arşivlenmesini sağlamak olarak belirtilmiştir. Bu sebeple, yapılan tüm işlemlerin bir örneği ilgili kurumların yürüteceği işlemlerde bir aksama olmasının önlenmesi veya karşılaştırma-denetleme ihtiyacı bulunması amacıyla yasal sürelerle sınırlı kalmak üzere TİB'de saklanmaktadır.

3.5.4.TİB'in Faaliyetlerinin Denetlenmesi

Telekomünikasyon İletişim Bakanlığının kuruluş, görev ve yetkilerini düzenleyen ilgili Yönetmelikte Başkanlığın denetiminin hangi şekilde yapılacağı da düzenlenmiştir. Başkanlığın Yönetmelikte yer alan faaliyetlerle ilgili denetimi, Başbakanın özel olarak yetkilendireceği kişi veya komisyon tarafından yapılmaktadır. Emniyet Genel Müdürlüğünün, Yönetmelikte yer alan faaliyetlerle alakalı kendi birimlerindeki işlemlerine ilişkin denetimi; sıralı kurum amirleri, Emniyet Genel Müdürlüğü ve İçişleri Bakanlığının teftiş elemanları ile Başbakanın özel olarak yetkilendireceği kişi veya komisyon tarafından yapılmaktadır. Jandarma Genel Komutanlığının Yönetmelikte yer alan faaliyetlerle alakalı kendi birimlerindeki işlemlerine ilişkin denetimi; sıralı kurum amirleri, Jandarma Genel Komutanlığı ve İçişleri Bakanlığının teftiş elemanları ile Başbakanın özel olarak yetkilendireceği kişi veya komisyon tarafından yapılmaktadır. Milli İstihbarat Teşkilatı Müsteşarlığının Yönetmelikte yer alan faaliyetlerle alakalı kendi birimlerindeki işlemlerine ilişkin denetimi ise; sıralı kurum amirleri, Başbakanlık teftiş elemanları ve Başbakanın özel olarak yetkilendireceği kişi veya komisyon tarafından yapılacaktır[1375].

[1375] 10/11/2005 tarihli ve 25989 sayılı Yönetmelik, 17 madde, http://www.tib.gov.tr/detay.aspx?cid=22.

SONUÇ

Küreselleşme; başta ulaşım, iletişim ve ekonomi gibi alanlarda olmak üzere, hayatın birçok sahasını başkalaştırmıştır. Bu değişikliğe paralel olarak, suç oranları ve nitelikleri de küresel bir boyuta ulaşmış, özellikle organize suç örgütleri müthiş bir güç kazanmıştır. Son derece kompleks yapılı terörist ve organize suç örgütleri ile karşı karşıya kalan devletler de, bu düşmanlara karşı başarılı olabilmek için, geleneksel güvenlik yapılanmalarını yeni ve özel bazı usullerle kuvvetlendirmek lüzumunu hissetmişlerdir. Çünkü; teknolojik ve bilimsel gelişmeler, suçların takibi ve suçluların yakalanması bakımından da yeni kapılar açmakta, bilimsel bulgu ve tekniklerle, suçların önlenmesi, takibi ve faillerin cezalandırılması kolaylaşmaktadır.

Bununla birlikte, kişilerin özel hayatı, suçla mücadele etme çabası içinde olan devletlerin bu haklı mücadelesinden olumsuz bir şekilde etkilenmektedir. Gerçekten de, dijital çağ olarak da adlandırılan bu dönemde, 'yalnız bırakılma hakkı' olarak da adlandırılan özel hayat hakkının en önemli boyutlarından biri olan haberleşme hürriyeti, yasal ve yasadışı birçok yöntemle müdahaleye maruz kalmaktadır. Üstelik, bazı ülkeler, iletişime müdahaleyi uluslararası boyuta da taşımaktadırlar. ABD, Birleşik Krallık, Yeni Zelanda, Avustralya ve Kanada, birlikte kurdukları dev 'kulak'lar vasıtasıyla kişilerin özel hayatlarına uluslararası düzeyde müdahale etmekte, şifreli bazı sözleri telaffuz eden kişilerin diyalogları bu gizli denetim sistemine takılmaktadır. Gerçekten de, Echelon denilen bu sistemle, 'kill the president'(başkanı öldür), World Trade Center (Dünya Ticaret Merkezi) gibi takip edilmeyi hak eden ifadelerin yanı sıra Soros, Flame (Alev), Archives (arşivler), investigation (soruşturma), Bugs Bunny (çizgi film kahramanı bir tavşan), secure(emin, korunaklı), Lexis-Nexis gibi masum ve günlük hayatın birer parçası olan kelimeler de otomatik kayda alınmaktadır.

Suçla mücadele ile kişi hak ve hürriyetlerinin korunması arasındaki dengeyi korumaya çalışan devletler, suçluların yakalanmasında çok etkin bir rol oynayan iletişimin denetlenmesi tedbirini yasal bir zemine taşımış ve bu tedbiri sıkça kullanmaya başlamışlardır. Bununla birlikte, bazı yasal düzenlemelerin orantılı olmadığı, suçla mücadele gibi meşru bir kaygı ile başvurulan bu tedbirde, araçla amaç arasındaki dengenin korunamadığı iddia edilmektedir. Bu eleştiriler, gerek ABD hukukunda gerekse hukukumuzda dile getirilmekte olmasına rağmen, ABD hukukunda bu alanda varolan çatlakların çok daha derinleştiği, özellikle önleme amaçlı iletişimin

denetlenmesinde insan haklarını ihlal iddialarının ağır boyutlara ulaştığı ifade edilmektedir. AİHM'nin yargı yetkisini kabul eden Ülkemizde, bu denli ağır ihlallerin bulunmadığı söylenebilse de, gerek mevzuatın yeni kaleme alınmış olması, gerekse uygulamanın bu konuya yeterince vakıf olmamasından kaynaklanan birtakım problemlerin bulunduğu söylenebilir.

İletişim teknolojisi bakımından dünyanın en gelişmiş birkaç ülkesinden biri olan ABD'de, 70 milyon telefon kullanıcısının bulunduğu 60'lı yıllara kadar iletişimin denetlenmesini düzenleyen bir yasama çalışması bulunmamaktaydı. Bu konuda verilmiş mahkeme kararlarının bazıları, iletişimin denetlenmesinin ABD Anayasasının 4. maddesi kapsamına girmediğine karar verirken, bazıları da bu hakkın özel hayat hakkı kapsamına girdiğini vurguluyorlardı. 1967 yılında verilen Berger ve Katz kararları, iletişimin denetlenmesi alanındaki ilkeleri tespit ederek, bir yıl sonra çıkarılan Teknik Dinleme Kanunu'nun altyapısını oluşturma misyonunu yüklenmiş oldu.

Teknik Dinleme Kanunu, iletişimin yasal olarak denetlenmesine imkan tanıyan, bireylerin iletişime müdahalelerini yasaklarken kolluk kuvvetlerinin Anayasal denetimine yetki veren ve iletişimin yasal denetlenmesi dışındaki tüm diğer müdahaleleri yasadışı ilan eden ilk spesifik kanun olmuştur. Bu kanun, çıkarıldığı tarihe kadar yasadışı yöntemlerle yapılan iletişime müdahaleyi yasal bir zemine oturtmuş ve Anayasal kontrol mekanizmalarını başlatarak keyfiliğin sona erdirilmesi sürecini tetiklemiştir. Özel hayatın korunması ile kolluk görevinin ifası arasında bir denge kurmayı amaçlayan Kanun; iletişimin mahremiyetinin korunmasını sağlarken, iletişimin denetlenmesine ilişkin yeknesak şartları da belirlemiştir. Söz konusu karardaki eleştiriler dikkate alınarak hazırlanan Teknik Dinleme Kanunu'nda yer alan temel prensipler, güncel kanunlarda yer alan ilkelere ışık tutar niteliktedir. Bu ilkelerden bazıları şunlardır.

- Sadece kanunla belirlenmiş suçlar hakkında yapılacak soruşturmalarda bu tedbire başvurulabilir (Hususilik ilkesi-Particularity requirement).

- Kullanılabilecek başka soruşturma yöntemlerinin varlığı halinde iletişimin denetlenmesi yöntemlerine başvurulmamalıdır. (Son çare ilkesi-Exhaustion requirement).

- İletişimin denetlenebilmesi tedbirine başvurulabilemesi için yeterli ve makul sebeplerin varlığı, olmazsa olmaz bir şarttır (Makul sebep ilkesi-Probable cause requirement).

• Hakkında iletişimin denetlenmesi kararı verilmiş kişinin suç unsuru ihtiva etmeyen konuşmalarının kayda alınması en aza indirgenmelidir. (En aza indirgeme ilkesi-Minimization requirement).

• Şartları oluşmadığı halde verilen bir iletişimin denetlenmesi tedbiri ile elde edilen deliller yargı sürecinde kullanılamaz.(Delil Yasağı ilkesi-Exclusion principle)

İletişimin içeriğinin denetlenmesine ilişkin hükümler ihtiva eden Teknik Dinleme Kanunu'ndan farklı olarak iletişim bilgilerinin tespiti hakkında düzenleme yapan Numara ve Rota Tespit Kanunu, Teknik Dinleme Kanunu ve Dış Güvenlik İstihbarat Kanunu'na (FISA) kıyasla daha ılımlı hükümler içermektedir. İçerik dışı bilgilerin anayasal koruma altında olmadığına karar veren Yüksek Mahkeme'ye tepki gösteren Kongre, 1968 tarihli Teknik Dinleme Kanunu'nda öngörülmemiş olan bu alanı düzenleyerek yasal bir boşluğu doldurmuştur. 1978 tarihli FISA ise, işlenmiş bir suçla ilgili delil elde etmeyi amaçlayan 1968 tarihli Teknik Dinleme Kanunu'ndan farklı olarak, yabancı istihbarat bilgisine ulaşmayı hedefleyen 'önleyici' bir kanundur. İletişimin denetlenmesi ile ilgili birtakım özel usulleri kapsayan bu kanun yüksek düzeyde gizlilik içeren bir tarzda çalışmaktadır. Bu kanun, yabancı istihbarat ve karşı istihbarat elde etmek amacına matuf olduğundan dolayı, hak ve hürriyetlerin korunması amacıyla 1968 tarihli Teknik Dinleme Kanununa dercedilen birtakım güvenceleri kapsamamaktadır. Teknik Dinleme Kanunu gibi içeriğe ilişkin müdahaleyi düzenleyen FISA, milli güvenliğe ilişkin suçlarda iletişimin denetlenmesi imkanını kullanabilmek bakımından gerekli olan yetki ve prosedürün belirlenmesi için çıkarılmıştır. Önleyici nitelikli bu tedbirin hayata geçirilmesi için mahkeme kararının öngörülmesi, hürriyetlerin korunması bakımından önemlidir. Bu kanunla ayrıca, tedbirin hukukiliğini denetleyen FISA mahkemesi kurulmuştur. Mahkemenin amacı, milli güvenliğe ilişkin suçlarda arama ve iletişimin denetlenmesi tedbirlerinin kullanılmasına ilişkin hükümet yetkilerinin denetlenmesi ve bu yetkilere makul sınırlar getirilmesidir. Kanun kapsamında, makul sebep ilkesi, hakimin kontrol edebileceği bir şart olmaktan çıkarılmış olup, bu şartın varlığını teyit eden Hükümet yetkilisinin beyanı yeterli sayılmaktadır. Bu tedbirin son çare olarak görülmemesi bir diğer eleştirilen nokta olsa da, FISA çerçevesinde bir mahkeme kararı verilebilmesi için en aza indirgeme ilkesi (minimization procedures) olarak adlandırılan kurala riayet edilmesi olumlu bir noktadır.

Bu temel yasalardaki birçok hükümde değişiklik getiren, yürütme gücüne diğer erklerden daha fazla yetki tanıyan Patriot Kanunu, ABD'de her şeyin bir anda değişmesine neden olmuştur. her şeyden önce adından dolayı eleştirilen bu kanun,

yargının yetkisini sınırlamak ve yürütmenin gücüne güç katmakla itham edilmiştir. Bu kanunun, yürütme gücü ile sivil haklar arasındaki dengeyi, yürütmenin lehine bozduğu iddia edilmektedir. Gerçekten de, ABD'de, hakların ve hürriyetlerin korunması bakımından çok iyi bir dönemde yaşanılmadığı herkesin malumudur.

Başta Teknik Dinleme Kanunu olmak üzere tüm yasal hükümler, özel hayatın ihlalini olabildiğince azaltmaya çalışan bir anlayış üzerine kurulmuş olmasına rağmen, zaman içinde belli bazı hükümler ve kurumlar yıpranmaya başlamıştır. Kanun koyucunun Berger kararındaki tespitlerden yola çıkarak belirlediği ilkeler bir bir zayıflamaktadır. Nitekim, Teknik Dinleme Kanunu'nun ilk olarak kanunlaştırıldığı tarihte, kapsamı dar tutma çabasının bir göstegesi olarak çoğunlukla organize suçlarla mücadeleye hasredilen bu tedbir, bugün çok basit suçlara bile uygulanır hale gelmiştir. Mevcut durum itibariyle; 1 yıldan fazla hapsi gerektiren suçların soruşturulmasında iletişimin denetlenmesine başvurulması, özel hayat bakımından ciddi bir risk oluşturmaktadır.

2001 yılında çıkarılan Patriot Kanunu tarafından getirilen hükümlerle, iletişimin denetlenmesi tedbirinin daha yaygınlaştığı, mahkemelerin kontrol yetkisinin azaltıldığı, İnternetin daha rahat takibe alındığı, İnternet servis sağlayıcılarının içerik dışı abone bilgilerini mahkeme kararı olmaksızın kolluk güçlerine verdiği, yapılan yeni terörizm tanımıyla daha çok kişinin iletişiminin denetlendiği ve ABD'nin yabancı istihbarat servislerinin artık daha fazla vatandaşı takibe aldığı iddia edilmektedir. NSL denilen Milli Güvenlik Mektupları vasıtasıyla, milli güvenlikle ilgili konularda bir yargı organının denetimini olmaksızın bilgi edinilebilmektedir. Bu tür hassas ve suiistimale açık bir tedbiri daha da ağırlaştırılan husus, tedbire muhatap olan kişiler hakkında, konuşma ve açıklama yasaklarının (gag order) konulmasıdır.

ABD'de iletişimin denetlenmesi bakımından durumu ağırlaştıran bir diğer faktör de son çare ilkesinin örtülü olarak gözardı edilmesidir. İletişimin denetlenmesine yönelik bir talep esnasında, kolluk görevlisinin, teknik takip dışındaki diğer yöntemlerin kullanılmasının zor olduğu şeklindeki beyanı bile, mahkemece yeterli görülmektedir. Gerçekten de bazı mahkemeler, iletişimin denetlenmesi dışındaki tüm diğer çareler denenmemiş olsa bile, iletişimin denetlenmesine ilişkin karar verebilmektedirler. Mahkemelere ilişkin bir diğer eleştiri de, bu kurumların, iletişimin denetlenmesi ile ilgili taleplerde filtreleme fonksiyonlarını gerektiği kadar yerine getirmemeleri ve sadece bir tasdik (rubber stamp) makamı olarak görev yapmaları hakkındadır. Nitekim, 1989 ile 1995 yıları arasında gerek eyalet gerekse federal düzeyde yapılan iletişimin denetlenmesi başvurularının hemen hepsi olumlu yanıt bulmuştur. Benzer şekilde,

FISA mahkemesine 1979 ile 2003 yılları arasında yapılan 16 450 başvurudan sadece 3 tanesi reddedilmiştir. Kontrol yetkisini kaybeden mahkemeler, ne gelirse onaylayan makamlar gibi algılanmaktadırlar. Hükümet yetkilileri mevcut durumu kendi profesyonellikleri ile açıklasalar da, bu husus tartışmalı bir durum olarak durmaya devam etmektedir. Bu tür bir filtreleme eksikliğinin yanısıra, usulüne uygun bir şekilde elde edilmeyen delilin kullanılmasına örtülü olarak izin verilmesinin de uygulamada karşılaşılan problemlerden olduğu iddia edilmektedir. Bu durum, ABD adalet mekanizmasının, şüphelinin itham edilmesi ile ilgili olarak elde edilen bilgileri her ne şekilde elde edilirse edilsin kullanmak istemesi olarak yorumlanmaktadır. Öte yandan, ABD'de her geçen gün biraz daha artan bir düzeyde, mahkeme dışı (extrajudicial) inisiyatiflere girişildiği iddia edilmektedir. Terörizmle ilgili soruşturmaya muhatap kişiler hakkında susma kararı (gag order) çıkarılmasının yasallaştırılması, üstelik bu tür uygulamaların Patriot Kanunu ile uygulamaya geçirilmesi eleştiri almaktadır. Oysa ki bu kanun, acele olarak hazırlanmış ve Kongre ve Senato'da yeterli bir düzeyde tartışılmamış hatta birçok milletvekili tarafından okunmamış bir metin olarak görülmektedir.

Bütün bunların yanısıra, Patriot Kanunu ile verilen güçlü yetkiler de kolluk güçlerini tatmin etmemektedir. Yetkilerinin iyice artırılmasını talep eden kolluk görevlileri, mahkeme kararı olmaksızın iletişimin denetlemesine imkan tanıyan yeni yetkiler talep etmektedirler. Bu bağlamda, Başkana, "Silahlı Kuvvetleri Kullanma Yetkisi" çerçevesinde, ABD'yi tehdit eden terörist faaliyetleri engellemek amacıyla, ilgili mevzuatı bertaraf ederek olağanüstü yetkiler kullanma imkanının verildiği hükümet tarafından savunulmaktadır. Bütün bu olaylar, ABD'deki mevzuatın sadece gerektiğinde başvurulan metinler olduğu şüphesini akla getirmektedir.

İletişimin denetlenmesi hususunda oldukça farklı ve tartışmaya açık bir durumda olan ABD hukukunun aksine, AİHM, sistemini oturtmuş ve olup biteni uzaktan denetleyen bir mahkeme olarak görev yapmaktadır. AİHM, iletişim kavramını belli bir iletişim aracı belirtmek suretiyle daraltmak yerine, geniş bir bakış açısı kabul etmek şeklinde bir tercih yapmıştır. Mahkeme, tedbire konu olacak iletişim araçlarının ilgili devletin ulusal düzenlemesi ile belirlenmesi gerektiğini belirtmiş ve konuyu ilgili devletin takdir hakkına havale etmiştir. Özel hayat hakkının sınırlandırılması ile ilgili olarak AİHS tarafından belirlenen 'müdahalenin yasayla öngörülmesi, müdahalenin meşru bir amaç için yapılması ve müdahalenin demokratik bir toplumda gerekli olması' kriterlerini

uygulamadaki ihtiyaçlar doğrultusunda yorumlayan AİHM, birtakım yeni kriterler belirlemiştir. Bu kriterler;

- İletişimin denetlenmesine konu suç ve insan kategorilerinin belirlenmesi,
- İletişimin denetlenmesine son çare olarak başvurulması,
- İletişimin denetlenmesine ilişkin sürenin belirlenmesi,
- İletişimin denetlenmesinden elde edilen verilerin korunması ve şartlar oluştuğunda yok edilmesi,
- İletişimin denetlenmesinin etkin bir denetim sistemiyle kontrol edilmesi,
- İletişimin denetlenmesi tedbirine muhatap kişiye şartları oluştuğunda bildirimde bulunulması,
- İletişimin denetlenmesine, yetkili merci tarafından karar verilmesi,

Olarak sayılabilir.

Hukuk mantığı ve uygulaması itibariyle, bir asırdan daha fazla bir süreden beri Avrupa perspektifini benimsemiş olan Türkiye, mevzuat ve uygulamasını AİHM kriterlerine göre yeniden belirleme çabası içindedir. Bu bağlamda, suçla mücadelede etkili bir koruma tedbiri olan iletişimin denetlenmesi, 5271 sayılı CMK'nın 135 ila 138. maddelerinde detaylı ve açık olarak düzenlenmiştir. CMK'nın 135. maddesinin 7. fıkrasında, bu madde hükümleri dışında başka bir şekilde iletişimin denetlenmesinin uygulanamayacağı açık şekilde ifade edilmiştir. Bu kanunda düzenlenen iletişimin denetlenmesi tedbiri adli amaçlı olarak sadece bir suç işlendikten sonra başka yollarla ulaşılamayan delillerin elde edilmesi amacıyla başvurulabilecek bir tedbir olarak yer almıştır. Önleme amaçlı iletişimin denetlenmesi hükümleri de, 5397 sayılı Kanun'da yer almaktadır. Adli amaçlı iletişimin denetlenmesi, işlenmiş olan bir suç hakkında delil elde etme amacına hasredilmişken, önleme amaçlı iletişimin denetlenmesi ise henüz işlenmemiş ancak işlenebileceğine dair şüphenin olması halinde başvurulacak bir tedbirdir.

CMK öncesinde, yani, bu tedbirin kıyas ya da yorumla uygulandığı dönemlerdeki mevzuat ve uygulamamızın AİHS ve AİHM kriterlerine uygun olmadığı bir gerçekti. Bugünse artık, gerek Sözleşme gerekse Mahkeme kriterlerine uygun mevzuat marifetiyle iletişimin denetlenmesi tedbiri hayata geçirilmektedir. CMK ile getirilen

sistemin, ana hatları itibariyle, AİHM kriterlerine uygunluk sağladığı söylenebilir. Verilen takdir hakkının orantılılık ilkesi çerçevesinde kullanıldığı, her suçun bu tedbir kapsamına alınmaması suretiyle birey merkezli ve insan haklarını koruma kaygısı taşıyan düzenlemelere yer verildiği, bu tür tedbirlere başvurabilmek için kuvvetli şüphe kriterinin arandığı, bir suçla ilişkisi olduğu düşünülen tüm bireylerle ilgili toplu izinlerin verilmesine imkan sağlayan düzenlemelerden kaçınıldığı ve ancak şüpheli veya bu kişiyle bağlantısı olduğu tahmin edilen kişiler hakkında bu tedbire başvurulabildiği görülmektedir. Önleme amaçlı iletişimin denetlenmesini düzenleyen 5397 sayılı Kanunda da, amaç, uygulanacak tedbir türleri, tedbirin uygulanma süresi, tedbirin uygulanmasına karar verecek mercii ve karar verme prosedürü, iletişimin denetlenme süresi ve bu sürenin uzatılma şartları, denetimle ilgili düzenleme, kayıtların imhası gibi hususların AİHM standartlarına uygunluk gösterdiği söylenebilir.

Haberleşme hürriyetinin ancak kanunla sınırlandırılabilmesi kuralını karşılaması bakımından CMK ve 5397 sayılı yasalardaki hükümler olumludur. Bununla birlikte, iletişimin denetlenmesi ile ilgili hususları düzenleyen bir kanunun var olması yalnız başına yeterli olmamaktadır. Nitekim, AİHM, Huvig ve Kruslin kararlarında, Fransa'yı, iletişimin denetlenmesine imkan tanıyan bir yasa bulunmadığı için değil, varolan yasa suiistimalleri önleyecek kalitede ve açıklıkta olmadığı için mahkum etmiştir. Bu bağlamda, önleyici denetimle ilgili olarak bir başvurunun AİHM önüne gelmesi halinde, Mahkemenin özellikle denetim bakımından Ülkemizi mahkum etme ihtimalinin bulunduğunu düşünüyoruz. Nitekim, denetimle ilgili ilkelerin belirlendiği Klass-Almanya davasında AİHM, Almanya'daki sistemin denetim bakımından gerekli güvenceleri içerip içermediğini tartışmıştır. Benzer bir olayda, Ülkemiz aleyhine Strasbourg'a taşınacak bir davada denetim sisteminin eksikliği bir ihlale neden olabilecektir.

Adli ve önleme amaçlı iletişimin denetlenmesi alanlarında mevzuat ve uygulamamızda atılan adımların değerlendirilmesi yapıldığında, aşağıdaki sonuçlara varmak mümkündür:

- Türk hukukunda iletişimin denetlenmesi tedbirine karar verme yetkisinin mahkemelere verilmiş olması, tedbire muhatap kişiler bakımından yeterli bir garanti sayılamaz. Bu merciin vereceği kararın kalitesi de önem arzetmektedir. AİHM, yasanın varlığını yetersiz görüp, yasanın kalitesinin de önemli olduğunu vurguladığı gibi, mahkeme kararının da belli bir kaliteye sahip olmasının gerekliliğine işaret etmektedir. Bu itibarla AİHM, kararların gerekçeli olmasını, istismarı ve keyfiliği önleyici bir güvence olarak görmektedir. Kararı verecek olan hâkimi, konu üzerinde daha ciddi düşünmeye

sevk etmek gibi önemli bir fonksiyon ifa eden gerekçelendirme, verilen kararların denetlenmeye açık bir hüviyet kazanması ve tedbirin uygulanma sebebinin ilgililerce net olarak anlaşılabilmesi gibi faydalar sağlayacaktır. Hususilik ilkesi olarak da nitelendirebileceğimiz bu yaklaşım marifetiyle, genel bilgi avcılığı amacına yönelik tedbirlerin uygulanması engellenmiş olacaktır. Gerçekten de, kararların gerekçelendirilmesinde görülen yetersizlik, özellikle AİHM önüne getirilen başvurulan bakımından çok eleştiri aldığımız bir husustur. Mahkeme, kararların gerekçeli olmamasını daha doğru bir ifadeyle gerekçenin yetersiz oluşunu eleştiri konusu yapmaktadır. Bu bağlamda, iletişimin denetlenmesi talebini değerlendirecek merci, yasal şartların varlığı hususunda yeterli bir araştırma yaptıktan sonra ve somut olayın özellikleri çerçevesinde gerekçeli olarak karar vermelidir. Mahkeme bu anlamda bir tasdik makamı olmaktan çıkarılmalı, şartları oluşmamış tedbir taleplerini reddetmelidir. Bu çerçevede değerlendirilmeden verilmiş bir mahkeme kararının hukuka aykırı olduğu izahtan varestedir. Bununla birlikte, uygulamada iletişimin denetlenmesi talepleriyle ilgili kararların yeterince değerlendirme yapılmadan verildiği, suçun işlenmesinin hemen sonrasında, daha birincil nitelikteki deliller ve soruşturma teknikleri kullanılmadan, başka bir ifadeyle son çare ilkesi dikkate alınmadan bu tedbire başvurulduğu bilinmektedir. Bu şekilde verilen hukuka aykırı kararlara karşı özel bir tazminat yolu öngörülmemiş olmakla birlikte, hakkında tedbir uygulanan kişinin genel hükümlere göre tazminat hakkını kullanması durumunda, kararda imzası bulunanların sorumlu olacakları şüphesizdir. Bu tedbirin en çok eleştirilen yönü olan denetim eksikliğinin kanun koyucu tarafından ikmal edilmesi halinde, örneğin ABD hukukunda olduğu gibi ilgiliye, yasama organına, üst düzey yargı organlarına ve Adalet Bakanlığına denetim yetkisi verilmesi gündeme gelecektir. Bu konudaki kararların daha sağlıklı olmasının sağlanması bakımından, haksız tedbire hükmeden karar nedeniyle tazminat ödenmesi halinde, kararı veren merciye rücu edilmesi gündeme gelebilecektir.

- Son çare olarak başvurulması gerekli olan iletişimin denetlenmesi tedbiri, uygulamada olması gerekenden daha erken başvurulan bir koruma tedbiri olarak karşımıza çıkmaktadır. Ülkemizde, diğer normal soruşturma teknikleri tüketilmeden bu 'sıra dışı' yola başvurulmakta, suç konusu olayın hemen sonrasında bu tedbir devreye konulmaktadır. İletişimin denetlenmesi tedbirinin bir son çare olarak kullanılması, sıkı sıkıya uyulması gerekli olan bir şart olarak algılanmalıdır. İletişimin denetlenmesi tedbirinin kullanılacağı vaka sayısını ve mahremiyete yönelik riskleri en aza indirgemeyi hedefleyen bu ilkeyi, AİHM, uygulayıcıların keyfi birtakım uygulamalara yeltenmesinin önlenmesi bakımından da önemli görmektedir.

- İletişimin denetlenmesine ilişkin mevzuatımızın yer yer boşluklar içerdiği görülmektedir. Temel hak ve özgürlüklere müdahale niteliği taşıyan bu tedbirlerin açık ve net düzenlemeler içermesi gerektiği dikkate alındığında, CMK'nın 135/2. maddesinin olması gereken bir şekilde kaleme alınmadığı görülmektedir. Maddenin sadece şüpheli ve sanığı kapsayacak şekilde kaleme alınmış olması, hakkında iletişimin denetlenmesi tedbiri uygulanabilecek diğer muhtemel kişiler hakkında düzenleme yapılmamış olması bir eksikliktir. Aslında, bu gibi eksiklikler, AİHM tarafından belirlenmiş, açıklık ve öngörülebilirlik kriterlerinin ihlali anlamına gelmektedir. Bu itibarla, muhtemel müdahalelerin niteliği, kapsamı, bu tedbirlerin emredilmesi için gerekli sebepler, emri vermeye yetkili merci, uygulayan ve denetleyen birimler, izlenecek usul gibi hususlar da kanunda ayrıntılı olarak düzenlenmelidir. Maddenin, bu haliyle, ilgiliye öngörülebilirlik (foreseebility) imkanı tanımaktan da uzak olduğu söylenebilir. Bu bağlamda, iletişimin denetlenmesi tedbirinin hangi evrelere ilişkin olduğunun açıklanması, kovuşturma aşamasındaki boyutunun da izah edilmesi gerekir. Diğer taraftan; hükümlü, müşteki, tanık, kamu görevlileri, milletvekilleri vb. kişilerin durumları hakkında açıklık içeren bir değişiklik yapılması, kanunun belli noktalarda detaycı bir yöntem belirlemesi, hak ve hürriyetlerin keyfi müdahalelere maruz kalmaması bakımından yararlı olacaktır.

- Mevzuatta müdafiin iletişiminin denetlenmesi konusunda da boşluk bulunmaktadır. Öğretide, mevcut düzenleme ile getirilen sınırlamaların belirli yerdeki telekomünikasyon araçları açısından olduğu belirtilerek, aracın türü açısından bir sınırlama bulunmadığı; müdafiin konutu, işyeri ve bürosunda olmak şartıyla, mobil telekomünikasyon araçları ile yapılan iletişimin de denetlenebileceği ifade edilmektedir. Kanaatimizce, 136. maddede yer alan düzenlemede kastedilen her türlü iletişim vasıtasıdır. Bu madde, müdafii ile müvekkili arasındaki ilişkiyi takipten bağışık kılmak amacıyla kaleme alındığından, mobil telefonun bağışıklık kapsamından çıkarılması doğru olmayacaktır. Kanun koyucunun amacının, bu kişilere mesleklerinin özelliğinden kaynaklanan bir koruma sağlamak olduğu kabul edildiğinde, bu korumadan mobil telefonu çıkarmak hayatın gerçekleriyle uyuşmayacaktır. Nitekim, günümüz dünyasında müdafii sıfatını da ihraz edebilecek durumda olan avukatlar, konuşmalarının çok önemli bir bölümünü mobil telefonları vasıtasıyla yapmaktadırlar.

- 5397 sayılı kanunda, "Bu maddede belirtilen işlemler ile 5271 sayılı Kanunun 135 inci maddesi kapsamında yapılacak dinlemeler, Telekomünikasyon İletişim Başkanlığı adıyla kurulan tek bir merkezden yürütülür." denilmektedir. Anılan maddede yer alan "5271 sayılı Kanunun 135. maddesi kapsamında yapılacak dinlemeler"

ifadesindeki “dinlemeler” kelimesinin “işlemler” olarak düzeltilmesi gerekmektedir. Nitekim, dinleme iletişimin denetlenmesi kavramının sadece bir parçasını oluşturmaktadır. İşlemler kelimesi ise, iletişimin tespit edilmesi, dinlenmesi, sinyal bilgilerinin değerlendirilmesi ve kayda alınmasını kapsamaktadır. Yine iletişimin denetlenmesine soruşturma ve kovuşturma aşamasında karar verileceği belirtilmiş olması ve bu kapsamda madde içeriğinde “şüpheli” ve “sanık” kavramlarına yer verilmesine karşın; kararı verecek makam olarak yalnızca “hakim “ ve “Cumhuriyet savcısının” belirtilmesi ve özellikle kovuşturma aşamasında karar vermeğe yetkili olabilecek “mahkeme” terimine yer verilmemiş olması isabetli değildir. Bu nedenle yapılacak ek bir düzenlemeyle kararı verecek makamlara “mahkeme” kavramı da eklenmelidir.

- Türk hukuku bakımından önleme amaçlı iletişimin denetlenmesine konu olan suçların tespiti bakımından katalog belirlenmesinin yararlı olup olmayacağı tartışma konusudur. Geniş bir suç listesi bakımından bu tedbire başvurulabilmesi, başka bir deyişle, geniş ve soyut nitelikteki bir suç listesinin öngörülmüş olması, bu tedbiri tartışmalı hale getirmektedir. Gerçekten de, iletişimin denetlenmesi tedbiri kişinin özel hayatı bakımından ciddi tehlikeler içermekte, diğer bazı koruma tedbirlerinden farklı olarak devamlılık arz etmekte, sadece belli bir alandaki delillerin değil iletişimin her türlü kapsamının tedbir kapsamına girmesi gibi sakıncalar taşımaktadır. Bundan dolayı özel hayata bu denli müdahaleyi kapsayan bu tedbirin, adli amaçlı iletişimin denetlenmesinde olduğu gibi bir kataloğa tabi tutulması faydalı olacaktır.

- İletişimin denetlenmesinde olduğu gibi denetleme sonucu elde edilen verilerin kullanılmasında da denetleme amacına uygun hareket edilmeli, elde edilen bilgiler, işlenmiş suçun kanıtlanması dışında başka bir amaçla kullanılmamalıdır. Elde edilen delillerin, gerekli olan koşullara uygun hareket edilmesi şartıyla, her türlü suçun yargılaması için kullanılabilmesi gerektiği düşüncesine katılmak mümkün değildir. Katalog suçlarla ilgili olarak başlanan tedbirle elde edilen delillerin her türlü soruşturma ve kovuşturma kapsamında kullanılması, haberleşme özgürlüğünün ve gizliliğinin özünün yok edilmesine yol açacaktır. Çünkü kanun koyucu, bu tedbire sadece belli suçların aydınlatılması amacıyla izin vermiştir. Olağanüstü bir nitelik taşıyan, diğer delillerden bir yarar elde edilemediğinde başvurulan, başka bir ifadeyle son çare olarak görülen bu tedbirden ikincil bir mahiyette yararlanılmasına izin verilmesi, kanaatimizce, devletin bireyle yaptığı sözleşmenin ihlali anlamına gelir. Devletin yaptığı sözleşme ifadesinden kasıt şudur ki, devlet, ancak belli suçlarda bu tedbire başvurulabileceğini

yaptığı kanunlarla deklare etmiştir. Bu deklarasyon sonucunda elde edilen bilgilerin başka soruşturma ya da işlemlerde kullanılmasına izin vermek ahde vefa ve 'öngörülebilirlik' ilkelerine aykırı bir tutum olur. Bir nevi 'örtülü af' ya da 'kovuşturma bağışıklığı' olarak ifade edilebilecek olan bu sistem, ABD'de uygulanan dava pazarlığı (plea bargaining) uygulamasıyla benzer bir mantığa sahiptir. Benzer bir diğer örnek de, Suçluların İadesine Dair Avrupa Sözleşmesinde varolan 'Hususilik Kuralı'dır. Anılan Sözleşmenin 14. maddesinin 1. paragrafında 'İade edilen şahıs iadeden evvel işlediği ve iadeye esas olandan başka bir fiilden dolayı takip veya muhakeme edilemeyeceği gibi bir ceza veya emniyet tedbirinin infazı için tevkif edilemez ve kezalik herhangi bir surette hürriyeti kısıtlanamaz' ifadesi yer almaktadır. Hususilik kuralı, iade edilen kişiye tanınmış bir nevi ayrıcalıktır. İade edilen kişi böylece sadece iadeye konu olan suçtan dolayı takibat altına girmekte, bu suçtan daha önce işlediği suç ya da suçları açısından bir tür takipsizlik garantisi elde etmektedir.

- Kanun koyucu, hangi araçlarla yapılan iletişimin denetlenebileceğini açıkça saymamak suretiyle telekomünikasyon aracı olarak nitelendirilebilecek mevcut ve gelecekte ortaya çıkacak tüm iletişim araçlarını bu kapsama dahil etmek istemiştir. Nitekim yönetmelikte de bu üslup korunmuştur. Hukuk ve iletişimin iç içe geçtiği bir alan olan iletişimin denetlenmesi ile ilgili bir yönetmelikte böyle bir üslubun tercih edilmesi de hak ve hürriyetlerin korunması bağlamında doğru olmayacaktır. İletişim teknolojisinin on yıl sonra ulaşacağı yer bugünden kestirilemese de, bundan on yıl geriye bakıldığında karşımıza çıkan tablo gelecek adına bizlere bir fikir vermektedir. Gerçekten de, bugün böyle bir tasarrufta bulunmak, yarın teknolojinin çok daha gelişeceği günlerde, mutlak surette müdahaleden uzak tutulması gerekli olan birtakım iletişim vasıtalarının da bu kapsama alınması anlamına gelir. Bu cümleden olarak, bugünü kuşatacak bir üslubun belirlenmesi, ihtiyaçlar yeni bir düzenlemeyi gerektirdiğinde de yeni bir çalışmaya gidilmesi uygun olacaktır.

- Ülkemiz mevzuatı bakımından, iletişimin denetlenmesi ile ilgili olarak karşımıza çıkan en önemli problem, tedbirin hukukiliğininin gereği gibi denetlenememesidir. Gerek adli, gerekse önleme amaçlı iletişimin denetlenmesi işlemlerinin gizli olarak uygulanması nedeniyle, denetleme işleminin devam ettiği süre zarfında ilgilinin bu işlemden haberdar olması, işlemin doğası itibariyle mümkün değildir. İlgili kişi, bildirim sonrasında, kendisi ile ilgili olarak uygulanan tedbir hakkında bilgi sahibi olduğu zaman bu tedbir uygulanmış ve bitmiş olacaktır. Bu itibarla, kişinin yargı önündeki çabası sadece tazminat boyutu itibariyle ortaya çıkabilir. Mevcut mevzuat itibariyle de, sadece

iletişimin denetlenmesi tedbirinden mağdur olmuş kişiler için öngörülmüş bir tazminat yolunun olmadığı da herkesin malumudur. Bu kapsamda, iletişimin denetlenmesi tedbirinden mağdur olmuş kişilere mahsus bir tazminat talep hakkının tanınması yerinde olacaktır. Öte yandan, iletişimin denetlenmesi tedbirinin gerek hukuka uygunluk, gerekse teknik boyutlarıyla kontrolunün birkaç farklı birim tarafından üstlenilmesi; şeffaflığı, şeffaflık da hak ihlallerinin azaltılmasını sağlayacaktır. Uygulamada, TİB, önleyici denetleme anlamında sadece bir tasdik makamı olarak görev yapmakta, verilen mahkeme kararlarına itiraz edememekte, dolayısıyla merkezi bir makam fonksiyonunu eda edememektedir. TİB'e bu anlamda yetki verilmesi ile, bu tedbir ülke genelinde yeknesak bir şekilde uygulanabilecektir. Öte yandan bu süreç, denetim ve teftiş aşamalarının sağlıklı işletilmesiyle yürütülebilecektir. Özellikle Başbakanlık, İçişleri ve Adalet Bakanlıkları Teftiş Kurullarının bu boyutta önemli sorumlulukları olmalıdır. Diğer yandan, önleme amaçlı denetleme kararlarını çıkaran özel yetkili mahkemelerin konuya özen göstermesi de önemlidir.

Tedbirin denetlenmesi ile ilgili eksiklikler giderilmeden, önleyici denetimle ilgili olarak bir başvurunun AİHM önüne gelmesi halinde, Ülkemiz aleyhine bir ihlal kararı verilmesi kuvvetle muhtemeldir. Nitekim, denetimle ilgili ilkelerin belirlendiği Klass-Almanya davasında AİHM, Almanya'daki sistemin denetim bakımından gerekli güvenceleri içerip içermediğini tartışmıştır. Mahiyeti itibariyle gizli olan bu tedbiri denetleyecek ve vatandaşa koruma getirecek bir sistemin kurulması devletin pozitif sorumluluğunun doğal bir sonucudur.

İletişimin denetlenmesinin çok etkin kullanıldığı ABD'de, denetim sistemi bir değil birden fazla yöntemle yapılmaktadır. ABD hukukunda var olan denetim sistemlerinin ne kadar sağlıklı çalıştığı tartışmaya açık olmakla birlikte, bu ülke sisteminin birikiminden yararlanılarak, keyfi uygulamaları önleme ve hak ve hürriyetleri koruma amaçlı yeni birtakım uygulamaların ülkemize ithal edilmesinin uygun olacağını düşünmekteyiz. ABD sistemi bir bütün olarak incelendiğinde, kişilerin bireysel şikayet hakkının yanı sıra, birçok denetim mekanizmasının düzenlendiği görülmektedir. Yasama denetimi, yargının hem kendini hem de denetleme sürecini kontrol edecek şekilde sürece katılması gibi uygulamalar; bilginin gerek parlamento gerekse yayınlanan raporlar marifetiyle kamuoyu ile paylaşılmasını sağlayan kurumlar olarak gözükmektedir. Bu denetim sistemlerinin sağladığı şeffaflık hem tedbire muhatap olan kişiye bir güven hissi vermekte, hem de uygulayıcıların keyfi olarak nitelendirilebilecek uygulamalara tevessül etmesi engellenmiş olmaktadır. AİHM'nin, birinci ve ikinci

aşamalar olarak nitelendirdiği denetimin başlatılması ve sürdürülmesi aşamalarında, bireyin bilgi eksikliği nedeniyle içinde bulunduğu zayıflığın devletin atacağı adımlarla telafi edilmesi gerekir. Aksinin kabulü, hukuk devletinden uzaklaşma anlamına gelecektir.

- Hak ve hürriyetlerin korunması ile suçla mücadele arasındaki hassas dengenin hak ve hürriyetler lehine bozulması suçla mücadeleyi sekteye uğratacak, bu dengenin suçla mücadele lehine bozulması ise telafisi olmayan müdahelelerin artmasına neden olacaktır. Bu anlamda, atılması gereken adımlardan en önemlisi, genel nitelikli tedbirlerin mutlak surette önlenmesidir. Herkesin şüpheli olarak görülmesi paranoyasından kaynaklanan genel nitelikli tedbirler, hem AİHM hem de diğer demokratik hukuk düzenleri tarafından reddedilmektedir. Gerçekten de, Klass kararıyla kabul edilemez bulunan genel nitelikli tedbirlerle, kanunlara bağlı masum insanların özel hayatları çiğnenmekte ve kişinin 'kendisine bırakılmasını istediği bir alan' olan özel hayatına müdahale edilmektedir. Yalnız bırakılma hakkı olarak tanımlanan özel hayat hakkı, etkin tedbirler alınmadığı takdirde, uygulaması mümkün olmayan bir hak haline dönüşecektir. Özel hayatı hiçe sayan tedbirlere yeşil ışık yakılması, artık hiç kimsenin kendisine sakladığı bir gizli alanının olamayacağı anlamına gelmektedir. Oysa ki herkes tabiatı itibariyle, başkalarıyla paylaşmak istemediği şeylerin gizli kulaklara malzeme yapılmasından rahatsız olmaktadır. Her ne kadar, bazı sözde demokratik ülkelerde, bu ülkelerin taraf oldukları uluslararası sözleşmeleri hiçe sayan anti demokratik kanun ve uygulamaların hayata geçirilmekte olduğu bilinmekte ise de, ülkemiz, kendi insanının huzuru ve refahı için hürriyetçi tavrından vazgeçmemelidir.

- İletişimin denetlenmesi tedbirine başvurulmasında aşırı hassasiyet gösterilmesinin demokratik yapımızı yıkmaya çalışan yıkıcı ve bölücü faaliyetlere verilmiş prim olarak anlaşılmaması bakımından kolluk güçleri birtakım ek metotlara kavuşturulabilir. Bunlardan akla ilk geleni, halen ABD'de uygulanmakta olan gezici takip (roving tap) sistemidir. Bu sistemle, hedef kişinin kullandığı bir cihazın takibe alınması yerine, verilecek bir karar marifetiyle kişinin kullanabileceği tüm cihazların denetlenmesine imkan tanınmaktadır. Teröristler ve organize suç şebekesi üyelerinin, kullandıkları iletişim araçlarını çabucak ve ustalıkla değiştirebildikleri ve bu konuda eğitim aldıkları gerçeğinden hareket edilerek çıkarılan bu hüküm, gelişmiş yöntemleri kullanan teröristlerin daha kolay takibinin sağlanması bakımından yarar sağlayacaktır. Bununla birlikte, bu yöntemin genele teşmil edilmesi ve uygulama ile masum kişilerin özel hayatlarının ihlal etmesi engellenmelidir.

- İletişimin denetlenmesi kararlarının yerine getirilmesi amacıyla kurulan TİB, uzun vadede, ilgili kurumlar için analiz ve değerlendirmelerde bulunan uzman bir kurum haline getirilmelidir. Merkeziyetçi bir anlayış üzerine bina edilmiş olan TİB'in varlığı, denetim süreci bakımından da oldukça yararlıdır. Bu bağlamda kurum, hukuk ve enformatik alanında uzmanlaşmış kişilerle takviye edilmeli, başka ülkelerdeki benzer kurumların çalışmaları değerlendirilmelidir. Nitekim, bu kurumun, kendi çabası ve tecrübesi ile belki bir çeyrek asırda edinebileceği bilgi birikimi, bu hususta tecrübesi olan on ülke ile yapılacak bir yıllık çalışma ile elde edilebilecektir. Böyle bir çalışmanın diğer bir faydası da, ülkemizde henüz karşılaşılmamış olan ancak günün birinde ortaya çıkması muhtemel bir problemle ilgili olarak şimdiden gerekli tedbirlerin alınması ve suçla mücadelede planlı adımların atılmasıdır. Bu tür faaliyetlerin yapılması, diğer ülkelerdeki tecrübelerden yararlanılması amacıyla yurtdışına uzman gönderilmesi, başta zaman ve para israfı olarak değerlendirilse bile, yetişmiş eleman ve gelişmiş bilgi dağarcığının faydası orta vadede anlaşılacaktır. Orta vadede verim alınabilecek bu tür çalışmaların yanı sıra, daha kısa vadeli faydalar bakımından, uluslararası nitelikte sempozyumların organize edilmesi, atölye çalışmalarının yapılması yarar sağlayacaktır. Üniversitelerle işbirliği halinde yapılması halinde daha sağlam bilimsel temellere oturtulabilecek bu çalışmalar, diğer ülkelerde uzun zamandan beri uygulanagelen sistemlerin ülkemiz kamuoyuna ve uygulayıcıları anlatılabilmesi bakımından önem taşımaktadır.

- TİB'de bulunan gizli bilgilerin hakim ve savcıların elektronik ortamda kullanımına açılması yargılamayı hızlandıracaktır. Hakimlerin karar verme aşamasında TİB'de bulunan bilgileri görebilmeleri, isim ve adres bilgilerini kontrol etmeleri, sorumluluk alanlarına göre kurumların görev ve yetki alanlarının denetlenmesini sağlayacaktır. Hakim ve savcıların, TİB'de bulunan bilgilere ulaşarak, tedbir talepleriyle ilgili işlem arşivini görebilmelerinde büyük yarar bulunmaktadır. Yargının modernizasyonu çerçevesinde uzun bir süreden beri yapılan çalışmalar sonucunda gerek adliyelerin ve adliye personelinin, gerekse hakim ve savcıların imkanları artırıldığından, böyle bir çalışmanın altyapı sıkıntısı olmayacaktır. Böyle bir çalışmanın gerçekleştirilmesi sonucunda, gereksiz yazışmalar ve bürokratik duvarlar ortadan kaldırılacaktır.

- Bu çalışmanın içeriğinde de vurgulandığı üzere, temel hak ve hürriyetlere ağır bir müdahale niteliği taşıyan iletişimin denetlenmesi tedbirinin uygulanması, toplumun huzur ve refahı ile suçla mücadele bakımından hayati bir zorunluluktur. Ancak temel

hak ve hürriyetleri güvence altına almak amacıyla yapılan yasal düzenlemelerdeki ve kurumsal yapılaşmadaki eksikliklerin de bir an önce giderilmesi gerekmektedir.

KAYNAKÇA

ACURMAN, Hüseyin, “Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi”, http,//www.kocaelibarosu.org.tr/dergi/makale,(15.7.2007),

ADLER, Andrew, “The Notice Problem, Unlawful Electronic Surveillance, and Civil Liability Under the Foreign Intelligence Surveillance Act”, *Lexis-Nexis Online*, (1.11.2007),

AKMANLAR, Bülent, (1982) “Avrupa Konseyi Üyesi Bazı Devletlerde Telefon Konuşmalarının Dinlenmesi Ve Telekomünikasyonun Kaydedilmesi”, *Yargıtay Dergisi*, S.1982/4.

ALCARAZ, Hubert, (2005) “Sonorisation et Ecoutes Téléphonique, La France Se Fait ‘Tirer L’Oreille’ A Propos Des Arrets Vetter Et Mahteron De La Cour Europeenne Des Droits De L’Homme”, *Revue Trimestrielle Des Droits De L’Homme,Bruylant,* dr.h.(66/2005).

ALTIPARMAK, Kemal (2006), “Büyük Biraderin Gözetiminden Çıkış, Telefonların İzlenmesinde Devletin Sorumluluğu”, *Türkiye Barolar Birliği Dergisi,* S. 63.

AMERİCAN CIVIL LIBERTIES UNION, “The Usa Patriot Act and Government Actions that threatens Our Civil Liberties”, http,//www. aclu.org/ FilesPDFs/ Patriot% 20 act%20flyer.pdf,(24.11.2007).

AN OVERVIEW OF ELECTRONİC SURVEILLANCE, HISTORY AND CURRENT STATUS,1996,http.//swiss.csail.mit.edu/6805/articles/crypto/nrc-report/nrc0d.txt , Cryptography's Role in Securing the Information Society, Prepublication, May 30, , Appendices. (15.10.2007)

ANAYURT, Ömer, (2004), *Avrupa İnsan Hakları Hukukunda Kişisel Başvuru Yolu*, Seçkin Yayınları, Ankara (Avrupa İnsan Hakları Hukukunda Kişisel Başvuru Yolu).

ANAYURT, Ömer, (1997) “Strazbourg İçtihatlarında Türk Ve Fransız Hukuklarında Telefon Dinlemeleri”, *Mülkiyeliler Birliği Dergisi*, C. XXI S. 197.

ARSLAN, Gülay,(2007), *Avrupa İnsan Hakları Mahkemesinin Özel Yaşam Hakkına Müdahaleyle Elde Edilmiş Deliller Hakkındaki Güncel Kararlarının İlgili Paragrafları, Özel Yaşam Medya ve Ceza Hukuku*, Ankara.

AYCİ, Emrullah, (2005), "İletişim Özgürlüğü Ve Özel Hayatın Gizliliği", *Polis Dergisi*, Sayı 45, Temmuz-Ağustos-Eylül, S. 13.

BALTACI, Vahit, (2007),*Yeni TCK ve CMK'da Terör Suçları ve Yargılaması*, Seçkin Yayınevi, Ankara.

BANKS, William C. ve M.E BOWMAN, (2001), "Executive Authority For National Security Surveillance", American University Law Review [Vol. 50,1,2001, http//www.wcl.american.edu/journal/lawrev/50/banks.pdf?rd=1, (16.11.2007).

BAYRAM, Levent, "Ses Ve Görüntü Kayıtlarının Türk Hukukundaki Yeri", *Polis Bilimleri Dergisi*, Cilt 6 (3-4), S. 1-11.

BERMAN, Jerry ve Paula BRUENİNG, (2006),"Is privacy still possible ın the twenty first century?", Center for Democracy and Tecnology, 6 November, http,//www.cdt.org/publications/privacystill.shtml , (12.11.2007).

BEŞE, Ertan , (2002), *Terörizm, Avrupa Birliği ve İnsan Hakları*, Ankara.

BULZOMI, MICHAEL J., (2003), "Foreign Intelligence Surveillance Act, Before and After the USA PATRİOT Act", The FBI Law Enforcement Bulletin, http,//www.fbi.gov/publications/leb/2003/june2003/june03leb.htm#page 26, (27.8.2007),

CENTEL, Nur ve Hamide Zafer, (2006), *Ceza Muhakemesi Hukuku***,** 4. Bası,İstanbul.

CENTEL, Nur ve Hamide Zafer, (2003), *Ceza Muhakemesi Hukuku***,** İstanbul.

CENTEL, Nur, (2001), "Ceza Muhakemesi Usulü Kanunu 2000 Tasarısına Eleştirel Yaklaşım", *Mahmut Teffik Birsel'e Armağan*, İzmir,(Armağan).

CENTEL, Nur, (1995), "Koruma Tedbirlerinde Gelişmeler", *Hukuk Araştırmalar Dergisi*, S.77.

CHARRIER, Jean-Loup, (2005), "Code de la Convention Européen des Droit de l'Homme", *Lexis-Nexis Yayınları*.

COLE, David, (2003),"What Patriot II Proposes To Do", Georgetown Univ. Law Center, February 10, http,//www.cdt.org/security/usaPatriot/030210cole.pdf (9.1.2008)

COMMUNICATIONS ASSISTANCE FOR LAW ENFORCEMENT ACT, http,//www4.law.cornell.edu/uscode/search/display.html?terms=2522&url=/uscode/html/uscode18/usc_sec_18_00002522----000-.html (3.11.2007)

CONGRESSIONAL TESTİMONY OF ROBERT S. MUELLER, (2005), "III, Director, Federal Bureau of Investigation Before the United States Senate Committee on the Judiciary Sunset Provisions of the USA Patriot Act" April 5, http,//www.fbi.gov/congress/congress05/mueller040505.htm (17.11.2007)

COUNCIL OF EUROPE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA, 28.I.1981,http,//conventions. coe.int/Treaty/en/ Treaties/Word /108.doc,(13 .12.2007)

CRIME CONTROL OMNIBUS CRIME CONTROL AND SAFE STREETS ACT,Public Law 90-351; 82 STAT. 197 [H. R. 5037], June 19 P.L. 90-351.

COŞKUN, Atilla, (2002), *Örgütlü Suçlar Ve Çıkar Amaçlı Suç Örgüleri İle Mücadele Kanunu*, Ankara.

CRS REPORT FOR CONGRESS, (2006) Updated December 21, Brian T. Yeh, Charles Doyle Senior Specialist, http,//www.fas.org/sgp/crs/intel/RL33332.pdf (19.11.2007).

ÇOKSEZEN, Atakan, (2006), *5271 Sayılı Ceza Muhakemesi Kanunu Ve Avrupa İnsan Hakları Sözleşmesi Çerçevesinde Ceza Muhakemesi Tedbiri Olarak İletişimin Dinlenmesi*, İstanbul.

ÇOLAK, Haluk ve Mustafa TAŞKIN, (2007), *Ceza Muhakemesi Kanunu Şerhi,* Ankara.

DETERMINING THE "INTERCEPTION" OF ELECTRONIC COMMUNICATIONS FOLLOWING, UNITED STATES V. COUNCILMAN'S REJECTION OF THE STORAGE/TRANSIT DICHOTOMY*, Lexis-Nexis Online,* (1.11.2007).

DECKER, Brian R., "The Future Of Unenumerated Rights, Part Two Of Three, Comment, "The War Of Information, The Foreign Intelligence Surveillance Act, Hamdan v. Rumsfeld, And The President's Warrantless-Wiretapping Program", Trustees of the University of Pennsylvania, University of Pennsylvania Journal of Constitutional Law, *Lexis-Nexis Online*, (1.11.2007).

DEMPSEY, James X., (1997), “Communıcatıons Prıvacy In The Dıgıtal Age, Revıtalızıng The Federal Wiretap Laws To Enhance Privacy”,Originally Published in the Albany Law Journal of Science & Technology,Volume 8, Number1,http,//www.cdt.org/publications/lawreview/1997albany.shtml#t33(25.9. 2007).

DİNÇ, Güney, (2006), “Sorularla Avrupa İnsan Hakları Sözleşmesi”, *Türkiye Barolar Birliği Yayınları*,

DOERNBERG, Donald L. "Can You Hear Me Now?", Expectations of Privacy, False Friends, and the Perils of Speaking Under the Supreme Court's Fourth Amendment Jurisprudence, *Lexis-Nexis Online*, (1.11.2007).

DOĞRU, Osman, (2002), *İnsan Hakları Avrupa Mahkemesi İçtihatları,* Cilt 1, İstanbul.

DONAY, Suheyl ve Mahmut KAŞIKÇI, (2005), *En Son Değişikliklerle Açıklamalı Ve Karşılaştırmalı Türk Ceza Kanunu,* Beta Yayınları, Ankara.

DONOHUE, Laura K., (2006), “Criminal law, Anglo-American Privacy and Surveillance”, Northwestern School of Law, Journal of Criminal Law & Criminology, 96 j. Crim. L. & criminology 1059, , *Lexis-Nexis Online*, (1.11.2007),(http//iis-db.stanford.edu/ pubs/21219/Privacy and Surveillance .pdf).

DÖNMEZER, Sulhi, (2000), “Çetelerle Mücadele Amacıyla 4422 Sayılı Kanunla Kabul Edilen Koruma Tedbirleri”, *Yargı Reformu 2000 Sempozyumu*, İzmir.

DÜLGER Murat Volkan, “Avrupa İnsan Hakları Mahkemesi Kararlarında Organize Suçla Mücadelede Özel Koruma Tedbirleri”, (http//www.hukukcu.com/bilimsel/kitaplar /aihmd organizesuc.htm).(15.09. 2007).

DUTERTRE, Gilles, (2003), *Key case-law extracts : European Court of Human Rights, Council of Europe Publications*, Strasbourg.

EFF ANALYSIS OF THE PROVISIONS OF THE USA PATRİOT ACT, (2001), That Relate To Online Activities (October 31,), Last updated October 27, 2003, http,//w2.eff.org/Privacy/Surveillance/Terrorism/20011031 eff usa Patriot anal ysis.php, (25.9.2007).

EHRLICH, Tim, "Case study on Lawful Intercept", *Presented to, Harward Law School Cyber Law and The Global Economy, Presented by*, Latham and Watkins LLP, (8.11.2007).

ELECTRONIC PRIVACY INFORMATION CENTER,(1998), Approvals for Federal Pen Registers and Trap and Trace Devices 1987-1998, http,//www.epic.org/ privacy/ wiretap/stats/penreg.html (18.11.2007).

ELECTRONIC PRIVACY INFORMATION CENTER, The US Patriot Act Sunset,(Patriot Sunset, EPIC Report), http,//www.epic. org/privacy/ terrorism/ usa Patriot/sunset.html (24.11.2007).

ELECTRONIC PRIVACY INFORMATION CENTER, The USA PATRİOT Act, (The USA Patriot Act, EPIC Report) http,//www.epic.org/ privacy/ terrorism/ usa Patriot / default.html (19.11.2007).

ELECTRONIC PRIVACY INFORMATION CENTER, (epic), Approvals for Federal Pen Registers and Trap and Trace Devices 1987-1998, (Source, US Justice Department Annual Reports to Congress) http,//www.epic.org/privacy /wiretap/ stats/ penreg.html (Source, US Justice Department Annual Reports to Congress) (10.11.2007).

ENGUÉLÉGUÉLÉ, Stéphane ve Stéphanie LOURDEL, " Three Recent Arguments For The Expansion Of Human Rights In French Criminal And Administrative Law", http,//www.gonzagajil. org/pdf/volume1/Engueleguele/Engueleguele.pdf (3.12.2007).

ERDEM, M. Ruhan ve Veli Özer ÖZBEK, (2000), "4422 Sayılı Çasömk Çerçevesinde Uzakla Haberleşmenin Denetlenmesi" , *Seyfullah Edis'e Armağan,* İzmir.

ERDEM, M. Ruhan, (2005), "5271 Sayılı Ceza Muhakemesi Kanunu'nda İletişimin Denetlenmesi", *Hukuki Perspektifler Dergisi*, Sayı 3, Nisan.

ERDEM, M. Ruhan, (2001), *Ceza Muhakemesinde Organize Suçlulukla Mücadelede Gizli Soruşturma Tedbirleri*, Ankara, (Gizli Soruşturma).

ERGEÇ, Ruşen,(2004) *Protection Européenne et Internationale des Droit de l'Homme,* Bruylant.

ERGÜL, Ozan, Yargıdan Telefon Dinlemeye Yeni Bir Yorum, www. Yasayan Anayasa.ankara.edu.tr/docs/analizler/telefon_dinleme.pdf, (14.03.2007).

ERRERA, Roger,(2003), "Les Origines de la loi Française du 10 Juillet 1991 sur Les Ecoutes Téléphoniques", *Revue Trimestrielle Des Droits De L'Homme*, Bruylant, dr.h.(5.5.2003).

ERYILMAZ, Mesut Bedri, (2006), "Suçla Mücadele Politikası Açısından Yeni Ceza Muhakemesi Kanunu", *Ceza Hukuku Dergisi*, Sayı 1, Eylül.

FACT SHEET, "Usa Patriot act provisions set for reauthorization",(Patriot act Fact Sheet), http,//www.lifeandliberty.gov/agPatriotactrevision.htm (24.11.2007).

FEINGOLD, Russ ,(2002)," Statement on the Anti-Terrorism Bill" (25.10.2002).

FENWICK, Helen*, Civil Liberties and Human Rights, Cavendish Publishing*, Third Editiion, 2002.

FREIWALD, Susan, First Principles of Communications Privacy, *Lexis-Nexis Online*, (1.11.2007).

FOREİGN INTELLIGENCE SURVEILLANCE ACT, http,//fas.org/irp/ agency/ doj/ fisa (last visited June 9, 2006). (Statistics compiled), (23.12.2007)

FOSTER, Steve, (2003*), Human Rights And Civil Liberties,* Longman.

GELERİ, Aytekin, (1998), "Organize Suçlarla Mücadelede Elektronik Takibin Rolü", *Asayiş Daire Başkanlığı*, Ankara.

GÖKCEN, Ahmet, (1994), *Ceza Muhakemesi Hukukunda Basit Elkoyma Ve Postada Elkoyma (Özellikle Telefonların Gizlice Denetlenmesi),* Ankara.

GÖZÜBÜYÜK, A. Şeref, (1995), "Avrupa İnsan Hakları Komisyonu Kararlarından Seçme Özetler",*İHMD*, Ocak 1995, C.III, S.1.

GÜVEL, Enver Alper, (2004), *Organize Suç Ekonomisi Ve Hukuk Uygulaması,* Ankara.

HANUCH_S. Sebastien,(2004), "İnterception",http,//www.supinfo-projects. com /fr/2004 /interception) (12.10.2007)

HARIS, D. J., M. O'BOYLE ve C. WARBRICK (1995), *Law of the European Convention on Human Rights,* London, Butterworths.

HOUSE PERMANENT SELECT COMMITTEE ON INTELLİGENCE, http //intelligence.house.gov/AboutTheCommittee.aspx?Section=1, (25.10.2007)

INTERCEPT ORDERS ISSUED BY JUDGES DURING CALENDAR YEAR 1997, http,//www.uscourts.gov/wiretap/table2.pdf; (29.10.2007)

INTERNATIONAL COVENANT ON CIVIL AND POLITICAL RIGHTS, http,//www.unhchr.ch/html/menu3/b/a_ccpr.htm , (4.12.2007)

JUDGE, Michael P, KALUNIAN Robert ve QUANT Kathy, "Brief Overwiev of the Wiretap Law", http,//pd.co.la.ca.us/overv.htm, (26.9.2007)

JURISDICTIONS WITH STATUTES AUTHORIZING THE INTERCEPTION OF WIRE, ORAL, OR ELECTRONIC COMMUNICATIONS EFFECTIVE DURING THE PERIOD (2006), January 1 Through December 31 2006", http,//www. uscourts. gov/wiretap06/Table1.pdf, (01.10.2007)

KALABALIK, Halil, (1997), " İdare Hukukunda Takdir Yetkisi Kavramı Ve Benzer Kurumlarla Karşılaştırılması", *Gazi Üniversitesi Hukuk Fakültesi Dergisi*, C. I – S. 1 (6/1997)

KALABALIK, Halil, "İdarenin Takdir Yetkisinin Sınırları Ve Yargısal Denetimi", *Gazi Üniversitesi Hukuk Fakültesi Dergisi*, CİLT I - SAYI 1, (6/1997)

KARAYAZGAN, Mehmet, (2005), "Yeni Tck İle İletişimin Tespiti, Dinlenmesi Ve Kayda Alınması", *Polis Dergisi*, Sayı 44, Nisan-Mayıs-Haziran.

KAYA, Abdulkadir, (2006), "Adalete Erişim İçin Sürekli Mesleki Gelişim, İnsan Hakları", *Boğaziçi Üniversitesi Avrupa Çalışmaları Merkezi*, İstanbul.

KAYA, Abdulkadir,(2006), "Avrupa İnsan Hakları Kararları Işığında "İletişimin Dinlenmesi Ve Teknik İzleme", *Yargı Dünyası*, Sayı 129, Eylül,(İletişimin Dinlenmesi).

KAYMAZ, Seydi, (1996), "Mevcut Yasal Düzenlemeler Karşısında Telefon İle Yapılan Haberleşmenin Denetlenmesi", *İstanbul Barosu Dergisi*, Sayı 1, İstanbul.

KEKLİK, Ramazan, (2005), "Ceza Yargılamasında İletişimin Denetlenmesi", *Adalet Dergisi*, Sayı 17.

KHAN, Zmarak, (2006), “The National Security Agency (NSA) Eavesdropping on Americans, A Programme that is Neither legal Nor Necessary”,*Utrecht Law Review*, Volume 2, Issue 2(December)- http,//www.utrechtlawreview.org/,63, (19.10.2007)

KILKELLY, Ursula, (2001), *Özel Hayata ve Aile Hayatına Saygı Gösterilmesi Hakkı,* İnsan Hakları El Kitabı, No 1, Strasbourg.

KOYUNCU, Tuğçe, (2005), “Telekomünikasyon Yoluyla Yapılan İletişimin Tespiti”, *Hukuk Gündemi Dergisi*, CMK Dosyası.

KÖROĞLU, Hasan , (2001), *Örgütlü Suçluluk* , Ankara.

KUNTER, Nurullah, F.YENİSEY ve A. NUHOĞLU, (2006), *Ceza Muhakemesi Hukuku,* 15. Bası, İstanbul.

KUZULOĞLU, M. Serdar, (2002), “Dikkat, e-kulaklar işbaşında!”, *Radikal*, 06/07/2002, (4.10.2007)

KÜNHE, Hans-Heiner, (2004), “Avukat Telefonlarının Dinlenmesi”, Karşılaştırmalı Güncel Ceza Hukuku Serisi 3”, Çev. Hakan Hakeri, Ankara.

LEACH, Philip, “Taking A Case to the European Court of Human Rights”, *Oxford University Press*, Second Edition.

LICHTBLAU, Eric ve James RİSEN, (2003), “Aftereffects, Intelligence Gathering; Broad Domestic Role Asked For C.I.A. and the Pentagon”, http,//query.nytimes.com/gst/fullpage.html?res=9F01E6D8173CF931A35756C0A9659C8B63(26.11.2007)

LUENING, Erich, “Don't be fooled, DCS1000 still a 'Carnivore' at heart”, http,//news.zdnet.com/2100-9595_22-528089.html, (4.10.2007)

MACARTHUR, Andrew P., “The NSA Phone Call Database, The Problematic Acquisition And Mining Of Call Records In The United States, Canada, The United Kingdom, And Australia”, *Lexis-Nexis Online*, (1.11.2007)

MADDOX, Laurie M.,(1984), “Criminal Procedure- Search and Seizure- Interception of Cordless Telephone Communication Does Not Violate Title III of Omnibus Crime Control Act of 1968*”, Missisipi Law Journal*, Heinonline, 54 Mss.339

MALKOÇ, İsmail ve Mert YÜKSEKTEPE, (2005),*Ceza Muhakemesi Kanunu,* Ankara.

MCCARTHY, Kieren, (2001), “What Are Those Words That Trigger Echelon?”, http,//www.theregister.co.uk/2001/05/31/what_are_those_words/, (4.10.2007)

MECHAM, Leonidas Ralph,(2006), “Report of the Director of the Administrative Office of the United States Courts on Applications for Orders Authorizing or Approving the Interception of Wire, Oral, or Electronic ommunications”, http,//www.uscourts.gov/wiretap06/Table22006.pdf (25.10.2007)

METİN, Yüksel, (2002) *Ölçülülük İlkesi, Karşılaştırmalı Bir Anayasa Hukuku İncelemesi,* Seçkin Yayınevi, Ankara.

MIHÇAK, Muhittin, (2003) *Çıkar Amaçlı Suç Örgütleri Ve Cürüm İşlemek İçin Teşekkül Oluşturmak Suçları,* Ankara.

MOWBRAY, A., (2001), *Cases and Materials on the European Convention on Human Rights,* Butterworths.

MUELLER, Robert S,(2005), “Congressional Testimony, Federal Bureau of Investigation Before the United States Senate Committee on the Judiciary Sunset Provisions of THE USA PATRIOT ACT” April 5, 2005, http,//www.fbi.gov/congress/congress05/mueller040505.htm (17.11.2007)

CASEY, Holland, “Neither Big Brother Nor Dead Brother, The Need for a New Fourth Amendment Standard Applying to Emerging Technologies”, *Lexis-Nexis Online*.

NEW YORK LAW REVIEW, ADMISSIBILITY OF EVIDENCE OBTAINED BY TAPPING TELEPHONE WIRES, Volume VI, Mart 1928, Sayı 3, sayfa 81, Hein Online—6, 80, 1928,(1.11.2007)

NOYAN, Erdal , (2005*), Ceza Muhakemesi*, Ankara.

NUHOĞLU, Ayşe, (2006), “Adli Amaçlı Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi”, *Yargı Dünyası*, Sayı 128, Ağustos.

OMNIBUS CRIME CONTROL AND SAFE STREETS ACT, Public Law 90-351; 82 Stat. 197 [H. R. 5037], June 19 P.L. 90-351. http,//www.fcc.gov/Bureaus/ OSEC/ library/legislative_histories/1615.pdf, (16.11.2007)

OSKAY, Ünsal, (1969), *Kitle Haberleşme Teorilerine Giriş*, Ankara.

OVEY, Claire ve Robin WHITE, *"Jacobs and White", European Convention on Human Rights,* Oxford Press, Third Edition, 2002.

ÖZBEK, Veli Özer, (2006), *Ceza Muhakemesi Hukuku*, Ankara.

ÖZBEK, Veli Özer, Koray DOĞAN, Pınar BACAKSIZ, ve M. Nihat KANBUR, ,(2007), *Ceza Muhakemesi Hukuku Bilgisi,* Ankara .

ÖZDOĞAN, Ali, "Alman ve Fransız Teknik Dinleme Mevzuatları", (www.egm. gov. tr/polis.dergisi.32.sayi.(23.9. 2007),

ÖZDOĞAN, Ali, (2004), Teknik Dinlemeye Dair, "Gizli Dinleme Kanunlarına ve Uygulamalarına Dair Bir Araştırma", *Emniyet Genel Müdürlüğü İDB yayınları* No. 92, Ankara,(2004).

ÖZEK, Çetin, 1998 "Organize Suç", *Nurullah Kunter'e Armağan*, İstanbul.

ÖZEN, Mustafa, (2007), "Haberleşmenin Gizliliğini İhlal Suçu", *Terazi Aylık Hukuk Dergisi*, Yıl 2, Sayı 10, Haziran.

ÖZTÜRK, Bahri, (2000) "Ses Ve/Veya Görüntü Kaydeden Araçlarla Yapılan Tespitlerin Ceza Muhakemesi Hukukundaki Yeri",Prof. Dr. *Seyfullah Edis'e Armağan, İzmir*,(Armağan)

ÖZTÜRK, Bahri , (1991), *Ceza Muhakemesi Hukukunda Koğuşturma Mecburiyeti İlkesi (Hazırlık Soruşturması),* Ankara.

ÖZTÜRK, Bahri, M. Ruhan ERDEM, ve Veli Özer ÖZBEK, (2004), *Uygulamalı Ceza Muhakemesi Hukuku,* Ankara.

PARLAR, Ali ve Muzaffer HATİPOĞLU, (2007), *5237 Sayıl Türk Ceza Kanunu Yorumu,* 1-2. Cilt, Ankara.

PAUL, M., (2007), "Reviving Telecommunications Surveillance Law", University Chicago Law School Surveillance Symposium, (June 2007),http,//www.law. uchicago. edu/Lawecon/events/schwartz.pdf, (16.11.2007)

PODESTA, John, (2002), USA Patriot Act, , "The Good, the Bad, and the Sunset American Human Rights Association", *Human Rights Magazine*, http,//www. abanet. org/irr/hr/winter02/podesta.html (19.11.2007)

POLAT, Ahmet, (2005), “Fransa’da Terörizme Karşı Mücadele”, *Polis Dergisi*, Sayı 46, Ekim-Kasım Aralık.

PRIVACY, WIRE TAP ACT, http,//ilt.eff.org/index. php/Privacy, Wiretap Act# Electronic Communications, (9.10.2007)

REHMAN, Javaid, (2003), *International Human Rights Law*, A Practical Approach.

RENUCCI, Jean, (2001), *Droit Européen Des Droit De L’Homme,* İkinci baskı.

REPORT OF THE U.S. DEPARTMENT OF JUSTICE, (2002), Office of Legislative Affairs, 26.7.2002, http,//www.lifeandliberty.gov/subs/congress/ hjcPatriotact combined responses3, (15.9.2007).

REPORT OF THE EUROPEAN PARLIAMENT, “ On The Existence Of A Global System For The Interception Of Private And Commercial Communications “(Echelon Interception System) (2001/2098(INI)) 11 July 2001, http,//www.fas.org/irp/ program/process/rapport echelon en.pdf, (4.12.2007).

ROSS, Brian ve Vic WALTER, (2007), “Exclusive, Report Says FBI Violated Patriot Act Guidelines”, 8 March 2007, http,//blogs.abcnews.com/ theblotter/2007 /03/ exclusive repor.html, (19.11.2007).

SAĞLAM, Fazıl, (1982), *Temel Hakların Sınırlanması ve Özü*, Ankara Üniversitesi Siyasal Bilgiler Fakültesi Yayınları.

SCHMID, Gerhard,(1999), “Rapport, Sur Le Projet De Résolution Du Conseil Relative À L'interception Légale Des Télécommunications Compte Tenu Des Nouvelles Technologies, Commission Des Libertés Publiques Et Des Affaires Intérieures”, 23 April 1999 http,//www.europarl. europa.eu/sides/getdoc. do?pubref=// ep// text+report+a4-1999-0243+0+doc+xml+v0//fr), (19.04.2007).

SCHWARTZ, Paul M.,(2007), “Reviving Telecommunications Surveillance Law” *University Chicago Law School Surveillance Symposium* (June 2007), http,//www.law.uchicago.edu/Lawecon/events/schwartz.pdf, (16.11.2007)

SÖZÜER, Adem, (1997), “Türkiye’de Ve Karşılaştırmalı Hukukta Telefon, Teleks, Faks Ve Benzeri Araçlarla Yapılan Özel Haberleşmenin Bir Ceza Yargılaması Önlemi Olarak Denetlenmesi”, *İHFM, Türkan Rado’ya Armağan*, C.LV, S.3.

STEVENS, Gina ve Charles Doyle, “Privacy: An Overview of Federal Statutes Governing Wiretapping and Electronic Eavesdropping”, *CRS Report for Congress*, Order Code 98-326.

STONE, R, (2004),*Textbook on Civil Liberties and Human Rights*, Oxford University Pres.

SUDRE, F, (2005), *Droit Européen et International des Droits de l’Homme*,(Droits de l’Homme) Presses Universitaires de France, 7. Baskı, (Droit de l’Homme).

SUDRE, F., J.P. MARGUENAUD, J. ANDRIANTSIMBAZOVINA, , A. GOUTTENOIRE, ve M. LEVINET, (2003),*Les Grandes Arrêts de la Cour Européenne des Droits de l’Homme,* Themis, yayınları, İkinci baskı.

ŞAHİN, Cumhur, (2006), *Ceza Muhakemesi Şerhi*, Ankara.

ŞAHİN, Cumhur, (2007), *Ceza Muhakemesi Hukuku*, C :1,Seçkin Yayınları,

ŞAFAK, Ali, (2003), *Suç Organizasyonu Ve Kovuşturma Usulü*, Temmuz.

ŞEN, Ersan, (2007), “İletişimin Dinlenmesi Tedbiri”, *Ceza Hukuk Dergisi*, Seçkin Yayınları, S. 4, (İletişimin Dinlenmesi Tedbiri)

ŞEN, Ersan, (2005), “5237 Sayılı Türk Ceza Kanununda “Özel Hayata Karşı Suçlar”, *İstanbul Barosu Dergisi*, C. 79, S.3, (ÖHKS).

ŞEN, Ersan,(1999), “Türk Hukukunda Telefonların Gizlice Dinlenmesi Sebebiyle Gündeme Gelen Hukuka Aykırılık Sorunu Ve Kişi Haklarına Keyfi Müdahaleler”,*Prof. Dr. Sahir Erman’a Armağan ,İÜHF Eğitim, Öğretim Ve Yardımlaşma Vakfı Yayını*, No.8 İstanbul.

ŞEN, Ersan, (1996), *Devlet Ve Kitle İletişim Araçları Karşısında Özel Hayatın Gizliliği Ve Korunması,* İstanbul.

ŞEN, Ersan, (1993), “Gizli Dinleme Ve Görüntüleme Fiillerinin Türk Hukukundaki Yeri Üzerine Bir İnceleme”, *İstanbul Barosu Dergisi* , 1993/7-8-9.

ŞİMŞEK, Oğuz, “4422 Sayılı Çıkar Amaçlı Suç Örgütleriyle Mücadlee Kanunu Ve Kanunun 4. Maddesine Göre “Kayıt Ve Verilerin İncelenmesi” Ve Kişisel Nitelikli Verilerin Korunması”, www.idealhukuk. com/hukuk_rehberi/ akademik/ kayıt _ve _verilerin_incelenmesi htm) (9.9.2007)

TEZCAN, Durmuş, M. Ruhan ERDEM, ve Oğuz SANCAKTAR, (2004), *AİHS Işığında Türkiye'nin İnsan Hakları Sorunu,* Ankara.

TEZCAN, Durmuş, M. Ruhan ERDEM, ve Oğuz SANCAKTAR, (2004),*Avrupa İnsan Hakları Sözleşmesi Ve Uygulaması,* Adalet Bakanlığı Eğitim Dairesi Başkanlığı, Ankara, (AİHM).

TEZCAN, Durmuş, M. Ruhan ERDEM, ve Murat ÖNOK, (2006), *5237 Sayılı Türk Ceza Kanunu'na Göre Teorik Ve Pratik Ceza Özel Hukuku,* Ankara.

TOROSLU, Nevzat ve Metin FEYZİOĞLU, (2006),*Ceza Muhakemesi Hukuku,* Ankara.

TOSUN, Öztekin, (1976), "Ceza Muhakemesinde Koruma Tedbiri Olarak Gizli Dinleme",*İÜHFM*,C.41, (Gizli Dinleme).

TOSUN, Öztekin, (1984),*Türk Suç Muhakemesi Hukuku Desleri,* C. I Genel Kısım, İstanbul.

TURHAN, Faruk , (2006),*Ceza Muhakemesi Hukuku,* Ankara.

UNITED KINGDOM PARLIAMENT, "Joint Committee on Human Rights" First Report http,//www. publications. parliament.uk/ pa/jt200001/jtselect/ jtrights/69/ 6917. htm#n123, (19.12.2007)

UNITED STATES CODE, Title 18 -- Crimes And Criminal Procedure, Chapter 119 -- Wire And Electronic Communications Interception And Interception Of Oral Communications http,//nsi.org/Library/Comm/ecpa.htm ,(6.9.2007)

UNITING AND STRENGTHENING AMERICA BY PROVIDING APPROPRIATE TOOLS REQUIRED TO INTERCEPT AND OBSTRUCT TERRORISM ACT, (Usa Patriot Act), Calendar NO. 198, 107th Congress, 1st Session H. R. 2975, http,//www.govtrack.us/data/us/bills.text/107/h/h2975.pdf ,(28.11.2007)

USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. 109-177, 102, 120 Stat. 192 (2006)

UZGÖREN, Orhan, (2004), "Özel Hayat, Aile Hayatı, Konut, Haberleşme", *Türkiye Barolar Birliği, İnsan Hakları Avrupa Sözleşmesi ve Adli Yargı Sempozyumu*, Ankara.

ÜNAL, Şeref, (2001), *Avrupa İnsan Hakları Sözleşmesi, İnsan Haklarının Uluslararası İlkeleri,* TBMM Kültür, Sanat ve Yayın Kurulu Yayınları.

ÜNVER, Naci, (2001), *Çıkar Amaçlı Suç Örgütleri Ve Cürüm İşlemek İçin Teşekkül Oluşturmak,* Ankara.

ÜNVER, Yener, (2006), "Ceza Muhakemesinde İspat, CMK ve Uygulamamız", *Ceza Hukuku Dergisi*, Yıl 1, Sayı 2, Aralık,(CHD).

ÜNVER, Yener ve Hakan HAKERİ, (2006), "Sorularla Ceza Muhakemesi Hukuku", *Türkiye Barolar Birliği*, Ankara.

WARREN, D. Samuel ve Louis D. BRANDEİS, "The right to privacy", Harvard Law Review, Vol.IV December 15, 1890 No.5, www.lawrence.edu/fast/boardmaw/ Privacybrand warr2.html, (15.5.2006)

WASHINGTON POST,(2007), "My National Security Letter Gag Order", Friday, March 23, 2007; Page A17, http,//www.washingtonpost.com/wp-yn/content/ article/ 2007/03/22/AR2007032201882.html , (8.9.2007)

WEINREB, Lloyd L., (1993), *Criminal Process, Cases, Comment, Questions,* Foundation Press, Fifthe Edition.

WONG, Thomas, "Regulation of Interception of Communications in Selected Jurisdictions", Research and Library Services Division Legislative Council Secretariat, 3.1.1. http,//www.legco .gov. hk/yr04-05/english/ sec/library/ 0405r p02e.pdf, (7.8.2007).

YARDIMCI, Mehmet Murat, (2005), *"Regulating Telephone Tapping In Turkey, The Influence Of The European Convention on Human Rights"*, University of Leicester (Faculty of Law),(Yayınlanmamış Yüksek Lisans Tezi).

YENİSEY, Feridun, (2000), "Çıkar Amaçlı Suç Örgütleri İle Mücadele Yöntemleri", *Hukuk Kurultayı 2000*, Ocak, Ankara,(Kurultay).

YENİSEY, Feridun , (1993), *CMUK Eki, 3842 Sayılı Kanunla Yapılan Değişiklikler Ve Zabıtayı İlgilendiren Maddeler* , İstanbul, (CMUK Eki).

YENİSEY, Feridun, (1991), *Ceza Muhakemesi Hukukunda Kovuşturma Mecburiyeti, (Hazırlık Soruşturması),* Ankara.

YENİSEY, Feridun ve Sinan ALTUNÇ, "Cmk 135 Hakkında", http,//www. hukukturk.com/fractal/hukukturk/pages/fhm.jsp, (25.07.2007).

YENİSEY, Feridun ve Erol CİHAN, (1997), *Ceza Muhakemesi Hukuku*, 5. Bası, İstanbul.

YILDIRIM, Gülşen, (2004), "Özel Hayat, Aile Hayatı, Haberleşme ve Mesken, İnsan Hakları Avrupa Mahkemesinin 8. Maddenin Genişletilmiş Yorumu İle Sağlanan Koruma", *Türkiye Barolar Birliği İnsan Hakları Avrupa Sözleşmesi ve Adli Yargı Sempozyumu*, Ankara.

YILDIZ, Ali Kemal , "Ses Ve/Veya Görüntü Kayıtlarının İspat Fonksiyonu", *Ceza Hukuku Dergisi,* Yıl 1, Sayı 2, Aralık 2006.

YİĞİT, Nuri, (2005), "Arama, Elkoyma Ve Gizli Koruma Tedbirleri", *Adalet Bakanlığı Seminer Notları*, Ankara.

YURTCAN, Erdener , *Ceza Yargılaması Hukuku,* 5. Bası, İstanbul 1994.

YURTCAN, Erdener,(1992), *CMUK Ceza Yargılaması Hukuku 1992 Değişiklikleri,* İstanbul 1992.

ZAFER, Hamide, (1999), *Ceza Hukukunda Terörizm,* İstanbul.

2005 Report of the Director of the Administrative Office of the United States Courts on Applications for Orders Authorizing or Approving the Interception of Wire, Oral, or Electronic Communications, Nisan 2006, http,//www.uscourts. gov/ wiretap 05/WTText.pdf, (9.8.2007)

2006 Report of the Director of the Administrative Office of the United States Courts on Applications for Orders Authorizing or Approving the Interception of Wire, Oral, or Electronic Communications, Nisan 2007, http,//www. uscourts. gov/ wiretap06 /2006WT.pdf, (19.8.2007)

ÖZGEÇMİŞ

1971 yılında doğan Mehmet Murat Yardımcı, Erzurum Anadolu Lisesi'nden 1989 yılında, Ankara Üniversitesi Hukuk Fakültesi'nden ise 1993 yılında mezun oldu. 1995 yılında Ankara Adli Yargı Hakim adayı olarak göreve başladı. Bir süre Altunhisar/Niğde Cumhuriyet Savcısı olarak görev yaptıktan sonra, Adalet Bakanlığı Uluslararası Hukuk ve Dış İlişkiler Genel Müdürlüğüne atandı. Halen anılan Genel Müdürlük bünyesinde Tetkik Hakimi olarak görevine devam etmekte olan Yardımcı, Dumlupınar Üniversitesi Sosyal Bilimler Enstitüsü bünyesinde (1997) 'Ölüm Cezası ve Uygulaması' başlıklı, İngiltere Leicester Üniversitesi Hukuk Fakültesi bünyesinde (2005) ise, 'Regulating Telephone Tapping: the Influence of European Court of Human Rights' başlıklı yüksek lisans tezlerini başarıyla tamamlamıştır.

Belçika'nın Brugges şehrindeki Avrupa Koleji'nde (College of Europe) yapılan eğitim programını ve Macaristan'ın Budapeste ve Visegrad şehirlerinde Avrupa Birliği hukuku alanında hakimleri eğitmeye yönelik olarak düzenlenen 'eğiticilerin eğitimi' programını başarıyla tamamlayan; suçluların iadesi, hükümlülerin transferi, sözleşme hukuku, çoçuk kaçırma suçları, uluslararası istinabe, insan hakları hukuku vb. konularda birçok yurtiçi ve yurtdışı toplantıya Adalet Bakanlığı'nı temsilen katılan Mehmet Murat Yardımcı, halihazırda Ülkemiz aleyhine Avrupa İnsan Hakları Mahkemesi'nde açılmış bulunan insan hakları davaları hakkında savunma hazırlamaktadır.

2002 yılında Avrupa Konseyi Pompideu araştırma bursunu kazanarak gittiği Hollanda'da 'Uyuşturucu suçları ve bu suçlardan mahkum olan kişilerin rehabilitasyonu' konusunda araştırmalar yapmış olan Mehmet Murat Yardımcı aynı yıl Fransız Kültür Merkezi tarafından yapılan bir sınav sonucunda başarılı olarak bir ay süre ile Fransa Milli Hakimlik Okulu'nda eğitim görmüş ve Fransız hukuk sistemi hakkında incelemelerde bulunmuştur. 2005-2006 yılları arasında 6 ay süre ile Avrupa İnsan Hakları Mahkemesinde de görevlendirilen Yardımcı, İngilizce ve Fransızca bilmektedir.